Санкт-Петербургский
институт
информатики и автоматизации
Российской Академии наук

Северо-Западный институт управления —
филиал Российской академии народного
хозяйства
и государственной службы
при Президенте Российской Федерации

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ И КОГНИТИВНАЯ БЕЗОПАСНОСТЬ

ПЕТРОПОЛИС
издательский дом

Санкт-Петербург
2017

ББК 87.6
УДК 1.14–327(470+571)
К 37

Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. ИД «Петрополис», Санкт-Петербург, 2017. —300 с. 32 рис., 8 табл.

ISBN 978-5-9676-0895-7

Рецензенты:

Белозеров Василий Клавдиевич, профессор, доктор политических наук, заведующий кафедрой политологии Московского государственного лингвистического университета;

Зегжда Петр Дмитриевич, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, руководитель отделения «Кибербезопасность» Санкт-Петербургского политехнического университета Петра Великого;

Щербаков Вячеслав Николаевич, доктор военных наук, профессор, контр-адмирал

В коллективной монографии «Информационно-психологическая и когнитивная безопасность» рассмотрен широкий круг вопросов, охватывающий исторические предпосылки и социально-политические реалии информационно-психологических угроз и безопасности в глобальном измерении, а также социально-психологические и когнитивные аспекты обеспечения национальной безопасности.

Книга предназначена для специалистов, занимающихся разработкой методов и средств ведения информационно-психологических операций и обеспечивающих информационно-психологическую безопасность, студентов и аспирантов, а также для широкого круга читателей.

ISBN 978-5-9676-0895-7

Содержание

Предисловие

Выход в свет данной книги весьма своевременен. Ее авторский коллектив сосредоточил внимание на разработке весьма актуальных проблем обеспечения национальной безопасности Российской Федерации. Обращает на себя внимание состав авторского коллектива — это крупные специалисты в области информационно-коммуникационных технологий, психологии и политологии, медиалогии и философии. Данный труд — наглядный пример формирования нового этапа синтеза научного знания в условиях четвертой промышленной революции. Судя по публикациям авторов книги, проблемы информационно-психологической и когнитивной безопасности давно уже стали предметом их исследовательской деятельности. Актуальность книги заключается, на наш взгляд, в том, что предложения и рекомендации, высказанные авторами во всех трех разделах, являются ответом на ряд ключевых положений Доктрины информационной безопасности Российской Федерации (5.12.2016), в которой прямо указано на то, что «расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств». Поэтому одним из основных направлений обеспечения информационной безопасности в области обороны страны должна выступать «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества». Надеюсь,

что данная работа вызовет большой интерес среди специалистов, учащейся молодежи и широкого круга читателей.

Хочу особо отметить, что данная коллективная монография явилась одним из важных результатов работы конференции «Информационная безопасность регионов России (ИБРР)», бессменным председателем Оргкомитета которой является директор Санкт-Петербургского института информатики и автоматизации РАН чл.-кор. РАН Р. М. Юсупов. По его инициативе в состав секций конференции несколько лет назад была включена и секция информационно-психологической безопасности, плоды деятельности которой представлены на страницах данной коллективной монографии.

Выход книги приурочен к 40-летию Санкт-Петербургского института информатики и автоматизации РАН (был образован 19.01.1978 г. на базе отдела вычислительной техники Физико-технического института им. А. Ф. Иоффе АН СССР как Ленинградский научно-исследовательский вычислительный центр АН СССР).

Академик РАН, научный руководитель
Санкт-Петербургского политехнического
университета Петра Великого
Ю. С. Васильев

Введение

Безопасность в предельно широком плане стала неотъемлемой принадлежностью всех сторон человеческой жизнедеятельности — от охраны труда до космической безопасности, от обеспечения информационно-психологической безопасности до разработки систем социальной и национальной безопасности. Авторы данной коллективной монографии [1] ограничились анализом одного из указанных выше направлений — информационно-психологической и когнитивной безопасности, — актуальность которого значительно возросла в условиях наступления новой, четвертой в индустриальной истории человечества, промышленной революции. Следует особо отметить, что еще в 1997 году Северо-Западное отделение

[1] Некоторые из них ранее посвятили этой проблеме ряд монографий (*Юсупов Р. М.* Наука и национальная безопасность. 2-е изд., перераб. и доп. СПб., 2011. 369 с.; *Кефели И. Ф., Малафеев О. А.* Математические начала глобальной геополитики. СПб.: Изд-во Политехн. ун-та, 2013. 204 с.; Социоинженерные атаки: проблемы анализа / Под общ. ред. Р. М. Юсупова. СПб., 2016. 349 с.) и статей (*Левкин И. М., Левкина С. В., Галкова Е. А.* Угрозы национальной безопасности и их информационно-признаковые модели // Геополитика и безопасность. 2015. № 1(29). С. 88–93; *Колбанёв М. О., Коршунов И. Л., Левкин И. М., Микадзе С. Ю.* К вопросу об информационно-экономической безопасности общества // Геополитика и безопасность. 2015. № 3(31). С. 87–91; *Мезенцев Д. Ф., Забарин А. В.* Психология восприятия «нормы» в политических процессах // Геополитика и безопасность. 2016. № 1(33). С. 46–52; *Ипатов О. С., Кефели И. Ф., Левкин И. М.* Информационная геополитика на службе российского государства // Геополитика и безопасность. 2016. № 2(34). С. 25–34; *Верзун Н. А., Колбанёв М. О., Татарникова Т.* М. Технологическая платформа четвертой промышленной революции // Геополитика и безопасность. 2016. № 2(34). С. 87–95).

Экспертно-консультативного совета по проблемам национальной безопасности при Председателе Государственной Думы РФ провело научно-практический семинар «Информационно-психологические проблемы безопасности личности и общества» [1]. Последователем этого семинара стала секция «Информационно-психологическая безопасность», включенная в работу регулярно проводимой в Санкт-Петербурге конференции «Информационная безопасность регионов России».

Следует особо отметить, что идеи, представленные в данной работе, в значительной мере сформированы и апробированы благодаря активному участию некоторых из ее авторов в Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР)». Конференция регулярно проводится в Санкт-Петербурге, начиная с 1999 г. (по инициативе В. В. Путина, занимавшего тогда пост секретаря Совета Безопасности Российской Федерации), при поддержке Совета Безопасности Российской Федерации, Правительства Санкт-Петербурга и ряда других учредителей.

Мы исходим из понимания опасности как совокупности реальных или потенциальных обстоятельств, при которых материальные, энергетические и информационные факторы нарушают функционирование и само существование, в конечном счете, жизненного мира человека, а не только биосферы и социотехнических систем. В то же время в современном мире одной из ключевых характеристик феномена безопасности является то, что временна́я дистанция между создаваемыми техническими средствами и технологиями, которые порождают опасности различного рода, и средствами, обеспечивающими возможность их упреждения, стремится к нулевой отметке. Так, например, НБИК-технологии (о них речь пойдет в одном из разделов книги) заключают в себе все задатки синхронного создания как систем «глобальной опасности» (новые системы ведения военных операций, «этнических войн», «экологического самоубийства», возможности замены (а не только дополнения) естественного интеллекта искусственным), так и систем «глобальной безопасности» — экологической, продовольственной, военной, национальной, международной. Как справедливо отмечает иностранный член РАН проф. А. А. Акаев, NBIC-технологии определяют основу 6-го технологического уклада, который выступает источником экономического роста на предстоящей длинной волне Кондратьева (2018–2050 гг.). «Именно

[1] Информационно-психологические проблемы безопасности личности и общества. Тезисы докладов научно-практического семинара. Санкт-Петербург, 26–27 ноября 1997 г. СПб., 1997. 42 с.

синергия NBIC-конвергенции, — согласно Акаеву, — будет оказывать мощное воздействие на экономический рост в XXI веке» [2]. Вместе с тем, NBIC-технологии сформировали «новые опасные вызовы для человечества и для геополитического взаимодействия между цивилизациями и государствами» [3].

Решение проблем обеспечения информационно-психологической и когнитивной безопасности базируется на четких представлениях о существе глобального информационного пространства, которое продолжает формироваться в ходе информационной революции как одного из ключевых направлений четвертой промышленной революции и предстает сферой растущего многообразия информационно-психологических и когнитивных процедур, угроз, операций. Прообразом общества, которое мы называем информационным, по сути своей предстает ноосфера, т. е., согласно В. И. Вернадскому, сфера разума, который черпает информацию из внешнего мира и с ее помощью управляет различными процессами, происходящими в информационном обществе. Ныне эта сфера разума, еще недавно казавшаяся сугубо умозрительной идеей-образом, обрела вполне четкие организационные контуры глобального информационного поля. Так, под руководством акад. А. И. Савина была разработана концепция поддержания стратегического равновесия и ракетно-ядерного сдерживания агрессии на основе глобальных информационно-управляющих систем, а также современная оборонная концепция стратегического равновесия в мире. Причем, как утверждал сам Анатолий Иванович, переход на сознание глобального типа дается любому человеку очень трудно. Человек привык мыслить конкретно, но в настоящее время этого недостаточно. Отметим лишь то, что созданные под руководством А. И. Савина космические информационно-управляющие системы (глобальные по охвату территорий и масштабу задач) позволили уже в 1970-х гг. достичь и по настоящее время сохранить военно-стратегический паритет с США и всем блоком НАТО [4].

---

[2] *Лаврова Л. Е.* Аскар Акаев: Человек из будущего. Монологи. М.: Молодая гвардия, 2014. С. 333.

[3] *Яковец Ю. В., Акаев А. А.* Перспективы становления устойчивого многополярного мироустройства на базе партнерства цивилизаций: Научный доклад. М., 2016. С. 68.

[4] http://www.mitropolitfound.ru/index.php? Itemid=35&catid=24:2009–08–18–07–03–12&id=3032: -l-r&option=com_content&view=article; http://www.redstar.ru/index.php/component/k2/item/22864-zhizn-otdannaya-otechestvu; http://idiinvest.narod.ru/new/sev/savin/savin-kosmos.html; http://www.politinform.su/soldaty-imperii/24348-akademik-ran-anatoliy-savin-zhizn-otdannaya-otechestvu.html.

Мотивом, побудившим авторский коллектив обратиться к понятиям жизненного мира и его смыслов (сугубо философского и социологического порядка), послужила необходимость сделать еще один шаг в анализе проблем информационно-психологической безопасности — выделить в качестве относительно самостоятельного предмета исследования когнитивную безопасность. Дело в том, что философия жизни изначально (в конце XIX в.) выдвинула, в качестве одного из основных тезисов, положение о том, что народ становится субъектом исторического процесса. Эта идея получила развитие в социологии жизни, базовыми понятиями которой выступают общественное сознание, охватывающее знание, информацию, потребности, мотивы, ценностные ориентации, установки, интересы и другие эмпирические элементы жизненного мира людей. Сознание становится реальной силой тогда, когда оно воплощается в поведении, деятельности, в действиях людей, превращается в «общественную силу» (К. Маркс). В рамках философско-социологической интерпретации поиск смысла жизни — это основная цель, которая выступает не только в качестве обобщенной ценности, но и ведущим мотивом различных видов деятельности людей.

Сохранение состояния перманентного поиска смысла жизни, в таком случае, как раз и выступает ключевой задачей когнитивной безопасности, поскольку, как справедливо отмечает Ж. Т. Тощенко, выявление сущности жизненного мира связано с определением основных его смыслов, заключенных в социально-экономических, социально-политических и социально-культурных позициях людей в их взаимоотношении с внешним миром и своим осознаваемым внутренним предназначением. Жизненный мир и его смыслы являются потому максимально удобными для использования в управленческой практике на всех уровнях социальной организации обществ, во всех без исключения организациях как экономического и политического, так и социального и духовно-культурного профиля [1].

Следует особо отметить, что проблема когнитивной безопасности только начинает становиться предметом самостоятельного анализа и принятия конструктивных решений. До недавнего времени эта проблема зачастую рассматривалась как некая необходимость предотвращения когнитивных войн. Так, к примеру, С. И. Репко, определяя когнитивную войну как «тайную деятельность Запада в отношении населения зарубежных стран информационными и наркотическими методами

[1] *Тощенко Ж. Т.* Главные смыслы жизненного мира россиянина // Жизненный мир россиян: 25 лет спустя (конец 1980-х – середина 2010-х гг.): Научное издание / Под ред. Ж. Т. Тощенко. М., 2016. С. 34–50.

с целью затруднить понимание информации, замаскировать сведения по геополитике, динамике истории и современной обстановке, скрыть действующих лиц и их цели, фальсифицировать сведения, побудить к неправильной оценке информации», усматривает задачи обеспечения когнитивной безопасности довольно тривиально: «Чтобы понимать прошлое России и современную обстановку, следует прекратить повторять мифы когнитивной войны» [2]. Можно встретить и суждение сугубо эмоционального порядка: «Используя все современные знания и опыт в социальной когнитивной психологии, против нашей страны, нашего культурного пространства, русской культуры, русского языка, всех народов на нашем евразийском пространстве, включая русский народ и его патриотичных представителей за границей, развязана и ведется широкомасштабная когнитивная война. Под атакой находятся не только наш имидж в мире, но и наши души и сердца, наши умы, наше здоровье, наше настроение, наши глубинные мотивации. И значит, пришло время занимать эшелонированную оборону, готовить масштабное контрнаступление и планировать занятие столиц (духовных центров) нападающих. Основная защита и основное оружие в этой войне — в первую очередь познание себя, самостоятельное раскапывание своих духовных корней, вековых ценностей, а также корней тех (если они у них прослеживаются), кто покусился на нашу духовную идентичность, на наши души» [3].

Приведенные выше высказывания позволяют судить о том, что проблемное поле когнитивной безопасности во многом остается пока еще уделом околонаучных призывов и заклинаний. Над умами многих довлеет груз безысходности когнитивной войны, а потому надо бороться с мифами и углубиться в познание самого себя. Напротив, современная наука имеет набор средств, методик и идей, позволяющих конструктивно вести разработки в такой междисциплинарной области, каковой выступает информационно-психологическая и когнитивная безопасность. Дело — за объединением усилий ученых различных областей знания — философии и психологии, социологии и политологии, информатики и медиалогии. Данная работа — пожалуй, одна из первых, объединивших усилия представителей указанных выше областей знания для решения одной из актуальных проблем современности и представляющих становление нового научного направления.

---

[2] *Репко С. И.* Когнитивная война. М., 2013. С. 180, 199.

[3] *Аргенбер В.* Когнитивная война против России. http://www.narodsobor.ru/events/analytics/32089-vyacheslav-argenber-kognitivnaya-vojna-protiv-rossii.

Авторский коллектив распределил свои усилия в написании данной книги следующим образом:

Введение — чл.- кор. РАН, д-р техн. наук, проф. Юсупов Р. М., д-р филос. наук, проф. Кефели И. Ф.

Раздел I: гл. 1 — д-р филос. наук, проф. Вассоевич А. Л.; гл. 2 — д-р полит. наук, проф. Баранов Н. А.; гл. 3 — канд. психол. наук., доц. Забарин А. В.; гл. 4 — д-р полит. наук, проф. Нурышев Г. Н.; гл. 5 — д-р полит. наук, проф. Комлева Н. А.

Раздел II: гл. 1 — д-р филос. наук, проф. Кефели И. Ф.; гл. 2 — д-р техн. наук, проф. Колбанев М. О., канд. техн. наук, доц. Касаткин В. В.; гл. 3 — д-р техн. наук, проф. Ковалев А. П., д-р воен. наук, проф. Левкин И. М.; гл. 4 — чл.- кор. РАН, д-р техн. наук, проф. Юсупов Р. М., д-р техн. наук, проф. Осипов В. Ю.; гл. 5 — д-р техн. наук, проф. Котенко И. В., д-р техн. наук, проф. Саенко И. Б., канд. техн. наук, ст. науч. сотр. Чечулин А. А.

Раздел III: гл. 1 — д-р филос. наук, проф. Кефели И. Ф.; гл. 2 — д-р филос. наук, доц. Плебанек О. В.; гл. 3 — д-р полит. наук, проф. Виноградова С. М., д-р полит. наук, проф. Мельник Г. С., д-р филол. наук, проф. Мисонжников Б. Я.; гл. 4 — канд. психол. наук, доц. Самуйлова И. А.; гл. 5 — канд. техн. наук, доц. Шишкин В. М.

Заключение — чл.- кор. РАН, д-р техн. наук, проф. Юсупов Р. М., д-р филос. наук, проф. Кефели И. Ф.

Р. М. Юсупов
И. Ф. Кефели

Раздел I.
Информационно-психологическая безопасность: исторические предпосылки и социально-политические реалии

Глава 1. Информационно-психологические войны: исторические реминисценции

Психологическую войну следует рассматривать как разновидность войны информационной, поскольку энергоинформационные природного происхождения и искусственно создаваемые информационные потоки оказывают влияние на психическое состояние человека, которое воплощается в его мыслях, поступках, поведении. Подобно тому, как человек ориентируется в окружающем его пространстве, он самоопределяется и в своем внутреннем мире, в мире психических явлений. Но этот внутренний мир часто видоизменяется под воздействием внешних информационных факторов. И если мы ставим перед собою цель принципиально изменить внутреннее содержание человека, мы начинаем оказывать на него интенсивное информационное воздействие, то есть встаем на путь информационной войны.

Приемы информационно-психологического воздействия в исторической практике. Всякое знание — сила, но знание о противнике — сила вдвойне. Эта нехитрая истина стала понятна человечеству со времен глубочайшей древности. Но не только секретные донесения разведчиков с территорий потенциальных противников и итоговые сводки, составленные на их основе, дошли до нас на клинописных табличках. Для предыстории информационных войн особый интерес представляет изобретение «дезинформационных» глиняных конвертов, внутри которых запрятывали табличку с достоверной информацией. Текст же, начертанный на «дезинформационном» конверте, должен был либо успокоить, либо ввести в заблуждение непосвященных. Получатель же, разбив

конверт, становился обладателем нужной информации. Не подлежит сомнению, что в старовавилонский период это хитроумное изобретение было хорошо известно.

Известно, сколь немаловажную роль в гибели Юлия Цезаря, упразднявшего республиканский строй в Риме, сыграли его честные, но жесткие высказывания о римской республике: Nihilesserespublicam, appella tionemsinecorporeacspecie — «Республика — ничто, наименование без тела и облика» (Suetonius. Devitaduodecim Caesarum, 1,77). Еще большее раздражение вызывало то обстоятельство, что среди ближайшего окружения Цезаря уже находились охотники именовать его Rex — «Царь». А ведь все это совершалось в ту пору, когда республиканские традиции в Риме были еще сильны. Естественно, что против диктатора, столь смело обнажавшего свои истинные намерения, был составлен заговор, кончившийся его убийством.

Август, без сомнения, извлек урок из гибели своего предшественника. Его режим, вошедший в историю под названием принципата, уже в полной мере использовал всю мощь политического лицемерия. Осуществленный тогда выброс **дезориентирующей информации** [1] позволил Августу управлять политической ситуацией. При Августе официальной формулой режима становится respublicarestituta — «восстановленная республика». Подобно тому, как в памятные нам дни горбачевской перестройки известная формула «Больше демократии — больше социализма» маскировала планы уничтожения социалистической системы, respublica restituta прикрывала рождение Римской империи. Иными словами, взяв на вооружение приемлемую для римского общества политическую фразеологию, Август смог добиться того, к чему Цезарь стремился, но чего так и не смог достичь, обнажая свои истинные цели [2].

Дискредитирующей информации часто принадлежит важное значение в деле формирования образа врага, а следовательно, и в процессе сплочения любого этноса в соответствии с принципом «*против кого дружим?*». Ведь с психолого-политической точки зрения «этнос — это любое объединение людей, которые осознают свою общность, то есть могут

---

[1] А. И. Юрьев предлагает понимать под **дезориентирующей информацией** — информацию «неправильно определяющую собственное местонахождение в историческом процессе, экономическом состоянии, отношениях с иными народами и государствами». См.: *Юрьев А. И.* Введение в политическую психологию. СПб.: Алетейя, 1992. С. 107.

[2] *Вассоевич А. Л.* Духовный мир народов классического Востока (Историко-психологический метод в историко-философском исследовании). СПб.: Алетейя, 1998. С. 73.

сказать о себе “МЫ”», справедливо замечал А. М. Зимичев и добавляет: «Для того чтобы этнос мог существовать, он должен быть противопоставлен окружающему миру, т. е. “НЕ-МЫ”. Иначе говоря, этнос всегда существует там, где есть разделение на “МЫ” и “НЕ-МЫ”» [1]. Учитывая основополагающее значение **веры** в таких противопоставлениях, необходимо признать, что талмудические законоучители, дискредитируя чуждые им религии, способствовали сплочению еврейских общин в непростых условиях рассеяния.

Следует особо подчеркнуть, что, наряду с дискредитирующей информацией, важнейшую функцию могут выполнять также **ложные сообщения**, *«которые вводят общественное мнение в заблуждение под видом истинных»* [2]. Именно они в классификационной схеме А. И. Юрьева именуются **дезинформацией**. Естественно, что общественное мнение в целом складывается из мнений отдельных лиц, а потому жертвами дезинформационных стратегий часто оказываются и малые группы, и конкретные личности (в первую очередь, принимающие ответственные решения).

История войн дает нам великое множество примеров, когда посредством дезинформации противника о своих планах полководцам удавалось реализовать свои истинные цели. Примечательно, что в нашей стране грозное дезинформационное оружие было использовано еще Петром I для прорыва к берегам Балтийского моря. В российских верхах прорыв планировался на осень 1702 г. При этом великий государь не только осуществил дерзкий замысел — проложить в безлюдных северных дебрях «Осудареву дорогу» — путь для перехода войск и переволоки двух боевых кораблей из одного морского бассейна в другой, но и дезинформировал шведов о своих истинных целях. Как пишет П. А. Кротов, «исследователи прежде не замечали информации, содержащейся в донесении австрийского дипломата в Москве О. А. Плеера», которое он отправил в Вену 15 апреля 1702 г. «За несколько дней до отъезда Петра I из столицы к Архангельску дипломат сообщал своему правительству, что на севере России готовятся встретить царя, который якобы намерен в течение лета предаваться забавам на берегах Белого моря» [3]. Тем не менее, О. А. Плееру удалось раздобыть и достоверные сведения о тайных планах русского

[1] *Зимичев А. М.* Психология политической борьбы. СПб.: Техническая книга, 1993. С. 55.

[2] *Юрьев А. И.* Введение в политическую психологию. СПб.: Алетейя, 1992. С. 108.

[3] *Кротов П. А.* Осударева дорога 1702 г. // Русский Север и Западная Европа. СПб.: Рус.-Балт. информ. центр БЛИЦ, 1999. С. 179–181.

царя, сознательно возвещавшего Европе о своем намерении, увеселяясь в Архангельске, поджидать возможного подхода шведской эскадры, чтобы дать ей отпор. Весьма осведомленный австрийский дипломат, меж тем, доносил своему правительству следующее: «…мне доверительно сказали, что это лишь предлог, а истинный замысел состоит в том, чтобы вновь пойти на Нарву, хотя некоторые убеждали царя идти к Ниеншанцу».

Сейчас уже сложно понять, не был ли упомянутый О. А. Плеером замысел Петра I «вновь пойти на Нарву» более глубоким дезинформационным слоем, призванным защитить тот главный стратегический замысел, благодаря осуществлению которого мы имеем сейчас возможность праздновать 300-летие основания Санкт-Петербурга. Примечательно, что в далеком 1702 г. даже проницательный австрийский дипломат придерживался мнения о предпочтительности для русского государя похода к Нарве и рассуждал следующим образом: «…когда он будет находиться в Архангельске, неприятель станет уверенно считать, что он там развлекается, а он, между тем, вознамерился быстро пройти через Архангельск на Новгород и Псков и затем продолжить поход к Нарве. А Шереметев, тем временем, должен с сильной армией наблюдать за врагом в поле, дабы (тот) не смог оказать помощи городу (Нарве)».

Замечательный знаток истории XVIII века П. А. Кротов, детально анализировавший эти исторические свидетельства, полагает, что России, оправившейся от ноябрьского поражения 1700 года под Нарвой, требовалось взять реванш именно на месте шведского триумфа двухлетней давности. Великий государь в таком случае оказывается едва ли не первооткрывателем той информационной технологии, которая должна быть положена в основу учения о глубинных дезинформационных слоях, призванных защитить главный стратегический замысел [4].

Другой, более известный пример удачного использования дезинформационных технологий для дезориентации противника связан с экспедицией Наполеона Бонапарта в Египет. Весной 1798 года вся Европа, конечно же, знала, что Франция готовит какую-то морскую экспедицию. Англичане же сверх того с особым вниманием следили за тем, как во всех южнофранцузских портах идет кипучая работа, как туда прибывают

---

[4] В. Б. Резун (Суворов), говоря о временах своего ученичества в системе ГРУ, вспоминает «матерого полковника», который повторял: «…нельзя верить тому, что демонстрируют… надо искать то, что от нас скрывают… Найдете то, что скрывают, — не радуйтесь. Это может оказаться вторым каскадом закрытия. Помните: хороший секрет закрывают в два каскада. Или в три». См.: *Суворов В.* Самоубийство: Зачем Гитлер напал на Советский Союз? М.: Изд-во АСТ, 2002. С. 11.

войска. Тайной не было и то, что главнокомандующим 5 марта 1798 г. назначили генерала Бонапарта. И это назначение указывало на всю важность предстоящего дела.

Разумеется, эскадра адмирала Нельсона была готова расстрелять и потопить все французские суда. И именно поэтому Наполеон искусно распространил слух, будто бы он намерен пройти через Гибралтар, обогнуть Испанию и затем совершить высадку в самом неприятном для англичан месте, в Ирландии. Дезинформация (или «информация для нас») Нельсоном была воспринята, и его эскадра стала поджидать Наполеона у Гибралтара. Французский же флот, выйдя из гавани, пошел прямо на Восток к Мальте, к острову, принадлежавшему еще с XVI века Мальтийскому ордену. Подойдя к острову, Бонапарт потребовал и добился его сдачи, объявил владением Французской республики и отбыл в Египет.

Половинчатость и непоследовательность принимаемых решений в информационной войне еще более опасна, чем непоследовательность и половинчатость командирских решений в ходе обычных военных действий. Это, кстати сказать, очень хорошо осознали политики, претендовавшие на мировое господство в следующем столетии. Они то уж очень хорошо понимали всю гибельность «половинчатости». Действительно, лишь XX век дал миру политиков беспредельно раскрепощенных, показавших, что для них не существует психологических барьеров в деле информационной войны.

«*Во время войны пропаганда должна быть средством к цели, цель же,* — по мнению Гитлера, состоит — *в борьбе за существование немецкого народа*». Анализируя неудачный опыт немецкой пропаганды 1914–1918 гг., будущий вождь Третьего рейха, заключенный с 1 апреля 1924 г. в крепость Ландсберг, возвышался до следующих обобщений: «На деле пропаганда есть средство и потому должна рассматриваться не иначе как с точки зрения цели. Вот почему форма пропаганды должна вытекать из цели, ей служить, ею определяться. Ясно также, что в зависимости от общих потребностей цель может изменяться и соответственно должна изменяться также и пропаганда» [1].

Принцип **необходимого видоизменения целей** в зависимости от меняющейся социально-политической конъюнктуры осознавался и политическими лидерами большевизма. Вспомним, как В. И. Ленин отказался от лозунга «Вся власть Советам!» после того, как реальное руководство советами перешло в руки меньшевиков. Вспомним, как в начале

---

[1] *Гитлер А.* Моя борьба. М.: Витязь, 2000. С. 148, 149.

Великой Отечественной войны И. В. Сталин приостановил официальный советский атеизм, ставший для СССР теперь просто опасным. Ведь в оккупированные районы страны вместе с немецкими войсками вступали и духовные миссии, вновь открывавшие поруганные большевиками православные церкви. Разумеется, германские оккупационные власти возвращали храмы верующим отнюдь не из православного благочестия. Для них эта акция также была важным элементом спецпропаганды среди войск и населения противника.

«Всякая пропаганда должна быть доступной для массы, — писал Гитлер, — ее уровень должен исходить из меры понимания, свойственной самым отсталым индивидуумам из числа тех, на кого она хочет воздействовать. Чем к большему количеству людей обращается пропаганда, тем элементарнее должен быть ее идейный уровень. А раз дело идет о пропаганде во время войны, в которую втянут буквально весь народ, то ясно, что пропаганда должна быть максимально проста. Чем меньше так называемого научного балласта в нашей пропаганде, чем больше обращается она исключительно к чувству толпы, тем больше будет успех. А только успехом и можно в данном случае измерять правильность или неправильность данной постановки пропаганды» [2].

Опора на **симплицизм мышления широких народных масс** была провозглашена Гитлером в самом начале своей политической карьеры. Но этим принципом он руководствовался и впоследствии, когда сосредоточил в своих руках всю полноту государственной власти. Весьма показательной в этом отношении является историческая речь фюрера от 22 июня 1941 г., в которой он возлагал всю меру ответственности за развязывание войны против СССР не только на Москву, которая «*нарушила условия нашего дружественного договора*» и «*позорнейшим образом изменила*», но и на «иудейско-английских поджигателей войны». При этом уверялось, что «германский народ никогда не питал враждебных чувств к народам, населявшим Россию. Но еврейско-большевистские владыки Москвы в течение двух десятилетий старались зажечь пожар не только в Германии, но и во всей Европе».Особые разделы в этой речи были посвящены британской политике окружения и советским приготовлениям на восточной границе. Гитлер, ссылаясь на слова американского генерала Вуда, утверждал, что Черчилль уже в 1936 г. заявил в комиссии Конгресса: «*Германия становится слишком могущественной и потому*

[2] *Там же.* С. 150.

должна быть уничтожена» [1]. Эмоциональной доминантой выступления становилась идея: с лета 1939 г. Англия сочла момент подходящим для возобновления политики окружения Германии и при этом преследовала одну цель — ее уничтожить. «Начатая кампания лжи, — говорил Гитлер, — стремилась убедить другие народы, что им грозит опасность», и тем самым побуждала эти народы поверить английским гарантиям с тем, чтобы впоследствии «заставить их участвовать в мировой войне против Германии». Таким образом, немецкий народ обретал возможность уверовать в то, что ответственность за неизбежно кровопролитную войну с Советским Союзом ложится на кого угодно, но только не на Германию.

Однако в хорошо продуманной речи от 22 июня 1941 г. даже британские козни меркнут в сравнении с «вероломными» советскими приготовлениями на восточной границе: «броневые соединения и отряды парашютистов все более приближались к германской границе. Германская армия и германская родина знают, что еще несколько месяцев тому назад на нашей восточной границе не было ни одной боевой или моторизованной дивизии…» И все это приуготовляло к принятию самого главного: «Германский народ! В этот момент происходит наступление наших войск, равного которому по размерам еще не видел мир».

Совершенно очевидно, что **методикам дегероизации** наиболее значимых событий исторического прошлого принадлежит весьма значимая роль в условиях ведения информационной войны, ибо успешное применение этих методик существенно облегчает стимулирование идеологического кризиса. По справедливому мнению В. П. Бранского и С. Д. Пожарского, «конечным итогом развития идеологического кризиса является достижение состояния **идеологического вакуума**. Здесь наблюдается **равенство сил** между идеалами и антиидеалами, в результате чего ни один из них не может быть реализован, все мероприятия взаимно блокируются и общество оказывается парализованным» [2].

Методика достижения равенства между антиидеалом и идеалом принадлежит к числу наиболее действенных средств стимуляции идеологического кризиса как внутри малой группы, так и внутри гигантского государственного образования. Подобно компьютерному вирусу, **равенство нейтрализующих друг друга идеалов** нарушает функционирование

---

[1] *Гитлер А.* Речь от 22 июня 1941 года // Волшебная гора. II. М.: Пилигрим, 1994. С. 133, 136, 140.

[2] *Бранский В. П., Пожарский С. Д.* Социальная синергетика и акмеология. Теория самоорганизации индивидуума и социума в свете концепции синергетического историзма. Изд. 2-е, испр. и доп. СПб.: Политехника, 2002. С. 105.

любой идеологической системы. Именно поэтому широкому тиражированию книг В. Б. Резуна (Суворова), разрушавших **доминирующий социальный идеал** советского общества, было придано столь важное значение.

Естественно, возникает вопрос, существовала ли информационная технология, способная нейтрализовать интеллектуальную экспансию разведчика-перебежчика. Такая методика существовала, но сводилась она отнюдь не к запоздалому уличению В. Б. Резуна в различного рода исторических неточностях и фактических ошибках. Автор «Ледокола» легко мог быть «задушен в объятиях» альтернативного антиидеала, но на исходе XX века в России не существовало **идеологического спецназа**, который был бы в состоянии справиться с подобного рода задачей. «Ледокольная» информационная конструкция В. Б. Резуна, дробившая на исходе XX столетия доминирующий социальный идеал советского народа, в новых исторических условиях XXI века может оказаться незыблемым фундаментом для становления **идеологии неосталинизма**. В изменившемся геополитическом контексте, когда величайшая прежде держава утратила одну пятую своей территории при полном бездействии высшего военного руководства, не защитившего национальные интересы страны, «суворовская» мысль о том, что Сталин в 1937–38 гг. совершенно правильно уничтожал командный состав Рабоче-Крестьянской Красной армии, кажется вполне убедительной. А значит, «злонамеренной хрущевской клеветой» становятся любые утверждения о необоснованности тогдашних репрессий в армии, о пресловутых «сталинских ошибках». Более того, уязвленное чувство национальной гордости «дорогих россиян» (связанное со все большей зависимостью внешней и внутренней политики РФ от США и ЕС) будет провоцировать у тысяч людей восхищение завораживающими «суворовскими» рассказами о том, как И. В. Сталин в «День М» собирался захватить всю Западную Европу.

Из всего сказанного о книгах В. Б. Резуна следует и куда более общий вывод о том, что возникновение нового информационного контекста с неизбежностью влечет за собой изменение психологических качеств исходной информации. Это изменение может оказаться столь радикальным, что конкретная информационная конструкция приобретет психологические качества, прямо противоположные изначальным.

А. И. Юрьев во «Введении в политическую психологию» четко противопоставляет (I) «объективности информации» «фальсифицирующую информацию», (II) «системности информации» «дезориентирующую информацию», (III) «организованности информации»

«деморализующую информацию», (IV) «достаточности информации» «дестабилизирующую информацию», (V) «ясности информации» «дезинформацию», (VI) «конкретности информации» «дезорганизующую информацию», (VII) «практичности информации» «дискредитирующую информацию», (VIII) «необходимости информации» «дезинтегрирующую информацию» [1]. Принимая такую классификацию, следовало бы сказать, что принадлежность к любому из перечисленных видов информации определяется более широким информационным контекстом, а стало быть, при его изменении (с субъективной точки зрения) «объективная информация» может превратиться в «фальсифицирующую информацию», «системная информация» в «дезориентирующую информацию» и так далее. Именно поэтому едва ли не самым действенным оружием информационной войны следует признать **метод изменения общего информационного контекста**, когда в свою противоположность начинают обращаться все создававшиеся прежде микро- и макроинформационные конструкции.

Разумеется, в одночасье изменить весь информационный контекст, хотя бы в рамках отдельно взятой страны, — задача исключительной сложности. Для этого требуются впечатляющие силовые акции, которые заставляли бы говорить о себе всех и в то же время **девальвировали** бы **представления**, формировавшиеся под воздействием прежних микро- и макроинформационных конструкций. Понятие микро- и макроинформационной конструкции было впервые введено в научный обиход Д. Ф. Мезенцевым, заложившим основы для создания **теории информационных фантомов** в рамках современной политической психологии [2]. По его мнению, системный анализ лавинообразных потоков всевозможных сведений об окружающем мире, который уже давно наблюдается в человеческих сообществах, невозможен без четкого различения микро- и макроинформационных конструкций. Ведь любые частные сообщения, будь то в печатных или электронных СМИ, неизбежно выстраиваются в гигантскую, порой общенациональную, а иногда даже транснациональную макроинформационную конструкцию [3].

---

[1] *Юрьев А. И.* Введение в политическую психологию. — СПб.: Алетейя, 1992. С. 110–111.

[2] *Мезенцев Д.* Ф. Психологическое воздействие информационных фантомов // Вестник полит. психологии. 2002. № 1. С. 28–31.

[3] *Мезенцев Д. Ф.* Психология влияния средств массовой информации на формирование политических установок личности: автореф. дисс. ….канд. психол. наук. СПб., 1998. С. 18.

Примечательно, что исторической основой для мезенцевских теоретических построений послужили события весны 1958 г. во Франции. Те события, которые в своем конечном итоге не только привели к падению режима Четвертой республики, но и к передаче власти генералу Шарлю де Голлю. Как известно, до момента весеннего кризиса Шарль де Голль находился «не у дел», но его час пробил, когда в правых кругах французского общества возникла глубокая убежденность в неэффективности тогдашней многопартийной системы. Существовавший республиканский строй, как тогда многим казалось, не способен защитить государственное величие Франции. Еще более радикальные настроения стали характерны для той части правых кругов, которая была тесно связана с армией. В связи с тяжелой и затяжной войной в Алжире настроения эти лишь крепли. Так формировалась политическая установка на ликвидацию Четвертой республики с тем, чтобы утвердить в стране режим авторитарной власти, свободной как от влияния политических партий, так и от «мелочного контроля» со стороны Парламента и общества.

В ту пору для правых сил единственно приемлемым носителем «авторитарного начала» и своеобразным «национальным арбитром» мог быть лишь генерал Шарль де Голль. К тому же, он был известен в народе как герой французского сопротивления. Однако, несмотря на некоторую внутреннюю напряженность во французском обществе, которую порождала не слишком удачная колониальная война в Алжире, в стране не было глубокого политического кризиса. Подавляющее большинство граждан поддерживало режим Четвертой республики. А это означало, что попытка осуществить смену режима путем открытого переворота оказалась бы для ее инициаторов опасной авантюрой с непредсказуемыми последствиями. Ведь полной готовности к смене политического режима силовым путем не было даже в рядах вооруженных сил.

Осознавая всю сложность политической ситуации, сторонники генерала де Голля встали на путь информационно-психологической войны с тогдашним республиканским строем. Началом этой войны можно считать 13 мая 1958 г., когда был инсценирован путч колониальной армии Алжира против правительства метрополии. Главная задача тех, кто осуществлял эту инсценировку, конечно же, заключалась в том, чтобы породить во французском обществе повсеместное ощущение угрозы — угрозы, связанной с начинающейся гражданской войной. Тем самым взрывался весь прежний **информационный контекст** и в свою противоположность обращались микро- и макроинформационные конструкции недавнего прошлого.

Г. М. Ратиани, бывший непосредственным свидетелем падения Четвертой республики во Франции, писал следующее: «Парижане, проснувшись 16 мая, сразу увидели, что город за одну ночь изменил свой облик: на улицах и площадях военные грузовики и военные патрули, часовые у государственных учреждений, усиленная внешняя и внутренняя охрана Бурбонского дворца. Этот военный облик Париж будет сохранять две недели. Еще ночью Пфлимлен объявил по радио, что правительство подготовило проект закона о чрезвычайном положении на территории Франции… Мобилизация полиции, жандармерии, войск СРС, которые фактически оккупировали весь Париж и другие промышленные центры, использовались, главным образом, как мера психологического давления на население. С утра до вечера в Париже можно было наблюдать загадочные маневры длинных колонн военных грузовиков с левого берега на правый, с площади Республики к Елисейским полям, из Булонского леса в Венсен. Никто не мог объяснить, почему войска СРС утром разбивали свой лагерь на Марсовом поле, а во второй половине дня вытаптывали траву на аллее между мостами Александра III и Альма. Все это казалось непонятным и бессмысленным, но создавало давящую, тревожную обстановку, и по Парижу среди обывателей поползли всевозможные слухи и самые невероятные предположения» [1].

В многочисленных исторических исследованиях, посвященных падению Четвертой республики, в том числе и в замечательной книге Г. М. Ратиани, убедительно доказано, что в мае 1958 года была осуществлена лишь **имитация путча** с целью «шантажа» французского общества. У алжирских заговорщиков, естественно, не было реальных сил организовать бросок на Париж и даже среди высшего военного командования в метрополии отнюдь не все сочувствовали их планам. Таким образом, «алжирский путч» и иные, сопутствующие ему политические события во многом носили фарсовый характер. «Однако он, — как замечает Д. Ф. Мезенцев, — был использован правыми политическими кругами, и что особенно важно, подавляющей частью французской печати, связанной, в основном, с правыми, для создания и стремительного внедрения в умы миллионов французов грандиозного **информационного фантома** — представления о том, что Франция глубоко расколота, стоит на пороге гражданской войны, и лишь приход к власти “национального арбитра”, стоящего “над партиями” и их политическими страстями генерала де Голля, может еще

[1] *Ратиани Г. М.* Франция: судьба двух республик. М.: Мысль Язык: Русский Формат, 1980. С. 346–359.

спасти страну» [2]. Здесь уместно напомнить, что под информационным фантомом, сокращенно ИНФА (от латинского informatio«*представление*» + греческого φάντασμα «*призрак*», т. е. «*представление-призрак*»), мы вслед за Д. Ф. Мезенцевым понимаем совокупность достоверной, недостоверной и/или заведомо неполной информации, используемой как инструмент формирования требуемых социальных и политических установок [3].

Но вернемся во Францию 1958 г., где дни 28 и 29 мая стали апогеем политико-психологического кризиса. В ответ на угрозу военного переворота, с которой открыто выступили сторонники смены режима, левые силы организовали грандиозную манифестацию в поддержку республики. В ней приняли участие, по меньшей мере, 200 тысяч человек. В ночь на 30 мая в Париже уже ожидали начала высадки отрядов алжирских парашютистов. Тогда же глава государства, вслед за отставкой законного правительства, поставил национальному собранию по существу политический ультиматум — либо призвание де Голля и наделение его чрезвычайными полномочиями, либо его собственный уход накануне военного переворота. Получалось, что республика может оказаться одновременно и без правительства, и без президента, а Национальное Собрание будет прямо противопоставлено французской армии и стоящей за ней «патриотической общественности». Именно такими методами сильнейшего психологического давления в 1958 году приводили к власти генерала де Голля.

Воздействие ИНФА и информационных фантомных конструкций на сознание широких народных масс поистине огромно. Об этом безжалостно свидетельствует не только новейшая политическая история стран Западной Европы, но и события последних месяцев существования СССР. Возможно, если бы советских людей получше учили истории в средней школе, а главное, если бы нашему народу в меньшей степени было свойственно историческое беспамятство, то примитивное повторение парижских наработок весны 1958 через 33 года в Москве не было бы возможно. Однако история не терпит сослагательного наклонения.

Ни для кого не секрет, что к лету 1991 г. основная масса населения Советского Союза испытывала глубочайшее разочарование в горбачевской политике «перестройки». Сам же Генеральный секретарь ЦК

---

[2] *Мезенцев Д. Ф.* Психология влияния средств массовой информации на формирование политических установок личности: автореф. дисс. ….канд. психол. наук. СПб., 1998. С. 26.

[3] *Мезенцев Д. Ф.* Психологическое воздействие информационных фантомов // Вестник полит. психологии. 2002. № 1. С. 29.

КПСС стал фигурой исключительно непопулярной как среди рядовых граждан, так и среди членов возглавляемой им партии. В рядах высшего партийного руководства уже назревали настроения, отчасти напоминающие те, что предшествовали октябрьскому Пленуму ЦК КПСС 1964 г., после которого Н. С. Хрущев был освобожден от всех занимаемых должностей. «Можно себе представить, какой и впрямь произошел бы в стране переворот, когда бы президент СССР был бы выведен из все еще правящей и многомиллионной партии, имевшей в своем пользовании огромное число техники, строений, издательств, типографий, на счетах которой лежали миллиарды рублей! — писал В. Хатюшин. — Такой переворот мог произойти в любую минуту, и допустить его демократы не имели права» [1].

В сложившейся ситуации (весьма неблагоприятной как для демократических сил, так и лично для М. С. Горбачева) возникли иллюзии, что самым простым выходом будет **упреждающая силовая акция**, призванная взорвать весь «информационный контекст» перестроечной действительности. Тем самым антигорбачевские силы будут полностью дискредитированы, а Президент СССР вновь обретет к тому времени утраченное народное сочувствие.

Министр иностранных дел СССР Э. А. Шеварнадзе был едва ли не первым, кто начал создавать фантомную, пока что микроинформационную, конструкцию о готовящемся «путче». Исходная идея в среде творческой интеллигенции была сразу же воспринята кинорежиссером С. О. Снежкиным, который смог получить необходимый материальный ресурс для съемки широко известного кинофильма «Невозвращенец». Фильм был отснят как раз к августовским событиям, когда произошло создание ГКЧП — Государственного комитета по чрезвычайному положению, в столицу двинулась бронетехника, а телевидение по всем каналам начало транслировать «Лебединое озеро». При этом в кратких официальных информационных передачах утверждалось, что Горбачев заболел, в то время как демократические силы через подконтрольные им СМИ доносили до народа «правду» о том, что президент СССР полностью блокирован путчистами в Форосе.

Весьма показательно и бессмысленное трехдневное стояние в центре Москвы танков и БТР (как свидетель, побывавший 21 августа 1991 г. в столице, не могу не поделиться своим тогдашним изумлением: бронетехники в Москву нагнали столько, словно готовились к сражению под Курской

---

[1] *Хатюшин В.* Переворот по плану «икс» // Глашатай. № 1.Февраль 1992. С. 2.

дугой). В действительности же она была едва ли не главным оружием психологической войны. Тем оружием, с помощью которого не только взрывался весь «информационный контекст» давно зашедшей в тупик горбачевской перестройки, но и унижалась, оскорблялась, дискредитировалась армия. Ведь в августовской информационной войне Советской Армии также была уготована участь жертвы. Согласно сценарию, ей отводилась роль «главной исполнительницы» «военного переворота», но чтобы вызвать у населения сильнейший всплеск негативных антиармейских эмоций, требовались, помимо прочего, еще и жертвы среди мирных, невооруженных граждан. Исключительно важно, что и «консервативный генералитет» Министерства обороны СССР, и нижестоящие командиры сделали все, чтобы не допустить бóльших человеческих жертв. Армия изо всех сил стремилась не поддаваться на провокацию тех, кто организовывал не мифический, а реальный заговор против государства и его вооруженных сил. Но высшие военные руководители в скорости все равно были смещены.

Весьма примечательно и то, что за три дня молчаливо-бездеятельного «путча» от имени Коммунистической партии Советского Союза в поддержку «путчистов» не последовало никаких заявлений. И Политбюро, и Центральный Комитет КПСС устранились от какой бы то ни было оценки происходящего. Подобным же образом отреагировало и политическое руководство Коммунистической партии Российской Федерации. Однако позиция демонстративного устранения от всего происходящего уже не могла спасти некогда «руководящую и направляющую силу советского общества». Ведь с 20 августа в сознание миллионов людей уже внедрялась будто бы народная «расшифровка» аббревиатуры ГКЧП — «Гады коммунисты, что придумали!».

На этом слогане имеет смысл остановиться подробнее, ибо он, действительно, представляет собой одну из лучших находок августовской информационно-психологической войны, подготовившей крушение СССР. По сути дела, перед нами воплощенная в слове **фигура Рубина,** широко известная всем психологам. Подобно тому, как на примечательной картинке из учебника психологии одни видят два женских профиля с развевающимися волосами, а другие — хрустальную рюмочку на черном фоне, слоган «Гады коммунисты, что придумали» сразу же давал возможность двоякого понимания. Для большинства «гадами коммунистами» становились члены ГКЧП, а для меньшинства — «форосская жертва» — генеральный секретарь ЦК КПСС М. С. Горбачев. Его участь, согласно доктрине Бетти Глэд о президентах-двойниках, сменяющих друг друга, чтобы довести до конца великое политическое предприятие,

естественно была предрешена уже в августе. Тем самым, слоган содействовал решению как первичной, так и вторичной задачи информационно-психологической войны.

Трагические события 11 сентября 2001 г. в США (по прошествии всего лишь одного года) приобретают облик тем более чудовищного злодеяния, что они были сознательно использованы для взрыва **мирового информационного контекста** с целью решения глобальных геополитических проблем. Без такого информационного взрыва чудовищной силы, приведшего к созданию фантомной макроинформационной конструкции планетарного масштаба, Соединенные Штаты не смогли бы объявить зоной своих жизненных интересов территорию исторической России или, пользуясь демократической фразеологией, «бывшего СССР». Американское военное присутствие в странах Центральной Азии, входящих в состав СНГ, в Афганистане и в Грузии просто не было бы возможным. Очевидно, что для психолого-политического закрепления достигнутого успеха в ближайшее время будет применена методика объективизации всего произошедшего.

Методика объективизации относится к числу весьма действенных информационных технологий Происходящие события или некий политический процесс объявляются не следствиями «субъективного фактора», то есть результатом волевых усилий конкретных заговорщических групп, политических партий, транснациональных корпораций или межгосударственных объединений, но воплощением естественного хода мирового развития, а стало быть, фатальной исторической неизбежностью. Применительно к геополитической ситуации, предшествовавшей избранию Д. Трампа на пост президента США, целесообразно было вспомнить господина Хантингтона с его войной цивилизаций, особо подчеркивая то обстоятельство, что сейчас отживающие агрессивные цивилизации прошлого атакуют современное человечество, вступающее в эпоху глобализма. Естественно, что «Глобализация — это объективный процесс», который «невозможно остановить». Конечно же, те, кто не утратил исторической памяти, могут возразить, что и «социализм победил в нашей стране полностью и окончательно», что «нынешнее поколение советских людей будет жить при коммунизме», аж в 1980 г., что «альтернативы перестройке нет». Во всех перечисленных политических лозунгах методика объективизации нашла свое достойное применение. Коль скоро событие или процесс начинает восприниматься населением как нечто неизбежное и неотвратимое, оно утрачивает интерес к сопротивлению. Однако методика объективизации может стать грозным информационным оружием также и в руках противников однополярного мира. Достаточно начать широкомасштабное внедрение

идеологем, которые провозглашали бы невозможность формирования «этноса» единого человечества. Ведь, как утверждают экологи, мир богат своим разнообразием. Попытки его силовой унификации противоречат объективно существующим законам бытия. К тому же в научной литературе убедительно доказано, что со времен, когда четвертый по счету правитель династии Аккада Нарам-Суэн (предположительно 2236–2220 гг. до н. э.) принял величание lugalan-ub-limmú-ba — «царь четырех сторон света», все попытки управлять миром из единого центра заканчивались провалом [1].

Тем не менее, борьба за формирование однополярного мира активизировала в ходе развертывавшихся информационно-психологических войн применение грозного этнического оружия. В годы «перестройки» разрушение Советского Союза осуществлялось прежде всего за счет провоцирования межэтнических конфликтов. Не случайно, что именно в 1992 г. А. М. Зимичев [2] упростил сложное гумилевское «уравнение», связанное с процессами этногенеза, и провозгласил: «этнос — это любое объединение людей, которые сознают свою общность, то есть могут сказать о себе "МЫ"… Для того чтобы этнос мог существовать, он должен быть противопоставлен окружающему миру, то есть "НЕ МЫ". Иначе говоря, этнос всегда существует там, где есть разделение на "МЫ" и "НЕ МЫ"» [3]. Следуя логике этого замечательного определения, такой суперэтнос, как советский народ, мог успешно формироваться лишь в условиях крайнего противопоставления окружающему миру. Взять хотя бы известные в СССР даже школьникам фразеологизмы: «молодая Советская Республика в кольце фронтов» или же «героическая борьба Советского народа против агрессии гитлеровской Германии и союзных ей стран Европы».

Трагические события, произошедшие в последние годы, как на Ближнем Востоке, так и на территории братской Украины, подтвердили правоту научных построений Зимичева. К примеру, как только победивший в ходе «революции достоинства» «Евромайдан» начал наступление на русский язык, население Крыма тотчас почувствовало, что его атакует враждебное «НЕ МЫ». И в считанные дни жители Севастополя и всего полуострова ощутили себя новым рождающимся этносом «МЫ — КРЫМЧАНЕ». Другое дело, что формирующаяся крымская контрэлита, противостоящая

---

[1] *Вассоевич А. Л.* Психологические основания контрглобализации // Вестник политической психологии. 2002. № 2. С. 3–4.

[2] Доктор психологических наук, профессор Анатолий Михайлович Зимичев — выдающийся отечественный ученый, создатель оригинальной психолого-политической теории этногенеза, ушел из жизни 22 июня 2016 года на 79-м г. жизни.

[3] *Зимичев А. М.* Психология политической борьбы. СПб.: САНТА, 1993.

нелегитимным киевским властям, оказалась достаточно дальновидна, чтобы понять: без России Крыму не выжить. И новый этнос по имени «МЫ — КРЫМЧАНЕ» влился в состав русского суперэтноса.

Еще в 2000 г. на научно-практической конференции «Российские элиты на рубеже веков» мною была предложена модификация известной зимичевской схемы из книги «Психология политической борьбы». В докладе, в частности, говорилось: «Отталкиваясь от схемы Зимичева, когда этнос изображается в виде овала, в который вписано местоимение 1-го лица множественного числа "МЫ", и овал этот противопоставляется окружающему миру, обозначенному словами "НЕ МЫ", для лиц, склонных к конкретно-образному мышлению, можно предложить новый наглядный образ. Этот образ — изображение живой клетки, находящейся в межклеточном веществе. При всем разнообразии по размерам, форме и функциям все клетки имеют общие черты строения. И подобно тому, как основные части любой клетки — *цитоплазма* и *ядро*, любой этнос включает в себя, помимо основной массы, его составляющей, еще и элиту этноса (его ядро). Скажут, что подобное сравнение не корректно, потому что элита чаше всего не едина. Напомним: существуют также клетки с двумя, тремя, несколькими десятками и даже сотнями ядер. Это многоядерные клетки» [1]. Классовая ненависть — уникальное по своей силе и устойчивости психолого-политическое состояние, в котором органически соединяются зависть к богатым и счастливым с естественным стремлением к справедливости. При этом такое психолого-политическое состояние может служить мощнейшим этнообразующим элементом. Естественно возникает вопрос: можно ли в таком случае считать и классы своеобразными этносами? Правильный ответ будет таков: класс приобретает свойства этноса лишь тогда, когда начинает ощущать себя как некое «МЫ». В таком случае он превращается в «класс для себя» или в осознающую себя социальную общность. Но «класс в себе» как этнос рассматриваться не может. Свойства этноса ему не присущи. Стоит ли говорить, что важнейшей задачей всех революционных партий в ходе информационно-психологических войн против ненавистного им общественного и государственного строя становилось воспитание классового, то есть по сути нового этнического сознания.

---

[1] *Вассоевич А. Л.* Идеология нового элитаризма в условиях криминально-мафиозного способа производства // Российские элиты на рубеже веков (социальные технологии нового элитаризма). Материалы научно-практической конференции. СПб.: Лики России, 2000. С. 67–68.

Глава 2. Информационная политика России в контексте концепции «мягкой силы»

В условиях информационного общества высокую значимость приобретает деятельность государства в информационной сфере. Она охватывает объекты информатизации, информационные системы, сайты в информационно-телекоммуникационной сети «Интернет», сети связи, информационные технологии и т. д.[2] Поэтому информационная политика «как особая сфера жизнедеятельности людей, связанная с распространением информации в интересах государства и гражданского общества»[3] занимает особое место в современном обществе. После окончания «холодной войны» возросла популярность «мягкой силы» (soft power), предназначенной для достижения целей при помощи привлечения целевой аудитории и формирования благоприятной обстановки (правил, институтов и внедрения ценностей)[4]. Однако события конца XX – начала XXI вв. свидетельствуют о сдвиге парадигмы влияния на современные политические процессы. Действенность «мягкой силы» стала ставиться под сомнение, и акцент теперь сосредоточен на сочетании «жесткой силы» для принуждения и возмездия с «мягкой силой» в виде убеждения и притяжения. Дж. Най, являющийся автором нового концепта,

---

[2] Доктрина информационной безопасности Российской Федерации. URL: http://www.kremlin.ru/acts/bank/41460.

[3] *Манойло А. В., Петренко А. И., Фролов Д. Б.* Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия — Телеком, 2012. С. 103.

[4] См.: *Nye J.* Softpower // Foreign Policy. 1990. № 80. P. 153–171.

не отказываясь от использования «мягкой силы», пишет в своей работе «Будущее власти» о необходимости сочетания ресурсов для реализации поставленных целей с использованием полного набора инструментов: дипломатических, экономических, военных, политических, правовых, культурных, коммуникационных, применение которых может быть как раздельным, так и в совокупности. Сочетание этих инструментов предлагается называть «умной силой». События на Украине лишний раз подтвердили, что в условиях, когда речь идет о базовых интересах западных стран, используется тот вариант силы, с помощью которого можно получить максимальный результат и который способен привести к поставленной цели независимо от этической стороны предпринятых действий.

В современном внешнеполитическом дискурсе феномену «умной силы» соответствует понятие гибридной войны, которое все чаще используется в официальных документах. Так, на встрече Совета министров иностранных дел НАТО, состоявшейся 1 декабря 2015 г., была принята «Стратегия гибридных войн». Под «гибридной войной» в НАТО понимают тактику, при которой не используется открытое применение обычных военных средств. Она включает в себя пропаганду и дезинформацию, методы экономического давления, а также тайное использование сил специального назначения. По словам генерального секретаря организации Йенса Столтенберга, суть новой стратегии базируется на «трех китах: подготовка, сдерживание и оборона». Среди ответов на гибридные угрозы, кроме улучшения в работе разведывательных служб и обмене развединформацией, значится также возможность применения специальных сил быстрого реагирования [1].

Гибридная война включает в себя совокупность методов военно-силового, политико-дипломатического, финансово-экономического, информационно-психологического и информационно-технического давления, а также технологий цветных революций, терроризма и экстремизма, мероприятий спецслужб, формирований сил специального назначения, сил специальных операций и структур публичной дипломатии, осуществляемых по единому плану органами управления государства, военно-политического блока или ТНК.

Цели гибридной войны — полная или частичная дезинтеграция государства, качественное изменение его внутри- или внешнеполитического

[1] НАТО приняла стратегию против гибридных войн. 2 декабря 2015 г. URL: https://newsland.com/user/4296735949/content/nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot/4854888.

курса, замена государственного руководства на лояльные режимы, установление над страной внешнего идеологического и финансово-экономического контроля, ее хаотизация и подчинение диктату со стороны других государств или ТНК.

По мнению И. Н. Панарина, стратегия ведения гибридной войны НАТО предполагает доминирование инструментов «мягкой силы» и нацелена на дезинтеграцию евразийского пространства, создание хаоса и нестабильности в соседних с Россией государствах с использованием технологий цветных революций, информационной войны, терроризма и экстремизма, финансово-экономического давления, военно-силового принуждения [2]. «Мягкая сила» страны зиждется на трех основных источниках: культуре, политических ценностях и ее внешней политике, и действует в условиях доверия, которое может быть легко разрушенным, если правительства начинают заниматься манипуляцией. Как полагает Дж. Най, в век глобальной информации и размывания силы негосударственных игроков «мягкая сила» станет все более важной частью стратегии применения «умной силы» [3].

Особую роль играют экономические ресурсы, которые могут быть расценены как инструменты и мягкой, и жесткой силы. Так, успешная экономическая модель, характеризуемая размером и качеством ВВП, доходом на душу населения, уровнем научно-технического развития, природными и человеческими ресурсами, является привлекательной и становится объектом для копирования в качестве образца другими странами. Но нередко экономическое влияние используется для принуждения государства, проводящего политику, не соответствующую интересам наиболее развитых стран, для чего вводятся экономические санкции, ограничения как со стороны определенных государств, так и со стороны международных организаций.

Отношение к «мягкой силе» в российском политическом руководстве неоднозначное. С одной стороны, отдается должное «мягкой силе» как комплексному инструментарию для решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии, с другой — высказываются опасения, что усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам деструктивного и противоправного использования

[2] *Панарин И. Н.* Гладиаторы гибридной войны. URL: http://www.maxpark.com/community/politic/content/5497351.

[3] *Най С. Дж. (младший).* Будущее власти / Пер. с англ. В. Н. Верченко. М., 2014. С. 151.

«мягкой силы» и правозащитных концепций в целях оказания политического давления на суверенные государства, вмешательства в их внутренние дела и дестабилизации обстановки, манипулирования общественным мнением и сознанием.

В Концепции государственной политики Российской Федерации в сфере содействия международному развитию (утв. Указом Президента РФ от 20.04.2014 г. № 259) термин «мягкая сила» не используется, однако многие ее положения свидетельствуют об использовании ее механизмов в сфере реализации государственной политики в указанном контексте:

- укрепление позитивного восприятия Российской Федерации и ее культурно-гуманитарного влияния в мире;
- развитие институтов демократического общества, включая защиту прав человека;
- развитие сотрудничества с иностранными общественными и благотворительными организациями, оказание содействия развитию культурных и гуманитарных связей, осуществляемое общественными объединениями, негосударственными и некоммерческими организациями, зарегистрированными в Российской Федерации;
- содействие позитивному восприятию Российской Федерации как государства-донора в государстве — получателе помощи, а также в других государствах-донорах [1].

В Основных направлениях политики Российской Федерации в сфере международного культурно-гуманитарного сотрудничества (утв. Президентом Российской Федерации 18.12.2010 г.) акцентируется внимание на культурной дипломатии, являющейся составной частью «мягкой силы». «Используя специфические формы и методы воздействия на общественное мнение, — говорится в документе, — культурная дипломатия как никакой другой инструмент “мягкой силы” способна работать на укрепление международного авторитета страны, служить убедительным свидетельством возрождения Российской Федерации в качестве свободного и демократического государства» [2].

Отдавая должное эффективности «мягкой силы», российские государственные институты применяют и «жесткую силу» в зависимости

---

[1] Концепция государственной политики Российской Федерации в сфере содействия международному развитию. URL: http://www.mid.ru/ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/64542.

[2] Основные направления политики Российской Федерации в сфере международного культурно-гуманитарного сотрудничества. URL: http://www.mid.ru/ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/224550.

от складывающейся ситуации. Так, конфликт на Украине свидетельствует о том, что Россия, как и США, тоже использует «умную силу», чередуя жесткие методы в политике с мягкими, проявляя гибкость в целях реализации собственных интересов. Например, в качестве твердой силы могут рассматриваться:

- действия «вежливых людей» в Крыму, обеспечивших мирный переход республики под юрисдикцию Российской Федерации;
- разрешение Совета Федерации на применение Президентом России военной силы за рубежом;
- действия военнослужащих, проводящих свой отпуск в ДНР и ЛНР;
- ответные экономические санкции в отношении стран, поддержавших санкционную политику в отношении России;
- свертывание газового проекта «Южный поток» из-за несговорчивости европейской бюрократии.

Выбор средств российского политического руководства зависит в значительной степени от поддержки политики со стороны общества: так поддержка соотечественников, ярко проявившаяся в присоединении Крыма к России, дополняет в целом политику, основанную на исторической справедливости, великодержавии, уникальности российского пути и патриотизме. Как справедливо отмечают авторы коллективной монографии «Национальная безопасность России в условиях глобализации: геополитический подход», «российская “мягкая сила” пока очень слаба и только начинает формироваться: мало специалистов, недостаточно опыта, не изучены зарубежные и не наработаны собственные концепции и технологии работы с гражданским обществом в различных областях, отсутствуют соответствующие институты». Вместе с тем, следует согласиться, что «проигрывая в “мягкой силе”, Россия проигрывает стратегически» [3].

Понимание важности данного направления деятельности у российского политического руководства присутствует. Так, в выступлении на заседании Валдайского клуба 24 октября 2014 г. В. Путин сказал: «Несомненно, что в глобальном соревновании вырастет роль гуманитарных факторов: образования, науки, здравоохранения, культуры. Это, в свою очередь, существенно повлияет на международные отношения, в том числе потому, что ресурс так называемой «мягкой силы» будет в большей степени зависеть от реальных достижений в формировании человеческого капитала, нежели чем от изощрённости пропагандистских приёмов» [4].

---

[3] Национальная безопасность России в условиях глобализации: геополитический подход / Под ред. А. П. Кочеткова, А. В. Опалева. — М.: ЮНИТИ-ДАНА, 2016. С. 122.

[4] Заседание Международного дискуссионного клуба «Валдай», 24 октября 2014 г. URL: http://www.kremlin.ru/news/46860 (дата обращения: 15.01.2017).

Отдавая приоритет «мягкой силе» как форме влияния, имеющей перспективное будущее, Россия вынуждена применять «жесткую силу» в качестве вынужденной меры для защиты своих интересов. Представляется, что «мягкая сила» будет иметь приоритет перед «жесткой силой» в условиях демократизации международных отношений, равноправия государств, выполнения всеми государствами норм международного права.

«Умная сила» — это промежуточный вариант между «жесткой» и «мягкой» силой для периода, при котором еще не созданы условия для коллективной ответственности, при сохраняющейся тенденции к однополярному миру. В сложившихся условиях целесообразно, чтобы решение о применении «жесткой силы» могла консолидированно принимать ООН, а не только одно государство или региональные международные организации; при этом силовые действия должны быть направлены против тех, кто грубо нарушает нормы международного права.

Все большее значение в арсенале «мягкой силы» имеют средства и методы воздействия, в основе которых лежит коммуникация. На уровне государств эти методы объединены в информационную политику, характер которой в полной мере свидетельствует о ценностных ориентирах и предпочитаемых способах достижения поставленных целей, свойственных данному политическому режиму и обществу в целом. В качестве действенного фактора «мягкой силы» следует отметить поддержку «русского мира». Так, с 1994 г. работает правительственная комиссия по делам соотечественников за рубежом. Ее работа выстраивается в соответствии с Федеральным законом от 24.05.1999 г. № 99-ФЗ «О государственной политике Российской Федерации в отношении соотечественников за рубежом» и внесенными в него изменениями. В 2010 г. была уточнена формулировка государственной политики в отношении соотечественников, которая, в соответствии с законом, «представляет собой совокупность правовых, дипломатических, социальных, экономических, организационных мер, мер в области информации, образования, культуры…» [1]

В 2007 г. в России создан некоммерческий фонд «Институт демократии и сотрудничества» (европейское представительство находится в Париже, возглавляет его Н. А. Нарочницкая, нью-йоркское представительство, функционировавшее до 2015 г., возглавлял А. М. Мигранян). Миссия института — служить «мостом» между Россией и иностранными

[1] Федеральный закон Российской Федерации от 23.07.2010 г. № 179-ФЗ «О внесении изменений в Федеральный закон “О государственной политике Российской Федерации в отношении соотечественников за рубежом”» // Российская газета. 2010. 27 июля.

государствами, быть местом для диалога общественных организаций с той и другой стороны, местом пересечения информационных потоков и налаживания связей.

Среди наиболее эффективно действующих СМИ, работающих на внешнюю аудиторию, является RT (Russia Today) — российская международная многоязычная информационная телевизионная компания. Russia Today — первый англоязычный информационный канал, представляющий российскую точку зрения на события, происходящие в России и за рубежом. Новостной канал RT имеет 22 бюро в 19 странах и охватывает потенциальную аудиторию в 700 млн человек более чем в 100 странах. Ее основной англоязычный канал RT International — первый российский информационный телеканал, ведущий круглосуточное вещание на английском языке. RT — это три круглосуточных информационных телеканала, вещающие из Москвы более чем в 100 странах мира на английском, арабском и испанском языках, телеканалы RT America и RT UK, выходящие в эфир из собственных студий в Вашингтоне и в Лондоне, документальный канал RTД, а также глобальное новостное видеоагентство RUPTLY, предлагающее эксклюзивные материалы телеканалам всего мира.

В условиях жесткого информационного противодействия использование различных информационных каналов на формирование альтернативной Западу точки зрения является не только оправданной, но и необходимой формой защиты национальных интересов России. Поэтому важным направлением внешнеполитической деятельности Российской Федерации в соответствии с новыми руководящими документами, принятыми в 2015–2016 гг., является доведение до мировой общественности объективной информации о позиции России по основным международным проблемам, ее внешнеполитических инициативах и действиях, процессах и планах социально-экономического развития Российской Федерации, достижениях российской культуры и науки.

В соответствии с Указом Президента Российской Федерации от 9.12.2013 г. № 894 было создано Международное информационное агентство «Россия сегодня» для создания и ретрансляции за рубеж информационного продукта, созданного с учетом национальных интересов и предназначенного для иностранной аудитории. В Указе констатируется, что «основным направлением деятельности федерального государственного унитарного предприятия “Международное информационное агентство „Россия сегодня” является освещение за рубежом государственной политики Российской Федерации и общественной жизни в Российской

Федерации» [1]. Для этих целей в октябре 2014 г. были созданы радиоканал и информационное агентство «Спутник», предполагающий вещание на 45 языках, в том числе стран Европы, Азии, СНГ, Северной и Южной Америки. Таким образом, Россия добивается объективного восприятия ее в мире, развивает собственные эффективные средства информационного влияния на общественное мнение за рубежом, содействует усилению позиций российских и русскоязычных средств массовой информации в мировом информационном пространстве, предоставляя им необходимую для этого государственную поддержку, активно участвует в международном сотрудничестве в информационной сфере, принимает меры по противодействию угрозам своей информационной безопасности. В этих целях предполагается широкое использование новых информационно-коммуникационных технологий.

В соответствии с Концепцией внешней политики Российской Федерации, утвержденной 30.11.2016 г., «внешнеполитическая деятельность государства направлена на укрепление позиций российских средств массовой информации и массовых коммуникаций в глобальном информационном пространстве и доведение до широких кругов мировой общественности российской точки зрения на международные процессы» [2]. Информационное воздействие в XXI веке приобретает еще большую значимость, так как его направленность влияет на поведение большого количества людей, у которых под влиянием той или иной информации могут возникать потребности как конструктивного, так и деструктивного характера, что существенным образом влияет на политическую ситуацию в стране и в мировом пространстве в целом. Недаром средства информационного воздействия называют информационным оружием, так как по своим разрушительным силам оно сопоставимо с обычными средствами вооружения, а иногда по своим последствиям превосходит их. В современном научном дискурсе под информационным оружием понимается «совокупность информации, а также специальных методов, устройств и средств манипуляции ею для скрытого воздействия на информационный

---

[1] Указ Президента Российской Федерации от 09.12.2013 г. № 894 «О некоторых мерах по повышению эффективности деятельности государственных средств массовой информации» // Официальный сайт Президента России. URL: http://www.kremlin.ru/acts/bank/37871.

[2] Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41451/page/1.

ресурс противника с целью достижения поставленных целей и решения задач информационной борьбы (войны)» [3].

В целях предотвращения угрозы такого воздействия Россия предпринимает необходимые меры для обеспечения национальной и международной информационной безопасности, противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства, для борьбы с терроризмом и иными угрозами с применением информационно-коммуникационных технологий, добивается выработки под эгидой ООН универсальных правил ответственного поведения государств в области обеспечения международной информационной безопасности, в том числе посредством интернационализации на справедливой основе управления информационно-коммуникационной сетью «Интернет». По мнению специального представителя Президента России по вопросам международного сотрудничества в области информационной безопасности А. В. Крутских, в системе управления Интернетом нужно обеспечить базовые принципы его демонополизации, а также необходимо, чтобы все страны имели общее право на управление и каждая страна отвечала бы за обеспечение своей информационной безопасности в рамках своего информационного пространства [4]. Для решения задач информационной безопасности в рамках ООН по инициативе России в 2004 году была создана Группа правительственных экспертов для рассмотрения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер для их устранения. Россия, являясь инициатором создания этой коллегиальной структуры, вносит существенный вклад в международное сотрудничество в области информационной безопасности. Так, Российская Федерация предложила на заседании Группы правительственных экспертов, которое состоится 23 июня 2017 г., рассмотреть концепцию проекта резолюции Генеральной Ассамблеи ООН «Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности» [5], подтверждая, таким образом, свою ведущую роль в данной сфере.

---

[3] *Новиков В. К.* Информационное оружие — оружие современных и будущих войн. М.: Горячая линия – Телеком, 2011. С. 53.

[4] *Крутских А.* Кто владеет Интернетом, тот владеет миром // Международная жизнь. 2016. № 11. С. 26.

[5] *Бойко С.* Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. 2016. № 8. С. 70.

В Стратегии национальной безопасности Российской Федерации высказывается озабоченность тем, что «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» [1]. В Стратегии отмечается, что появляются новые формы противоправной деятельности с использованием информационных коммуникационных и высоких технологий. В целях осуществления государственной и общественной безопасности совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им; принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных спецслужб и пропагандистских структур. В подтверждение опасений, высказанных в Стратегии, 23 ноября 2016 г. депутаты Европарламента одобрили резолюцию о противодействии антиевропейской пропаганде, которую ведут Россия и исламистские террористические группировки. За резолюцию, которая носит рекомендательный характер, проголосовали 304 депутата при 179 голосах «против» и 208 воздержавшихся. В принятом документе говорится: «Враждебная пропаганда против ЕС и его государств-членов направлена на то, чтобы исказить истину, вызвать сомнения, разобщить Евросоюз и его партнеров в Северной Америке, парализовать процесс принятия решений, дискредитировать институты ЕС, а также посеять страх и неуверенность среди граждан Евросоюза». Для пропаганды, указывается в резолюции, «российское правительство использует широкий диапазон инструментов, включая ТВ-каналы, вещающие на разных языках (в том числе Russia Today), псевдоновостные агентства и мультимедийные сервисы (в том числе Sputnik), а также соцсети и интернет-троллей» [2]. Евросоюзу, подчеркивается в документе, необходимо более активно принимать меры по борьбе с кампаниями по дезинформации и пропагандой.

---

[1] Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 31.12.2015 г. № 683 // Официальный сайт Президента России. URL: http://www.kremlin.ru/acts/bank/40391.

[2] Европарламент принял резолюцию против российской пропаганды // Информационный портал Meduza.URL: https://www.meduza.io/news/2016/11/23/evroparlament-prinyal-rezolyutsiyu-o-protivodeystvii-rossiyskoy-propagande.

Резолюция рекомендует усилить «Оперативную группу по стратегическим коммуникациям на Востоке» (East Stratcom Task Force), превратив ее в полноценное ведомство в составе Европейской службы внешних связей. Оперативная группа, существующая с 2015 г., призвана оказывать информационную поддержку политики ЕС в отношении стран Восточного партнерства, поддерживать в этих странах независимые СМИ и противостоять «внешней дезинформации» [3].

Агрессивная информационная политика, проводимая западными странами против России, вынуждает российское политическое руководство принимать адекватные меры, и прежде всего в концептуальном плане. 5 декабря 2016 г. Президентом России (Указ № 646) была утверждена Доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере на основе анализа основных информационных угроз и оценки состояния информационной безопасности. В соответствии с документом, под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [4].

Возникает потребность в создании соответствующей инфраструктуры в целях формирования общества знаний, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации. Такая цель перед государством поставлена в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента России от 9 мая 2017 г. № 203, в которой определены задачи и меры по реализации внутренней и внешней политики страны «в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики,

---

[3] Там же.

[4] Доктрина информационной безопасности Российской Федерации. URL: http://www.kremlin.ru/acts/bank/41460.

обеспечение национальных интересов и реализацию стратегических национальных приоритетов» [1].

Технологии передачи информации с использованием сети «Интернет» все чаще используются для манипулирования общественным мнением. Происходит смещение акцентов в восприятии окружающего мира с научного, образовательного и культурного на развлекательно-справочный, что формирует новую модель восприятия — так называемое клиповое мышление, характерной особенностью которого является массовое поверхностное восприятие информации. Такая форма освоения информации упрощает влияние на взгляды и предпочтения людей, способствует формированию навязанных моделей поведения, что дает преимущество в достижении экономических и политических целей тем государствам и организациям, которым принадлежат технологии распространения информации. В сложившихся условиях национальными интересами страны становятся развитие человеческого потенциала, обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления, повышение эффективности государственного управления, развитие экономики и социальной сферы, формирование цифровой экономики.

Таким образом, использование полного набора инструментов воздействия на мировое сообщество, включающее в себя атрибуты как «мягкой», так и «умной» силы, наступательный характер в информационно-коммуникационной сфере, продвижение российских интересов на международной арене, противодействие угрозам информационной безопасности, составляет сущность информационной политики России в современном мире в условиях глобализации.

---

[1] Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=216363&fld=134&dst=1000000001,0&rnd=0.18778857851126673#0 (дата обращения: 10.06.2017).

Глава 3. Когнитивные технологии как инструмент сетевых войн

Бурное развитие и доступность информационных технологий перевели неформальные и формальные сети общения в цифровую форму, и есть тенденция к тому, что эта форма вскоре станет определяющей. По данным Фонда общественного мнения на весну 2015 г., доля граждан России, выходящих в Сеть хотя бы раз за сутки, составила 53% (61,5 млн чел.). 65% российских интернет-пользователей выходит в Сеть хотя бы раз в месяц. И за год показатель суточной аудитории Интернета вырос на 5% [2]. Это инфраструктура для проведения информационно-психологических операций сетевых войн [3].

Сетевую войну можно определить как борьбу за навязывание участникам реальных или виртуальных сетей общения своей картины мира, понимания событий, смыслов, потребностей, целей, мотивов, ценностей, состояний. Когнитивные технологии — инструменты этой борьбы, которые позволяют управлять процессами познания пользователей сетей: ощущения, восприятия, оценки, категоризации, выделения главного, построения причинно-следственных связей, связи воспринятого с целями, мотивами, потребностями поведения и деятельности участников сетей общения. Войны крайне редко ведутся за прямое физическое

---

[2] Интернет в России: динамика проникновения. Весна 2015. Интернет-ресурс: http://www.fom.ru/SMI-i-internet/12275.

[3] *Губанов Д. А., Новиков Д. А., Чхартишвили Г. А.* Социальные сети: модели информационного влияния, управления и противоборства. Сетевые структуры и организационные системы. М.: Физматлит, 2010; *Чумичкин А. А.* Модели управления сетевыми сообществами в условиях развития стратегий информационных войн // Национальные интересы: приоритеты и безопасность. 2012. № 11. С. 47–52.

уничтожение противника. В основе войн лежит разное представление о соотношении позиций субъектов конфликта в будущем. Условно говоря, если мирное население будет с нетерпением ждать, когда же армия противника освободит его от ненавистного тирана и обеспечит ему изобилие и процветание, свободу и демократию, война теряет всякий смысл. Соответственно возникает вопрос, как внедрить в сознание гражданского и военного населения противника установку на приемлемость, оправданность и желательность подобной предательской позиции.

Когда противник перешел в нашу веру, стал разделять наши взгляды, ценности и убеждения, переоделся в нашу униформу, стал мечтать о нашем образе жизни, смущаться и стыдиться своей принадлежности к недемократической стране, он стал нашим союзником. Глобализация, распространение единых ценностей, кумиров, стандартов понимания, отношений, стремлений, потребления, экономических и политических принципов по всему миру — это модель установления когнитивного господства, навязывание и закрепление в контролируемом семантическом поле информационной политики правильных смыслов. Когнитивные технологии сетевой войны выстраиваются на двух предположениях:

1. Определяющее воздействие на поведение человека часто оказывают не сами явления и события окружающего мира, а характер отношения человека к ним.
2. Поскольку человек является существом социальным, именно референтные для него социальные группы (сети общения) являются ключом к наиболее оперативному и эффективному воздействию на него.

У участников социальных сетей сформировано некоторое отношение к своей стране, ее властям, политике, обществу, его проблемам, другим странам…, и на это отношение можно влиять. Настраиваемый интерфейс площадки виртуального общения, топ новостей, новости друзей, новости групп, работа модераторов, комментарии, речевое поведение участников форумов, политика блокирования комментариев, блогов и др. — все это инструменты менеджмента восприятия [1] в отношении соответствующих событий. Для понимания управляемости этого процесса приведем официальную статистику по сети Твиттер: 5% пользователей Twitter создают 75% всего контента, распространенного в Сети [2].

---

[1] *Забарин А. В.* Менеджмент восприятия как психолого-политический феномен: генезис проблемы // Вопросы политической психологии. 2001. № 1. С. 33–38.

[2] Цит. по: *Коровин В. М.* Третья мировая сетевая война. Интернет-ресурс: http://www.loveread.ec/read_book.php?id=43903&p=36.

10–15 лет назад в Интернете распространялись программы интерактивного общения пользователя с искусственным интеллектом (Болтун, Viking Botovod и др.) Доработка и совершенствование этих программ вдохнули жизнь в виртуальных пользователей, способных поддерживать виртуальный диалог на общие темы на минимально приемлемом уровне. Дальнейшим развитием этих технологий искусственного интеллекта стало создание фейковых аккаунтов, озвучивающих на форумах заданную заказчиками позицию для формирования группового и общественного мнения в сети. Подобные программы оказались востребованными коммерческим сектором интернета — для написания отзывов и формирования рейтингов товаров, услуг и компаний.

Другой их точкой приложения стал политический сектор Интернета, имитирующий игру в демократию. Виртуальные группы фиктивных граждан призваны демонстрировать, как общественность активно включается в обсуждение решений, реформ, событий, что общественность не одобряет или горячо поддерживает такие-то взгляды, переключать внимание аудитории на другие темы, дискредитировать идеи, верования, идеалы и личности авторов, сеять сомнения в достоверности приводимых ими фактов, обоснованности доводов и логичности выводов, создавать онлайн-восстания, порождая впечатление включенности в протест сотен, тысяч, миллионов людей. Организуется классическая «борьба нанайских мальчиков»: зритель видит ожесточенную и драматичную борьбу двух кукол, но не знает, что эти куклы лишь правая и левая рука актера.

Психика современного пользователя социальных сетей оказалась удивительно беззащитным заложником когнитивных технологий сетевых войн. Информационно-психологическое воздействие совсем не всегда воспринимается человеком как опасность. Напротив, первично оно манит, поражает, пленяет, впечатляет. Поскольку информация является источником ориентации человека в окружающей среде, именно на ее основе он принимает решения, формирует собственные оценки событий и других людей, выстраивает свои убеждения. СМИ, Интернет, социальные сети стали на сегодняшний день ведущими средствами формирования картины мира человека.

Создаваемая ими виртуальная реальность стала периодически выдавать постановочные декорации за факты, подменять целостную картину событий односторонними фрагментами, подтверждающими какую-либо позицию. Давайте посмотрим глазами современника на следующие четыре оценки социальных событий:

1. Когда группа приносит себя в жертву во имя спасения всех остальных («победа одна на всех» и «за ценой не постоим»), создается имидж героев.
2. Когда группа приносит себя в жертву во имя идеи (спасения себя, спасения мира), далекой от реальности (с точки зрения здравого смысла подавляющего большинства граждан), то создается имидж деструктивной, психически неадекватной, преступной группы, секты фанатиков.
3. Если группу людей, представляющих особую угрозу безопасности других людей, их прав, свобод, законных интересов, в ходе захвата ликвидируют (то есть, по сути, приносят законным образом в жертву во имя спасения всех остальных), то данная деятельность государства и международного сообщества обретает имидж легитимного применения насилия, какими бы мессианскими мотивами при этом ни прикрывалась сама уничтоженная группа (действия СССР и союзных войск в отношении нацистской Германии, фашистской Италии, Японии, действия России в отношении бандформирований в Чечне, действия государственных властей и международных организаций в отношении террористической угрозы).
4. Если ликвидируют группу людей во имя идеи спасения демократии, других людей, их прав, свобод, идеалов, то в оценках современник начинает теряться: косовары и албанцы, Ирак, Ливия, Сирия и государства-члены ООН.

Способность человека видеть за словами реальную действительность, основанную на тесной связи первой и второй сигнальных систем, А. Л. Вассоевич очень метко назвал психической ориентацией на реальность, неспособность — ориентацией на имя [1]. В современном информационном обществе реальность (факты) начинают активно подменяться именами (имиджами). Реальной ли была угроза? Реальным ли было спасение других людей? Реальной ли была защита прав и ценностей демократии? Конструирование информационных фантомов в ответ на эти вопросы становится предметом перманентных информационно-психологических войн. Факты терроризма психологическая война начала подменять декорациями имиджей борцов за свободу и демократию. Расплатой за подобные войны становится экстремизм и фанатизм со стороны граждан, имеющих психическую ориентацию

[1] *Вассоевич А. Л.* Духовный мир народов Классического Востока. СПб.: Алетейя, 1998. 542 с.

на имя, и правовой нигилизм со стороны граждан, имеющих психическую ориентацию на реальность.

Избыточность информационных потоков современных виртуальных сетей общения подтвердила смысл известной формулы «максимум информации всегда равен нулю». Новостные посты как хроника кошмаров текущего дня стали катализатором тревог, страхов и политической агрессии. Порождаемые рекламой алогичные стереотипы суждений стали угрозой шизофренизации мышления. Коммерческое использование панических настроений потребителей стало проверкой на прочность волевых качеств современника. Развитие характера личности сменилось потаканием слабостям, а из способностей оказались востребованными лишь те, которые служат увеличению дохода. Содержанием направленности стала формула «Ничего личного, только бизнес». Личность превратилась в рекламную вывеску. Востребованной в условиях рыночной экономики стала особь с ее набором биологических и социально-биологических инстинктов, не отягощенная способностью критической оценки реальности.

Сегодняшние сетевые войны — это не только конкурентная борьба за формирование аддиктивных пристрастий потребителей к правильным фирмам в виде проектов по созданию коммерческих фетишей и сект поклонников новых брендовых продуктов. Это информационно-психологическое противостояние, утверждающее, прежде всего, политическое господство. Это геополитическая борьба государств и этносов за роль союзников, противников или нейтральной стороны в национальных, религиозных, иных конфликтах. Воюющие государства всегда стремились посеять смуту и раздоры в армии и среди гражданского населения противника, вызывали страх, панику, дискредитировали военных и политических лидеров, противопоставляли друг другу различные религиозные и национальные группы. Все это старо как мир, но приобрело невероятный размах в связи с бурным развитием информационных технологий. Самая эффективная геополитическая борьба происходит сегодня не на полях сражений, а в сознании социальных групп, в их картине мира, ценностных ориентациях, идеалах, стереотипах мышления, образе жизни.

Апогеем развития сетевых войн стала технология цветных революций, использующих мобилизованные и простимулированные человеческие ресурсы страны противника для свержения государственной власти. С развитием арсенала когнитивных технологий появилось качественно иное измерение массовых беспорядков. Образ массовых беспорядков как

агрессивно настроенной толпы, противодействующей властям и органам правопорядка, совершающей погромы, поджоги, насилие [1], обрел внешне законопослушную форму в виде технологий ненасильственных действий толпы, направленных, согласно декларации их идеологов, на «организацию демократического перехода власти народу».

Твиттерные революции, события «Арабской весны», массовые беспорядки в Кишиневе (2009), Евромайдан на Украине, где именно быстрое нагнетание протестных настроений по поводу «жертв режима» и оперативная координация организационных усилий провоцировали и поддерживали гражданские протесты, продемонстрировали высокую эффективность когнитивных технологий сетевой войны.

Как сетевая толпа превращается в творца твиттерных революций? Сетевая толпа объединяет различные группы пользователей интернета (как правило, молодежи) в рамках одной или нескольких Интернет-площадок (социальных сетей, форумов, сайтов) в целях последующей их мобилизации для проведения совместных акций, выступлений, протестов, погромов, восстаний и т. д. «Меняй жизнь к лучшему! Не мирись с ущемлениями своих прав! Не жди, когда перемены вызреют сами собой! Вступай в нашу сеть!» Как написали в свой книге «Новый цифровой мир» руководители компании Google Э. Шмидт и Дж. Коэн: «Больше не нужно терпеть несправедливость в изоляции и одиночестве. Возможность получить глобальную обратную связь, то есть комментарии и реакцию людей со всего мира, позволит жителям многих стран встать во весь рост и заявить о том, что они чувствуют. Как показала «Арабская весна», стоит только людям преодолеть так называемый барьер страха и понять несправедливость правительства, как к революции без колебаний присоединяются даже прежде тихие и лояльные граждане» [2]. Пользователь Интернета присоединяется к сетевой толпе на основе общности «лайков» выступлений, комментариев, фотографий, «перепостов» сообщений, тем, статусов и других признаков. Происходит максимально широкое и оперативное знакомство и общение всех со всеми, последующий отбор «единочувственников» и единомышленников.

Участник сетевой толпы воспринимает и пересылает другим участникам фильтруемые им информационные потоки. Так, в Твиттере организована система создания ретвиттов — цитирования понравившегося высказывания.

---

[1] См.: *Waddington, David P.* Contemporary issues in public disorder: a comparative and historical approach. N-Y., 2003. 243 p.

[2] *Шмидт Э., Коэн Д.* Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств. URL: http://www.lithub.me/book/403438.

В частности, через эту систему в ходе событий «цветных революций» шло массовое распространение инструкций о способах и средствах противостояния силам правопорядка, продвижение статей типа «Как использовать Facebook, если ты живешь в стране с репрессивным режимом». Через организацию интерфейса, систему рейтингов, рассылку однотипных, в том числе повторяющихся сообщений администрация сети также продвигает соответствующие темы для целевого информирования и создания соответствующего эмоционального резонанса в сетевой толпе. Вступая в сетевое сообщество, участник посредством каждодневного общения со знакомыми и близкими по духу людьми начинает корректировать, а в отдельных вопросах и формировать свою картину мира, свое понимание событий, свои смысложизненные ориентации, потребности, мотивы, ценности.

Традиционная парадигма работы с массовыми беспорядками выстраивалась, исходя из управления конфликтами для их разрешения, сегодня в международной практике мы наблюдаем стратегию и тактику управления конфликтами для их провоцирования и поддержания. Традиционная цель пресечь деструктивность, скорректировать, удержать в рамках социальных и юридических норм сменилась целью подогревать, провоцировать, культивировать деструктивность и направлять ее на разрушение противника.

Когнитивные технологии массовых беспорядков связаны с обострением и поддержанием информационно-психологических угроз (актуальных и потенциальных) общественной безопасности — защищенности личности, социальной группы, общества в целом от нарушения их жизненно важных интересов, прав, свобод. Гражданин как социальная роль, обусловленная реализацией соответствующих гражданских прав, свобод и ответственности, нуждается в обеспечении физической, психологической, экономической, информационной, правовой безопасности. Все эти виды безопасности используются когнитивными технологиями массовых беспорядков в качестве мишеней.

Физическая безопасность должна гарантировать гражданину отсутствие преступных посягательств на его жизнь и здоровье. Когда новостные топы в социальных сетях превращаются в хронику криминальных новостей, для общества наступает время тревог, страхов и депрессии.

Психологическая безопасность означает обеспечение гражданину уютной социально-психологической среды. Когда вместо культуры взаимного уважения трендом социального взаимодействия в сетях становится обстановка скандала, охота на ведьм, демонстративное игнорирование меньшинством мнения большинства, проявляется рост социально-психологической напряженности и числа конфликтов в обществе.

Экономическая безопасность связана с возможностью материального обеспечения гражданином своей семьи, потребностей. Гражданин становится экономически уязвим не только когда государство отказывается выполнять свои социальные гарантии, но и тогда, когда существо разумное сменяется в нем существом хотящим, желающим, оценивающим собственное достоинство через те материальные блага, которые у него есть, и вечно недовольным тем, что у него материальных благ так мало и они такие устаревшие. Когда умение жить по средствам заменяется потребностью жить в кредит, открывая двери баснословным прибылям спекулятивного капитала. Кризисы платежеспособности и банкротства, так же как и настроения хронического недовольства, могут представлять угрозу общественной безопасности.

Информационная безопасность подразумевает защищенность гражданина от воздействия вредоносной информации. Угрозы в данном случае возникают при использовании фантомов и иных информационных конструкций в СМИ (в вербальной и невербальной формах) [1]. Данная асоциальная практика используется для управления мыслями, чувствами и поступками гражданина, не считаясь с его истинными желаниями, волей и убеждениями, с явной или скрытной выгодой для источника информации. Ложь и полуправда, реклама и пиар — все это формы информационного насилия над личностью. Так, когда реклама каждый день объясняет гражданину, что он не успешный, не достойный, не настоящий, если он не может позволить себе…, если у него нет…, появляются фрустрированные социальные группы, трансформирующие свое экономическое недовольство в политическое, часть которых готова вымещать свою агрессию на представителях государства, внешнем мире и других социальных группах, у которых есть соответствующие блага.

И, наконец, правовая безопасность сопряжена с возможностью гражданина реализовывать закрепленные за ним права при исполнении соответствующих обязанностей. Демонстрация тотального фактического бесправия российских граждан и творимого чиновниками правового беспредела — это популярная сетевая игра, которая направлена на повышение градуса общественного недовольства политической системой.

Для этносов и «субэтносов» (в терминологии Л. Н. Гумилева) (социальных групп, общностей, субкультур) должна быть обеспечена этническая безопасность, связанная с защищенностью от дискриминации

---

[1] *Мезенцев Д. Ф.* Психологическое воздействие информационных фантомов // Хрестоматия к учебнику по политической психологии. СПб.: Коло, 2012. С. 253–266.

по национальному, религиозному и иному признаку. Этой мишени обычно адресуется максимальное количество ударов, провоцирующих противопоставление и раскол этноса по любым возможным признакам.

Другой мишенью когнитивных технологий массовых беспорядков является деформация представлений о самом общественном порядке. Под общественным порядком понимают сложившуюся в обществе систему отношений между людьми, правил взаимного поведения и общежития, регулируемых действующим законодательством, обычаями и традициями, а также нравственными нормами.

Организаторам массовых беспорядков необходимо создать для членов общества такой информационный и социально-психологический контекст, такие смыслы, которые позволили бы им лояльно, а в идеале даже позитивно, отнестись к требуемым радикальным социально-политическим и экономическим изменениям. Для этого, например, коллизию о том, определяется ли общественный порядок нормами права или общественным мнением, стали разрешать в пользу общественного мнения: «Государство погрязло в коррупции — это проявление общественного беспорядка, а свержение власти коррупционеров — это наведение общественного порядка».

Если рассматривать общественный порядок с точки зрения методологии А. М. Зимичева (категории Истины, Красоты, Добра, Справедливости, Изобилия как социальные цели жизнедеятельности человека)[2], можно выделить четыре его системообразующих элемента. Этими элементами являются идеологическая, символическая, нормативная и экономическая системы. Идеологическая и символическая системы связаны с регламентацией сознания граждан, нормативная и экономическая системы — в большей мере связаны с регламентацией поведения. Рассмотрим более подробно каждый из этих элементов.

Первым базовым системообразующим элементом общественного порядка выступает идеологическая система, связанная с социальным целеполаганием. Одним из основополагающих рефлексов, управляющих жизнедеятельностью, как отдельного человека, так и любой социальной общности, как отмечал еще И. П. Павлов, является рефлекс цели[3]. Утрата целей порождает экзистенциальный вакуум, потерю осмысленности существования, характерную для суицидального поведения. На смерть звал Гарибальди, и за ним пошли. За веру шли на костер и принимали мучения. Почему? Появлялся убедительный образ цели, идеализированное

---

[2] *Зимичев А. М.* Психология политической борьбы. СПб., 1993.

[3] *Павлов И. П.* Рефлекс свободы. СПб.: Питер, 2001. 432 с.

представление будущего, движение к которому наделяло смыслом человеческую жизнь. Если эти смыслы носят биологический характер, то с угрозой самосохранению под сомнением оказывается и возможность дальнейшего движения к цели.

Политическая деятельность формирует целеполагание на уровне общества через такой инструмент, как идеология. Государственная идеология воплощает в себе систему идеалов (светских, религиозных) в системе отношений субъектов гражданского общества между собой, с государством, отношений государства с другими международными субъектами. Государственная идеология формирует систему объединяющих сообщество смыслов, определяющих смысложизненные ориентации, стремления, личностную направленность граждан, специфику восприятия и оценки ими поступков и ситуаций, эмоционального реагирования, поведенческих стереотипов. Усваиваемые гражданами в процессе политической социализации идеологические смыслы выступают основой и залогом их лояльности и приверженности существующему общественному порядку.

Естественно, что идеологическое поле подавляющего большинства современных государств не является ни статичным, ни однополярным. Идеологическая конкуренция, институционально определяемая фактором многопартийности, задает вектор развития государственной идеологии в целом. Но при этом государство обязано защищать от эрозии базовые смыслы национальной политической системы (национальные ценности), рассматривая любую попытку их дискредитации как акт враждебного информационно-психологического воздействия. Вытеснение вступающих в конфронтацию с национальными идеалами и подрывающих доверие населения к ним альтернативных социально-политических идеалов на периферию политического спектра является условием самосохранения самой политической системы и устанавливаемого ею общественного порядка.

Второй системообразующий элемент общественного порядка — это символическая система, связанная с политическими символами. Любая идея, для того, чтобы она могла быть воспринята и усвоена, нуждается в определенной форме своего выражения. Такая форма выражения существует и применительно к национальной идеологии. Постижение тонкостей сложных идей в любом обществе — это удел его интеллектуальной элиты. Подавляющее большинство рядовых граждан в этом плане довольствуются формой (крестится двумя перстами или тремя). Формой национальной идеологии являются символы государства

и политической системы (флаг, герб, гимн), национальные праздники, ритуалы, церемонии, логотипы фирм и бренды, ассоциирующиеся с ценностями определенного образа жизни, и т. п. Конфуцию приписывают слова о том, что с соблюдения ритуалов начинается порядок в государственном управлении [1]. Выбор национальных праздников — это утверждение в массовом сознании значимости тех или иных исторических событий, выступающих точкой отсчета в формировании национально-культурной идентичности гражданина. Это формирование кумиров для подражания, галереи референтов для подрастающего поколения. Участие в ритуалах — это важнейшая социальная практика по освоению гражданами ценностей политической системы. Красота ритуала связывает положительные эмоции граждан с символизированными ценностями политической системы.

Подобно тому, как знамя полка на поле боя служит для солдата символом несгибаемого боевого духа, символы национальной идеологии являются средством мотивационного воздействия на дух гражданский. Выражаемые и разделяемые совместно с другими гражданами положительные эмоции по поводу символов национальной идеологии не только сплачивают сообщество, но и выступают важнейшей мотивационной составляющей относительно желания граждан быть полезными для своего отечества. Напротив, эстетическое чувство уродливости в оценке существующих социально-политических практик и отношений вызывает демотивирующее воздействие на граждан.

Форма, в которой закрепляется в обществе национальная идеология, как фактор эмоционального и мотивационного воздействия на гражданина, также является объектом информационно-психологического воздействия на политическую систему со стороны организаторов цветных революций. Это воздействие проявляется в такой форме массовых беспорядков, как вандализм. Происходит глумление над памятниками, культурными ценностями и святынями общества, героизм начинает относиться к области психиатрии. В информационном пространстве появляется армия клоунов, задача которых создать впечатление комичности в отношении традиционных для данного общества ритуалов. Символы национальной идеологии помещаются в такой смысловой контекст, который изменяет их эмоциональные коннотации с положительных на отрицательные. Оценка значимости этой составляющей находит свое отражение и в УК РФ, где статьи, связанные с оскорблением

---

[1] *Конфуций.* Суждения и беседы. М.: Мир книги, 2006. 352 с.

государственной символики, относятся к преступлениям против порядка государственного управления.

Третий системообразующий элемент общественного порядка — это нормативная система, которая включает в себя два подуровня — уровень социальных и юридических норм. Любой идеал остается положительно окрашенной умозрительной конструкцией до тех пор, пока он не начнет воплощаться в конкретных поведенческих практиках. Когда эти практики принимаются и осваиваются большинством членов того или иного сообщества, они становятся социальными обычаями. Обычай как исторически сложившаяся стереотипная форма массового поведения представлял собой воспроизводимые в неизменном виде стандартизированные действия, которые воплощали в себе определенные этнические ценности. Обычай выступал в качестве нормы, которая обеспечивала стабильность форм массового поведения.

Возможность предсказывать поведение друг друга, упорядочивать совместную жизнедеятельность и более эффективно удовлетворять основные потребности делает социальные нормы незаменимыми регуляторами социального поведения, без которых ни одно сообщество не может существовать. Если социальные нормы являются в значительной мере отражением условий развития и культуры самого социума, то нормы юридические часто оказываются средством управляющего воздействия на общество со стороны государства, устанавливающего законы. В юридических нормах через предписание правил дозволенного и недозволенного поведения закрепляются ценности государственной идеологии.

Четвертым системообразующим элементом общественного порядка является экономическая система, система распределения ресурсов, благ, доходов членов сообщества. Система распределения ресурсов является в значительной степени производной от сложившейся системы социальных норм, устанавливающих критерии справедливого распределения благ в обществе. Таким образом, идеология, система верований общества закрепляется в положительно окрашенных символах, выражается в системе неписанных и писаных правил поведения (социальных и юридических норм), в соответствии с которыми осуществляется справедливое распределение благ в обществе. Все эти четыре системы (идеологическая, символическая, нормативная и экономическая) закрепляют и воспроизводят общественный порядок. Они неразрывно связаны между собой, испытывают обратное влияние.

Общественный порядок основан на системе взаимоотношений граждан и различных формальных и неформальных социальных групп,

складывающихся в рамках каждой из четырех систем. Эти отношения могут варьироваться по шкале принятия — непринятия общественного порядка по различной степени выраженности положительного, индифферентного или отрицательного отношения: приверженность — лояльность — безразличие — нелояльность — предательство (как пассивная форма отношений) и открытая конфронтация (как активная форма отношений).

Очевидно, что в любом обществе характер отношений граждан к общественному порядку не будет замыкаться на какой-то один полюс. Устойчивость системы общественного порядка связана с приверженностью и лояльностью граждан и их объединений национальной идеологии, ее символам, этическим и юридическим нормам и принципам распределения благ в обществе. Угроза существованию общественного порядка возникает при увеличении выше критического уровня процента граждан, демонстрирующих неприятие установленного общественного порядка.

Деформация представлений общества об общественном порядке как мишень когнитивных технологий цветных революций подразумевает изменение этих систем. Для этого то, что субъективно воспринималось членами сообщества как Истина, объявляется ложью, то, что представляло в сознании членов сообщества категорию Красоты, объявляется уродством, категория Добра (юридических и социальных норм в отношениях) трансформируется в категорию Зла, а Изобилие, как принцип достаточности благ члена сообщества, объявляется Нищетой. Другим вариантом технологий деформации категорий общественного порядка является провозглашение мировоззренческого, эстетического, этического релятивизма: все идеалы, ценности, принципы относительны. «Пусть расцветают все цветы жизни!»

Определяющим и первоочередным является воздействие на идеологический компонент общественного порядка (категория Истины), которое должно сформировать у граждан приверженность новым социально-политическим идеалам. Так, идеологи перестройки трансформировали социалистический идеал служения народу и Отечеству в культ личного богатства (обогащайся, кто может) и накопления. Понятно, что эти идеалы закрепляются качественно различными и социальными, и юридическими нормами. Им соответствуют качественно разные символы и принципы распределения благ в обществе. Поскольку идеологическая система является источником жизненных смыслов членов общества, ее разрушение влечет за собой экзистенциальный вакуум, переход членов общества от социальных к биологическим смыслам.

Воздействие организаторов цветных революций на символическую систему общественного порядка направлено на формирование у членов общества негативного отношения к символам национальной идеологии. То, что считалось красивым, объявляется смешным, уродливым. Как следствие, происходит демотивация, потеря вкуса, желания действовать в соответствии с осмеянными социальными идеалами.

Воздействие на нормативную систему (категория Добра) нацелено на формирование у граждан переживания несправедливости существующих этических и юридических норм. То, что считалось добром, объявляется злом. Как следствие, у граждан возникает утрата ценностных ориентиров, наблюдаются внутриличностные кризисы, кризисы во внутригрупповых и межгрупповых отношениях. Исчезает доверие правосудию, законам перестают подчиняться. Возникает ситуация беспредела, закона тундры или аномии (Э. Дюркгейм). Юридическая норма не может держаться исключительно на страхе наказания. Если она не принимается обществом, образцом поведения она не станет. Если же юридическая норма прямо противоречит нормам социальным, возникает политическая агрессия. Общество становится неуправляемым, когда более 30–40% его членов перестают сознательно следовать установленным в нем нормам. Наконец, воздействие на экономическую систему направлено на формирование у граждан переживания несправедливости распределения ресурсов и недостаточности благ для удовлетворения потребностей. Мера интенсивности этого переживания определяет готовность граждан начать борьбу или идти за теми, кто обещает распределить ресурсы справедливо и дать благ больше (табл. 1).

Беспорядки существуют там, где есть четкое представление о том, что такое порядок. Там, где народная вера и идеалы объявляются ложью, там где, то, что воспринималось гражданами как красивое, объявляется уродством, там, где усвоенные гражданином с детства нравственно-этические нормы объявляются злом, там, где справедливое начинает расцениваться как несправедливое, исчезает и всякое понимание общественного порядка гражданином. Там, где нет уважения к законам, где закон не понятен гражданину и дискредитирован практикой правоприменения, где социальные нормы размыты, где нарушение норм — не исключение, а правило, где нельзя определить правого и виновного, там исчезают отличия и порядка от беспорядка. Когда в сознании населения противника исчезают критерии того, что такое норма, или вводится множество взаимоисключающих критериев нормы, то соответственно разрушается граница и между нормами и их нарушением, порядком и беспорядком.

Таблица 1

Когнитивные технологии массовых беспорядков (МБ)

Системный элемент общественного порядка	Идеологическая система (Истина)	Символическая система (Красота)	Нормативная система (Добро)	Экономическая система (Справедливость)
Уровень психической регуляции	Регламентация сознания	Регламентация сознания	Регламентация поведения	Регламентация поведения
Формируемые организаторами МБ установки	Приверженность новым социально-политическим идеалам	Негативное отношение к символам национальной идеологии	Несправедливость этических и юридических норм	Несправедливость распределения ресурсов
Последствия внедрения данных установок	Дискредитация и разрушение национальных политических идеалов	Формирование отрицательных эмоциональных коннотаций символов национальной идеологии	Дискредитация национальных этических и юридических норм	Убеждение в несправедливости национальной системы распределения ресурсов
Формы МБ	Экстремизм	Вандализм	Девиантное, делинквентное поведение	Различные формы экспроприации ресурсов

Когнитивная сфера, национальные ценности, традиции, нормы должны стать объектом особой охраны для обеспечения информационно-психологической безопасности России. Некогда этническая культура была мощнейшим инструментом обеспечения информационно-психологической безопасности для членов этноса. Человек, живущий в этносе, был защищен от деструктивного информационно-психологического воздействия извне фетишами и табу данного этноса, его религиозной и идеологической системами. Размытие сегодня понятий «нация», «раса», «государственность» приводит к тому, что человек превращается в многоэтническую систему, причудливо сочетающую в себе элементы различных субкультур. Эти элементы могут вступать в противоречие с ценностями национальной культуры, затруднять этническую идентификацию и порождать внутриэтнические конфликты. Ценности одних социальных групп могут становиться и источником дохода для других социальных групп, паразитирующих на том, что является для первых содержанием совести. Государственная идеология в России, согласно конституции, оказалась и вовсе под запретом. А что такое 150 телевизионных каналов, предлагаемых

современнику, с точки зрения формирования единых ценностей сообщества, общественного мнения? Это механизм их разрушения.

Мы можем объяснять подрастающему поколению содержание всевозможных приемов информационно-психологического воздействия. Но опытный шулер и начинающий игрок заведомо оказываются в неравной позиции. Поэтому основная роль в обеспечении информационно-психологической безопасности должна принадлежать российской культуре, ее ценностному измерению [1]. Манипуляции процветают на ниве культуры эгоцентризма, где человек человеку если и не волк, то во всяком случае объект, за счет которого должны быть удовлетворены в первую очередь собственные интересы. Но стая во все времена выживала эффективнее волков-одиночек. Человек может рождаться и альтруистом, и эгоистом, и садистом, и мазохистом, и если каждому позволить себя вести так, как ему хочется, общество не сможет быть цельным. Поэтому необходима ориентация не на отдельную особь, а на личность. А личность начинается с уважения и заботы о других, с умения и желания быть полезным другим, своему этносу. И главным измерением этноцентрической культуры является приоритет интересов этноса над частным эгоистическим интересом. Именно эта установка является секретом непобедимости России, и она же должна послужить основой обеспечения общественного порядка.

---

[1] *Мезенцев Д. Ф., Забарин А. В., Зимичев А. М.* Психологические основания обеспечения геополитической безопасности // Геополитика и безопасность. 2014. № 2. С. 98–105.

Глава 4. Информационно-психологические операции в системе гибридных войн

Гибридные войны в решении современных геополитических проблем сегодня все чаще проявляются в виде своей системообразующей составляющей — психологической войны, войны ментальной, смысловой, поведенческой и т. д. Об этом наглядно свидетельствуют драматические события на Украине. Массовые манипуляторные технологии, которые были использованы для информационно-психологического воздействия на массовое общественное сознание с учетом этнопсихологических, гендерных, психолого-возрастных и других особенностей населения, позволили породить хаос на Украине. Одновременно достаточно эффективно были героизированы и интегрированы в массовое общественное сознание украинские деструктивные образы (С. Бандера, Р. Шухевич и др.). В этих искусственно созданных условиях когнитивного диссонанса была незаметно подменена когнитивная карта сознания значительной части населения. В результате в украинском общественном сознании стали отмечаться эрозия этнополитического кода и проявление фрагментов архаичного сознания, порождающие массовое деструктивное поведение[2]. Так Украина, вопреки ее национальным интересам, стала из-за успешно проведенных информационно-психологических операций объектом геополитической экспансии Запада. В настоящее время и в России заметно расширились масштабы использования западными спецслужбами средств оказания

[2] *Собольников В. В.* Место и роль психологического воздействия в стратегии ведения «гибридных» войн НАТО // Гуманитарные проблемы военного дела. 2015. № 3(4). С. 25–31.

информационно-психологического воздействия, направленного на дестабилизацию внутриполитической ситуации в различных регионах страны, на подрыв ее суверенитета и территориальной целостности. Активно наращивается информационное воздействие, в первую очередь, на молодежь для размывания традиционных российских духовно-нравственных ценностей, ее исторических основ и патриотических традиций. На Западе все более усиливается предвзятая оценка государственной политики Российской Федерации в средствах массовой информации. И в то же время попытки объективного анализа зарубежными или российскими СМИ подвергаются откровенной дискриминации. Не случайно в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5.12.2016 г. № 646, в качестве одной из стратегических целей и основных направлений обеспечения информационной безопасности отмечается нейтрализация информационно-психологического воздействия на население страны. В связи с этим Л. Г. Ивашов, президент Академии геополитических проблем, напоминает, что мы в советское время как-то не обратили внимания на то, что в США еще в 1963 г. было издано наставление по информационно-психологическим операциям вооруженных сил США. И с тех пор американцы планомерно осваивают этот фронт новой борьбы. Так, несколько лет назад в Пентагоне было создано главное киберкомандование, в настоящее время насчитывающее более 40 тысяч специалистов. Эти силы способны с помощью кибератак полностью выводить из строя систему государственного, финансового и военного управления той или иной страны [1]. В настоящее время имеются специальные органы по ведению психологической войны у целого ряда стран. Они носят наименования подразделений «психологических операций» (Великобритания, Южная Корея), «информационных операций» (Канада), «оперативной информации» (ФРГ), «психологического обеспечения» (Израиль), «психологической обороны» (Швеция), «психологических действий» (Польша), «психологической войны» (Турция) и т. д. Более того, в 2014 г. в Латвии начал функционировать Центр стратегических коммуникаций НАТО (NATO Strategic Communications Centre of Excellence), среди задач которого наиболее значимыми являются вопросы ведения «гибридных войн» [2].

---

[1] *Ивашов Л.* Доктрина информационной безопасности. URL: http://www.news-front.info/2016/12/0/doktrina-informacionnoj-bezopasnosti-leonid-ivashov.

[2] *Собольников В. В.* Место и роль психологического воздействия в стратегии ведения «гибридных» войн НАТО // Гуманитарные проблемы военного дела. 2015. № 3(4). С. 25–31.

Информационно-психологическое воздействие на людей не является изобретением сегодняшнего дня, а имеет давнюю историю, описанную в целом ряде историко-философских трактатов восточных, древнекитайских, а также более поздних европейских авторов [3]. Но систематизировать и получать научное объяснение информационно-психологическое воздействие на людей в широких масштабах стало возможным только в начале XX века. Начиная со Второй мировой войны пропагандистская работа стала проводиться всеми странами в форме информационно-психологических операций и других мероприятий информационно-психологического воздействия [4].

В современных условиях глобального внедрения информационных технологий в жизнедеятельность общества военные американские специалисты одними из первых отметили повышение роли информационно-психологических операций в мире и стали изучать возможности их использования для достижения своих геополитических целей [5]. По мнению специалистов Пентагона, в настоящее время перед службами специального назначения в первую очередь стоит задача в подрыве взглядов, ценностей, мировоззрения людей и закладке ложных целей общественно-политического развития в сознание населения государств, являющихся геополитическими конкурентами. Для большинства западных стран сегодня использование информационно-психологических операций стало неотъемлемой частью их геополитики благодаря отсутствию у большинства граждан понимания той угрозы, которую представляют современные информационно-психологические технологии при их латентном использовании для достижения геополитических и других целей [6].

Информационно-психологические операции в настоящее время представляют собой осуществление на практике совокупности различных видов

---

[3] 10 древних тактик ведения психологической войны. URL: http: //www.ucmopuockon.livejournal.com/12502591.html.

[4] *Баришполец В. А.* Области применения информационно-психологического воздействия. URL: https://www.docviewer.yandex.ru/?url=http%3A%2F%2FCyberLeninka.ru%2Farticle%2Fn%2Foblasti-primeneniya-informatsionno-psihologicheskogo-vozdeystviya. pdf&name=oblasti-primeneniya-informatsionno-psihologicheskogo-vozdeystviya.pdf&lang=ru&c=584bbcd54fca&page=2.

[5] *Лайнбарджер П.* Психологическая война. Теория и практика обработки массового сознания. М., 2013. 445 с.

[6] *Скоробогатов В. В.* Информационная война в современном мире: цели, составные элементы, последствия (теоретический аспект изучения) // Проблемы современной науки и образования. 2016. № 7(49). С. 190–192.

информационно-психологического воздействия, скоординированных и взаимоувязанных по целям, объектам, месту и времени, представляющих в результате настоящую психологическую войну. Объектами воздействия информационно-психологических операций являются психика отдельных людей, общественное сознание, мнение и настроение больших социальных групп, населения всего государства. При этом информационно-психологические операции представляют одну из форм геополитического противоборства — достижение и удержание информационно-психологического превосходства. В результате информационно-психологического воздействия у граждан, подвергающихся геополитическому воздействию, формируется положительный стереотип по отношению к государству, осуществляющему геополитическую экспансию. Опираясь на поддержку обманутого населения, это государство сможет проводить необходимую ему линию. Информационно-психологические операции, использующие технологии массовой манипуляции для явного и скрытого управления психикой, поведением человека, разных социальных групп путем формирования у них представлений, ценностей, потребностей, оказывают репрессивное воздействие на социальное окружение, порождающее хаос и перманентный конфликт. При этом с помощью явного и скрытого управления психикой, действиями и поведением человека эти операции делают ставку не на сознание, а на подсознательные и бессознательные пласты психики, порождающие эмоциональное неконтролируемое поведение. Так осуществляется политическое манипулирование, скрытое управление политическим сознанием и поведением людей для принуждения их действовать вопреки собственным интересам [1].

Манипуляция представляет собой вид скрытого, неявного психологического воздействия на людей с целью управления их поведением. Манипуляцией являются все формы воздействия, как сознательно организованные, так и бессознательные. Мишенью манипуляции являются эмоции людей, чтобы, вызвав чувство вины или страха, зависти или эйфории, изменить их поведение в соответствии с желанием и целью манипулирующего геополитического оппонента. Все многообразие манипулирования общественным сознанием направлено на замену мировоззренческих основ общества, его политических, нравственных, эстетических и других

[1] *Корчемкин С. Е., Капитонова Е. В.* Социально-психологические аспекты манипулирования общественным мнением как одна из стратегий современной гибридной войны // Риск и безопасность: социально-психологические аспекты: Материалы VI Международного симпозиума. Екатеринбург: Гуманитарный ун-т: Рос. психол. о-во, 2015. С. 55–56.

ценностей. Достигается это с помощью определенной манипулятивной подачи информации, с использованием определенных речевых психотехник и тотальной манипуляцией телевидения. Манипулирование направлено на дезинтеграцию и обвинение политических оппонентов, на провоцирование конфликтного и деструктивного взаимодействия. Исследователи выделяют целый ряд часто встречающихся манипуляций:

— провоцирование защитных реакций;
— провоцирование замешательства;
— дезориентация личности;
— формирование впечатления, что партнер настроен на сотрудничество;
— игра на вашей нетерпимости — «висящая морковка»;
— игра на вашем чувстве безысходности;
— игра на чувстве жадности;
— использование запланированных «трудных» уступок;
— намеренное затягивание времени обсуждения;
— провоцирование вашего интереса к партнеру — «Убаюкивание», чтобы «убить» позднее[2].

В современных условиях существует большое количество конкретных приемов таких манипуляций. Эти приемы хорошо описывает С. Кара-Мурза[3]. Среди них можно выделить:

— «***навешивание ярлыков***»: оскорбительные названия, имена, эпитеты, метафоры, вызывающие эмоционально негативное отношение к конкретным людям, всему государству — объекту геополитической экспансии;
— «***трансфер***» («***перенос***»): ненавязчиво и незаметно переносится общепризнанный авторитет на нужную при геополитической экспансии фигуру, явление, процесс для формирования между ними ассоциативных связей, имеющих ценность и значимость у окружающих;
— «***ссылка на авторитет***»: установления доверительных отношений с манипулируемой аудиторией или конкретными людьми;
— «***перетасовка***» («***подтасовка карт***»): односторонняя подача только положительных или только отрицательных фактов, свидетельств, доводов, при одновременном замалчивании противоположных;

---

[2] *Романова К. С.* Манипуляция как форма «мягкой» власти // Дискурс-Пи. 2014. № 1(11). С. 133–134.

[3] *Кара-Мурза С. Г.* Манипуляция сознанием. М.: Эксмо, 2009. 528 с.

- «***общий вагон***»: подбор суждений, высказываний, фраз, требующих единообразия в поведении, для создания впечатления, будто так делают все;
- «***обратный эффект***»: большое количество негативной информации вызывает прямо противоположный эффект;
- «***принцип контраста***»: одна информация подается на фоне другой;
- «***правда — наполовину***»: манипулируемой аудитории преподносится только часть достоверной информации;
- «***осмеяние***» конкретных лиц, взглядов, идей, программ, организаций для усиления информационно-психологического воздействия на целевые аудитории;
- ***слухи***: пропагандистское воздействие в условиях дефицита информации;
- ***провокации***: как целенаправленное создание событий в качестве информационного повода;
- «***захват***» медиапространства: люди получают информацию только от одной организации как единственно верной;
- «***утвердительные заявления***»: распространение различных утверждений как самоочевидных и не требующих доказательств заявлений;
- «***принуждающая пропаганда***»: использование слов и выражений принуждающего характера, типа «голосуй или проиграешь»;
- «***общественное неодобрение***»: создание негативного образа политика путем тенденциозного подбора различных высказываний «групп влияния», «представителей» различных слоев населения;
- ***«прямое опровержение»*** всех элементов пропаганды другой стороны;
- «***игнорирование***»: преднамеренное умолчание нежелательных элементов и тем другой стороны;
- ***«нарушение логических и временных связей между событиями»*** для создания иллюзии тех или иных тенденций и ситуаций;
- ***«замена источника сообщения»*** для увеличения или уменьшения доверия к сообщению за счет манипулирования источниками;
- ***«формирование информационного окружения»*** вокруг какого-то события для снижения или увеличения его значения;
- ***«рейтинги»*** для манипуляции общественным мнением других стран.

В ходе различных информационно-психологических операций в пределах «окна возможностей Овертона» совершенно чуждые обществу идеи

двигают от стадии «немыслимых», полностью отвергаемых, до стадии широко обсуждаемых и принятых массовым сознанием. Такая опасная технология позволяет легализовать самые низменные людские пороки, окончательно убивая в людях последние остатки человечности [1]. Степень изученности феномена информационно-психологических войн носит междисциплинарный характер и является результатом исследований широкого круга историков, политологов, философов, правоведов [2]. Эти исследования показывают, что информационно-психологические операции следует трактовать как совокупность методов и приемов трансформации информационного пространства и поведения населения геополитического противника. При этом базовым элементом таких операций является навязывание населению геополитического противника определенной картины мира, в которой заложены желаемые типы социального поведения.

В настоящее время разработан целый ряд информационно-психологических операций, показавших свою эффективность в манипулировании людьми в разных странах. Эти операции сегодня становятся все более масштабными и политически результативными. Традиционными политическими технологиями, используемыми для достижения эффективного результата в создании у населения определенных политических убеждений и ориентаций, являются:

1. **Политическая мифологизация** — процесс формирования у населения государства (геополитического конкурента) установок, стереотипов, групповых норм, массовых политических настроений, общественного мнения для развития некритичного мышления, неустойчивого, импульсивно воспринимающего состояния в целях управления поведением людей в нужном для геополитического субъекта направлении. При конструировании политического мифа и для эффективного его внедрения в массовое сознание решающее значение имеет героизация того или иного образа политического лидера. Такая героизация опирается на социальную востребованность в герое на базе несоответствия желаемого и действительного в политической жизни страны. Положительный образ героя играет значительную роль для оправдания, легитимизации действий в данной стране внешнего геополитического субъекта.

2. **Политическое имиджирование**, при котором распространенными политическими имиджформирующими приемами являются:

---

[1] *Соколов А.* Тихо и незаметно: способы ведения информационной войны. URL: http://evrazia.org/article/2842.

[2] *Лукин В. Н., Мусиенко Т. В.* Изменение стратегической культуры: подходы и модели, операции и нарративы // Credonew. 2015. С. 197–221.

— внедрение образа-посредника для отождествления политического лидера с образом другого известного или неизвестного человека на основе позитивного его восприятия в массовом сознании;
— систематическая публикация результатов рейтингов, социологических опросов, которые, как достоверные источники, ориентируют население с помощью использования образа большинства на соответствующие политические нормы, ценности;
— сравнение с зарубежными политиками, при котором на фоне негативного, ироничного характера информации, например, об отечественных политиках в массовом сознании в определенном позитивном ракурсе представляются те или политические лидеры геополитического субъекта, которые становится все ближе к своему народу, понимают его и живут его чаяниями и проблемами. При этом о своих политиках допускается дозированная негативная информация, чтобы не допустить их идеализации;
— политические скандалы, «грязные» политические истории, которые имеют актуальность на данный период и целенаправленно предлагаются массовому сознанию для определенного восприятия той или иной политической фигуры данной страны, нежелательной для внешнего геополитического субъекта. Для создания у граждан страны негативной оценки о политике СМИ преподносят в соответствующий момент различные политические скандалы в виде таких «грязных» историй, имеющих разоблачительный и резонансный характер, как громкие некорректные высказывания политиков, нелепые истории, коррупционный скандал, шпионаж за политическими оппонентами, компромат на аудио-видеозаписях, фальшивые дипломы, плагиат в диссертациях, алкогольные истории, любовные романы и т. д. Многие такие скандалы имеют достаточно спорный характер из-за отсутствия официальных доказательств причастности политика к тем или иным событиям [1].

3. **Деструкции дискурса**, понимаемые как «нарушения кодирования (декодирования) информации, влияющие на процесс восприятия и интерпретации мировых событий и обусловленные культурными различиями, этноцентризмом, стереотипами, свойственными участникам коммуникации» [2].

---

[1] *Нестерчук О. А.* Традиционные и инновационные политические технологии в информационно-психологическом противоборстве // PolitBook. 2015. № 2. С. 94–95.

[2] *Кошкарова Н. Н.* Лингвистические подходы к изучению конфликтного дискурса // Вестник Новосибирск. гос. ун-та. Серия: История, филология. 2015. Т. 14. № 2. С. 143.

Деструкция дискурса имеет свои характерные черты и в пространстве современных СМИ проявляется в различных приёмах и методах, как:

— изменение аксиологических приоритетов и установок;
— замена идеологической парадигмы;
— цензура на высказывания в СМИ;
— идеологическое преследование людей, имеющих собственную точку зрения на происходящие события [3].

4. **Хоррор-менеджмент**, который предполагает выполнение следующих задач:

— целенаправленное внедрение негативной информации как истинной в массовое сознание для решения геополитических задач;
— формирование чувства собственной незащищенности посредством поддержания обстановки постоянной ненависти, агрессии, страха, тревоги;
— реализацию замыслов, достижение которых связывается с поддержкой общественного мнения.

Постоянная негативная информация в СМИ заставляет население чувствовать себя беззащитной, неполноценной, разобщенной нацией и нуждаться в другой, более сильной политической власти, которая бы смогла объединить граждан, решить социальные проблемы, взять на себя ответственность за судьбу страны. В политические технологии информационно-психологического противоборства внедряются элементы деструктивной инновационности табуированного характера, выраженной в сокрытии манипулирования массовым сознанием. Так, одной из табуированных целей политических технологий цветных революций является деформация общества. Для достижения этой цели активно привлекаются СМИ, одной из главных задач которых становится смена ценностной ориентации граждан, особенно молодежи, разрушение «культурного ядра» и дестабилизация общества. Это необходимо реформаторам для установления культурной диктатуры ради дальнейшего перехвата управления государством [4].

5. **Когнитивное моделирование**, направленное на переформатирование сознания. Наглядным примером такого моделирования сегодня является

---

[3] *Кошкарова Н. Н.* «Как слово наше отзовется»: Почему информационная политика может перерасти в информационно-психологическую войну // Теоретические и прикладные аспекты изучения речевой деятельности. Нижний Новгород, НГЛУ им. Н. А. Добролюбова, 2015. С. 88.

[4] *Нестерчук О. А.* Традиционные и инновационные политические технологии в информационно-психологическом противоборстве // PolitBook. 2015. № 2. С. 96–97.

фальсификация истории Великой Отечественной войны, ядра сакральной исторической матрицы России. Она осуществляется в несколько этапов. Сначала внедряются в сознание людей такие установки, как «советские войска, а не гитлеровские, были и оккупационными». Далее на базе подобных закреплённых образов и представлений происходит пересмотр отношения ко всем советскому, а далее — и к русскому. На следующем этапе уже следуют конкретные действия — начинается уничтожение военных памятников и всего того, что связано с Великой Победой. Главной целью фальсификации истории становится не только пересмотр важнейших геополитических итогов Второй мировой войны, но и реабилитация преступных идеологий, их институциональное возрождение и легализация. Основным ее направлением является концептуальная фальсификация, предполагающая на первом этапе постановку знака равенства между гитлеровской Германией и Советским Союзом, как представляющими тоталитарные режимы, и возложение на них равной ответственности за развязывание Второй мировой войны [1]. Если же советский режим подобен фашистскому, то, по этой логике, СССР к победе не причастен и его нахождение в числе государств-победителей и празднование Дня Победы 9 Мая являются нелегитимными. Советский Союз должен быть не среди триумфаторов, а среди тех, кто был осужден за преступления против человечества. На роль победителей утверждаются страны англосаксонского мира.

На следующем этапе выдвигается тезис о преимущественной виновности СССР в развязывании Второй мировой войны. Так, активно муссируется тезис о том, что Сталин якобы готовил нападение на Германию и Гитлер вынужден был упредить его. Сегодня уже идут дальше — оказывается, наша страна развязала и Первую мировую войну [2]. И отсюда вывод: раз Россия вчера развязала Первую и Вторую мировые войны, то сегодня она развязывает Третью мировую войну. Так из процесса десоветизации вытекает процесс дерусификации, осуждения России как цивилизации [3]. При таком подходе происходит реабилитация позиции Запада, который поощрял нацистов в предвоенные годы и снисходителен

---

[1] *Пономарева Е.* Фальсификация истории Великой Отечественной войны — технология трансформации сознания // ОБОЗРЕВАТЕЛЬ–OBSERVER. 2016. № 5. С. 7–8.

[2] Кто развязал Первую мировую войну. URL: http://www.bbc.co.uk/russian/international/2014/02/140213_wwi_start_10_versions.

[3] *Багдасарян В. Э.* Великая Отечественная война в фокусе информационно-психологической войны против России // Вестник Московского гос. обл. ун-та. Серия: История и политические науки. 2015. № 2. С. 27.

к ним в настоящее время. Поэтому общественному мнению предлагается сознательное искажение фактов. Следующим направлением фальсификации итогов Второй мировой войны является искажение, умолчание и сокрытие неприглядных для Запада исторических фактов. Так, умалчивая о битвах на советско-германском фронте, на Западе исключительно ведется речь о сражениях в Западной Европе, Африке и Тихом океане.

Например, с первых дней Великой Отечественной войны Германия имела в составе своих войск десятки дивизий своих союзников из Западной Европы, которые в целях усиления вермахта мобилизовали свыше 1 млн 800 тыс. чел. для борьбы против Советского Союза. Из них было сформировано 59 дивизий, 23 бригады и ряд отдельных полков, легионов и батальонов. В войсках СС было создано 26 добровольческих дивизий, в которых служили албанцы, голландцы, датчане, венгры, бельгийцы, французы, латыши, литовцы, эстонцы, украинцы и др. В составе военнопленных в СССР были и венгры, румыны, австрийцы, чехи, словаки, поляки, итальянцы, французы, хорваты и т. д. [4]

В фальсификации исторических фактов важное место отводится кампании дегероизации участников Великой Отечественной войны. В этой кампании можно выделить несколько подходов. Первый подход заключается в утверждении, что подвига не было, он оказывается вымыслом, развенчиваемым дегероизатором. Так, отсюда вытекают, например, попытки отрицания существования «Молодой гвардии». Другой подход предполагает, что подвиг был совершен, но героями являются неизвестные никому люди, не те, кто официально почитался. Этот подход иллюстрирует попытки лишения подвига Николая Гастелло [5]. Третий подход состоит в маргинализации героев, не достойных подражания. Примером тому является муссирование криминального прошлого Александра Матросова. Четвертый подход состоит в утверждении, что совершенные подвиги являлись преступлениями. Так, например, Зоя Космодемьянская определяется в качестве террористки. Пятый подход в дегероизации состоит в «замещении героев», вытеснении образов настоящих героев преступниками, как С. Бандера или Р. Шухевич [6]. Фальсификации исторических фактов приводят к чудовищным результатам. Так, сегодня более

---

[4] *Пономарева Е.* Фальсификация истории Великой Отечественной войны — технология трансформации сознания // ОБОЗРЕВАТЕЛЬ–OBSERVER. 2016. № 5. С. 14.

[5] Подвиг Гастелло. URL: http:/www.alternathistory.org.ua/podvig-gastello.

[6] *Багдасарян В. Э.* Великая Отечественная война в фокусе информационно-психологической войны против России // Вестник Московского гос. обл. ун-та. Серия: История и политические науки. 2015. № 2. С. 31–32.

30% японских школьников считают, что атомные бомбы на Хиросиму и Нагасаки сбросили советские, а не американские самолеты [1].

В фальсификации истории Великой Отечественной войны геополитические противники важное место отводят внутрироссийской пропаганде. Красноречивы в этом отношении высказывания ряда известных представителей либеральной, антироссийской оппозиции. Так, А. Минкин пишет: «Может, это лучше бы фашистская Германия в 1945 году победила СССР, а еще бы лучше, в 1941-м. Не потеряли бы мы свои то ли 22, то ли 30 миллионов людей, и это не считая послевоенных бериевских миллионов. Мы освободили Германию. Может, это лучше бы освободили нас» [2]. Л. Гозман считает: «У СМЕРШ не было красивой формы, но это, пожалуй, единственное их отличие от войск СС… И само это слово — СМЕРШ — должно стоять в одном ряду со словами "СС", "НКВД" и "гестапо", вызывать ужас и отвращение, а не выноситься в название патриотических боевиков» [3]. Е. Ихлов полагает: «Генерал Власов был прав. Лучшая участь для нашей страны — это разделиться на этнические государства, высшим достижением которых будет интеграция в Западную Европу на правах трудновоспитываемых младших братьев» [4]. Фальсификация, ревизия итогов Второй мировой войны имеет четкую геополитическую цель: снижение геополитической субъектности России и оттеснение ее на периферию мировой политики. Не случайно В. Э. Багдасарян вполне обоснованно подчеркивает: «Сакральная историческая матрица — это фундаментальная основа бытия национальных сообществ. Разрушение этой матрицы приводит в конечном итоге социум к гибели. Поэтому сакрализация и ресакрализация подвига в Великой Отечественной войне есть на сегодня вопрос обеспечения национальной безопасности России. Именно так об этом и надо говорить и именно таким образом к этому относиться» [5].

---

[1] *Пономарева Е.* Фальсификация истории Великой Отечественной войны — технология трансформации сознания // ОБОЗРЕВАТЕЛЬ–OBSERVER. 2016. № 5. С. 17.

[2] *Минкин А.* Чья победа? // Московский комсомолец. 2005. № 1690. 22 июня. URL: http://www.mk.ru/editions/daily/ article/2005/06/22/194712-chya-pobeda.html.

[3] *Гозман Л.* «Подвигу солдат СС посвящается…» URL: http://www.echo.msk.ru/blog/leonid_gozman/1072194-echo.

[4] *Ихлов Е.* Власовская альтернатива. URL: http://www.kasparov.ru/material.php?id=4C340173653B2.

[5] *Багдасарян В. Э.* Великая Отечественная война в фокусе информационно-психологической войны против России // Вестник Моского гос. обл. ун-та. Серия: История и политические науки. 2015. № 2. С. 34.

6. Среди информационно-психологических операций активно применяется так называемая технология информационно-психологического воздействия через сетевые структуры, являющиеся своего рода «экономической и идеологической диверсией» против государств. В современном информационном обществе сетевые структуры оказывают непосредственное влияние на политику, экономику, духовную культуру, а также на систему государственного управления, финансово-кредитную, информационно-аналитическую деятельность. Под воздействием этих сетевых структур была деформирована общественная психология и культура в постсоветском пространстве, что привело к нарушению устоявшихся культурно-этических представлений в обществе и разрушению единого советского геополитического пространства.

В настоящее время миллиарды людей не могут жить без контактов в социальных сетях. Для них количество получаемых стилизованных графических изображений в виде смайликов стало более референтным, чем нравоучения родителей, учителей или других окружающих их людей. Именно такие сети легко формируют, особенно среди молодежи, деструктивное, делинквентное поведение. Одним из эффективных методов формирования такого поведения является игра в этих сетях. В опытных руках игра превращается в очень грозное оружие, принимая во внимание высокую скорость распространения информационных технологий, их привлекательность и способность смешивать мир виртуальной игры с миром реальным. Так, игры в поиск монстров-покемонов могут стать сравнительно безобидной прелюдией безумного тотального совмещения компьютерной интерактивной игры и реального мира, воли конкретного человека и приказов неведомого ему программиста.

7. Одну из ведущих мест среди информационно-психологических операций занимает такой популярный вид манипулирования людьми, как флэш-моб. Его популярность основана на возможностях быстрого обмена информацией друг с другом участниками флэш-моба через социальные и мобильные сети. Флэш-моб позволяет участникам в большой организованной толпе в сети почувствовать свою силу, свою возможность для самоутверждения и эмоциональной подзарядки, ощутить чувство свободы от общественных стереотипов поведения, свою причастность к общему делу. Основными участником флэш-моба, как правило, является молодежь как основной пользователь мобильной связи. Кроме этого, активными пользователями этих сетей являются образованные люди с активной жизненной позицией, критически настроенные к власти и, соответственно, в состоянии постоянной готовности к активным

действиям. Используя нервозность людей, даже далеких от центра событий, можно привлечь их к протестным действиям. Так можно за короткое время вывести на улицы тысячи недовольных и успешно тем самым обострить и дестабилизировать общественно-политическую ситуацию в целой стране. С этим явлением, как показывают события в мировой арене, справиться пока невозможно. Огромную роль флэш-моб сыграл в ряде североафриканских государств, на постсоветской территории и, конечно же, на Украине. Эта технология собирает огромные толпы, создает революционную ситуацию, вырабатывает четкую политическую позицию и умело скоординированные действия. Свою роль флэш-мобу еще предстоит сыграть в геополитическом противоборстве в Европе, Азии и на других континентах.

8. Одним из видов технологий информационно-психологического воздействия является нейролингвистическое программирование (НЛП), подбор «ключа» к подсознанию человека. В качестве такого «ключа» используется специально подобранный нейросемантический гипертекст с наиболее значимыми словами и фразами для суггестируемого лица. Областью применения НЛП являются средства массовой информации, система образования, медицина, торговля, реклама. С помощью нейролингвистического программирования осуществляется воздействие на эмоции человека для искусственного формирования представлений, побуждений, установок посредством образов и воображения. Манипулирование такими образами позволяет произвести в сфере подсознания человека локальные операции, направленные на изменение его представлений, взглядов, привычек и, в конечном итоге, — трансформации национального сознания.

9. К числу информационно-психологических операций относится и психотронное (парапсихологическое, экстрасенсорное) воздействие, предполагающее коррекцию поведения людей путем передачи информации через неосознаваемое восприятие. Так, широко известны факты применения американскими войсками акустического воздействия на психофизическое состояние человека, вызывающего головокружение, слуховые галлюцинации, под влиянием которых объект совершает неконтролируемые поступки.

В последнее время в геополитических целях стало практиковаться психотропное манипулирование психикой с помощью психотропных вирусов, медицинских препаратов, химических, биологических веществ. Они способны контролировать, усиливать или подавлять агрессивное поведение человека, разрушать его психику. При этом могут быть

использованы различные цвета, запахи, оказывающие сильное воздействие на психику человека [1].

Современные методы и средства информационно-психологического воздействия взаимосвязаны и рассчитаны на формирование новых психических мотивов, ценностей, стереотипов, на модификацию психических процессов и состояний. С помощью информационно-психологических операций достигается цель интенсивного воздействия на различные геополитические процессы, протекающие на уровне общественно-государственного устройства в любой стране в любом регионе мира. Политическая элита, не осознающая смысла ведущихся против нее информационно-психологических операций, обречена на поражение. Поэтому сегодня важнейшая задача является — дать достойный ответ на эти вызовы и угрозы. Не случайно Л. Г. Ивашов подчеркивает: «Для того, чтобы проводить мирную политику, нужно иметь силу, в том числе и мощные информационные «войска» [2]. В России должны быть институты, штабы, которые планируют информационно-психологические операции, отрабатывают теорию и технологию психологической войны.

---

[1] *Токсоналиева Р. М.* Современные технологии информационно-психологического воздействия // Вестник Кыргыз.-рос. славянского ун-та. 2016. Том 16. № 6. С. 172–175.

[2] *Ивашов Л. Г.* Доктрина информационной безопасности. URL: http://www.publikatsii.ru/stats/10889-doktrina-informacionnoy-bezopasnosti-leonid-ivashov.html.

Глава 5. Идеологическая граница: сущность и специфика

Главным объектом изучения для геополитической науки является взаимосвязь пространства и социума.

Классическая геополитическая наука полагала пространством лишь географические реалии. В таком случае основным актором освоения пространства неизменно оказывается государство, а наиболее распространенная технология пространственного расширения (экспансии) — это силовой захват с использованием регулярных вооруженных сил. В рамках географического пространства граница является условной линией территориального соприкосновения государств, которая закрепляется юридически и охраняется с помощью военной силы.

Со второй половины XX в., в связи с общецивилизационным переходом к постиндустриальному обществу, в типологию геополитических пространств наряду с географическим пространством (суша, море, воздух, космос) вошли экономическое, информационно-кибернетическое и информационно-идеологическое пространства. Новые пространства по преимуществу осваиваются так называемыми «новыми акторами», т. е. структурами негосударственной природы — экономическими, кибернетическими и медиа-корпорациями. Необходимо отметить, что новые пространства — это и новое качество границ. Постклассическая геополитика, выделяя нетрадиционные типы пространств, меняет и традиционное понимание границы. Это не только географическая (территориальная), но шире — пространственная граница, качество и способы защиты которой меняются в зависимости от специфики соответствующего типа геополитического пространства. Возникает

понятие нетерриториальной границы: экономической, информационно-кибернетической и информационно-идеологической.

В рамках постклассической геополитической парадигмы границу можно обозначить как предел допустимого проникновения во все виды пространств некоего актора государственной или негосударственной природы. Следовательно, в идеологическом пространстве также существуют границы, а сущность и технологии защиты идеологических границ различаются в зависимости от того, какова природа как самого по себе идеологического пространства, так и геополитического актора, который идеологические границы формирует и защищает.

По нашему мнению, идеологическое пространство определенного общества представляет собой систему ментальных ценностей данного общества. Эта система частично оформлена теоретически, концептуально, а частично существует в «дисперсной» форме внешне разрозненных, несистемных ценностей массового сознания. Соотношение концептов и дисперсных форм в идеологическом пространстве данного конкретного общества в разные периоды его развития различно и определяется совокупностью факторов объективного и субъективного порядка.

В таком случае идеологическая граница общества — это степень допустимого проникновения в его идеологическое пространство. Допустимым же проникновением является воздействие на массовое сознание данного общества оформленных теоретических концептов или дисперсных форм ценностей другого общества, не разрушающее существующую в данном обществе систему ментальных ценностей. Разрушительное воздействие, тем более имеющее целенаправленный характер, представляет собой информационно-идеологическую агрессию, т. е. акт войны.

В любой системе, в том числе в системе ментальных ценностей, существуют ключевые элементы, «краеугольные камни», разрушение которых является фатальным для системы в целом. Информационно-идеологическая агрессия (война) направлена именно на ликвидацию и замещение базовых ментальных ценностей общества-противника как «краеугольных камней» структуры его идеологического пространства.

Представляется, что для любого типа геополитических пространств существует два основных способа контроля: панельный (сплошной) и точечный, при использовании которого достаточно контролировать лишь ключевые точки пространства, определяющие его качество. Точечный контроль позволяет значительно экономить силы и средства актора-экспансиониста. Оптимальным является сочетание панельного

и точечного контроля пространств. Применение того или иного метода контроля зависит от конкретной геополитической обстановки, типа геополитического пространства и реальных возможностей данного геополитического актора.

В географическом пространстве положение таково, что чем больше объемы контролируемой территории, тем меньше шансов на успех панельного контроля. Недаром любая попытка создания всемирной территориальной империи заканчивалась крахом.

В идеологическом пространстве положение иное. Здесь панельный контроль возможен и обеспечивается замещением базовых ценностей данного общества на иные, не являющиеся для него автохтонными. Таким образом, контроль «ключевых точек» идеологического пространства (точечный контроль) является в равной мере контролем панельным, поскольку базовые ценности массового сознания являются системообразующими.

Думается, что ключевых точек идеологического пространства не так уж много. Это, прежде всего, признание ценности семьи, почитание предков (одобрение генерального хода истории данного общества), уважение к государству и его официальной идеологии, догматы доминантной религии. Совокупность ментальных приоритетов массового сознания и составляет идеологическую границу общества. Указанные ценности, сложенные в систему, предопределяют устойчивость общества к испытаниям, его ментальную выживаемость, поскольку именно они обеспечивают адекватную социальную самоидентификацию как на уровне массового, так и на уровне индивидуального сознания.

Важность ментальных приоритетов, или ментальной доминанты, состоит в том, что они определяют форму и степень осознания национального интереса как обществом в целом, так и его политической элитой. Временная утрата ментальной доминанты ведет к геополитической дезориентации общества до момента обретения им другой доминанты и может явиться одной из причин геополитического сжатия данного государства. Ментальные ресурсы — это то самое «пространственное чувство» народа [1], без развития которого не может осуществляться геополитическая экспансия.

Идеологическая граница общества создается, сохраняется и укрепляется благодаря деятельности акторов как государственной, так и негосударственной природы. Это прежде всего СМИ, учреждения культуры, а также такие социальные институты, как искусство, литература, спорт высоких

[1] Термин введен в научный оборот «отцом» геополитики Ф. Ратцелем.

достижений. В либерально-рыночном обществе негосударственные акторы играют более значительную роль, чем акторы государственной природы. Государство, во-первых, не может осуществлять панельный контроль сфер материального и духовного производства, а во-вторых, мелкий и средний капитал гораздо активнее, чем государственные структуры, осваивает рынки любого рода, в том числе и рынок идеологический, базирующийся на функционировании символического капитала.

По нашему мнению, только в географическом пространстве понятие границы связано исключительно с государством как актором ее формирования и защиты. Государственная граница — внешнее оформление притязаний органов политической власти на определенную территорию. Государственная граница и есть граница данного общества в географическом пространстве, они тождественны. Внутри государства, имеющего территориально-административное деление, существуют также и внутренние, административные, границы.

В негеографических пространствах существует не одна, а две внешних границы: граница общества и граница государства. Количество и качество внутренних границ зависит от числа и совокупной мощи соответствующих негосударственных акторов (например, глобальных корпораций). Нарушение внутренней границы, если оно отслеживается и осознается данным негосударственным актором, воспринимается им как акт агрессии и даже войны. Известны так называемые экономические войны: «стальные», «рыбные» и т. п. — за контроль определенного сектора мирового или внутригосударственного рынка. Примером идеологических войн являются избирательные кампании с применением так называемого «черного пиара».

Идеологическая граница ***общества*** не тождественна идеологической границе государства.

Идеологическая граница государства, по нашему мнению, это совокупность ментальных приоритетов массового сознания, обеспечивающих поддержку большинства избирателей в процессе формирования выборных органов государственной власти и лояльность подвластных ко всем трем ветвям государственной власти в период между выборами.

Состояние идеологической границы общества и государства влияет на состояние экономической и географической границы — и наоборот. Так, распространение в России среди населения некоторых этнических республик идеологии пантюркизма и панисламизма приводит к возникновению идеологических конструкций типа «Волга — священная река мусульманской цивилизации» или «Волга — последняя надежда ислама».

Панмонголоизм используется в качестве ментальной базы геополитической экспансии Японии в географическом пространстве. Среди японской университетской элиты звучат призывы возвратить Бурятии название Бурят–Монголия и восстановить государственное единство всех ветвей монгольского народа: Бурятии, Внутренней Монголии и бывшей Монгольской Народной Республики. Утверждается, что монголы — это ближайшие этнические родственники японцев, поэтому конечный результат объединения монгольских народов — воссоединение их с Японией. Для достижения этой цели Япония должна увеличить помощь монголоязычному населению в азиатских странах и России.

Понятие идеологической границы тесно связано с понятием идеологической мощи, т. к. именно идеологическая мощь данного общества и государства во многом определяет состояние его идеологической границы.

Мощь, по нашему мнению, это интегральное понятие, обозначающее конкурентные возможности данного государства в геополитической борьбе, т. е. его реальную способность к геополитическому расширению во всех пространствах.

В классической геополитике понятие «мощь» практически было равнозначно понятию «военная сила», поскольку основным средством геополитического расширения классическая геополитика считала силовой захват. Постклассическая геополитика применяет понятия «экономическая мощь», «информационно-кибернетическая мощь» и «информационно-идеологическая мощь». Военная, экономическая и информационная мощь являются самостоятельными факторами геополитического существования конкретного государства, но также каждая из них стимулирует развитие других и взаимодействует с ними. К примеру, необходимость создания новых, более эффективных видов оружия всегда стимулировала развитие определенных отраслей экономики, а начиная с XX в. — и развитие информационных технологий.

Идеологическую мощь можно определить как реальную способность геополитического актора к экспансии в ментальном пространстве.

В качестве элементов идеологической мощи можно выделить следующее:

- идеология, признаваемая (реже — имеющая юридический статус) официальной идеологией данного актора;
- ценности традиционной культуры общества, геополитическим актором которого выступает государство или негосударственная структура (в т. ч., такие ценности, как национальный характер и традиционный образ жизни);

- достижения науки, искусства и литературы;
- спортивные достижения.

Искусство, литература и спорт отражают национальный характер и традиционный образ жизни и потому являются элементами идеологической мощи.

Экспансия в ментальном пространстве имеет две основные формы:

- экспансия управляемая, когда государство стремится использовать престиж и достижения определенного вида искусства, литературы, спорта для укрепления своего собственного престижа;
- экспансия неуправляемая, т. е. самостоятельное проникновение учреждений культуры и спорта, а также отдельных выдающихся деятелей искусства, литературы, спорта в ментальное пространство иных обществ. Конечно, неуправляемая экспансия также работает на престиж того или иного государства, но ее источник иной, несмотря на одно и то же качество результата.

Одной из наиболее действенных и распространенных форм проявления идеологической мощи и осуществления экспансии в ментальном пространстве является создание и распространение мифов как с положительным, так и с отрицательным когнитивным смыслом.

Мифы с отрицательным когнитивным смыслом используются для разрушения идеологического пространства геополитического противника и для ослабления его ментальной сопротивляемости. Например, миф об изначальной лености и беспробудном пьянстве русского народа, о его якобы повальной тяге к воровству и иждивенчеству служит ментальному разрушению и ослаблению русских как этноса-носителя российской государственности. Этот миф также порождает недоверие и презрение к русским как со стороны других этносов России, так и со стороны этносов государств — геополитических союзников России, и таким образом способствует ослаблению Российской Федерации.

Мифы создаются различными средствами. Одно из наиболее действенных — искусство. Искусство соединяет рациональный и эмоциональный моменты восприятия мира человеком. Именно эмоциональная составляющая делает мифы, создаваемые или отражаемые деятелями искусства, частью как индивидуального и массового сознания, так и сферы индивидуального и коллективного бессознательного. Искусство — средство выражения и формирования национального характера, через создание мифов в том числе. Оно напрямую влияет на развитие «пространственного чувства» народа, выражая его в образно-эмоциональной форме. Управляемая экспансия в ментальном пространстве осуществляется

преимущественно посредством поощрения деятельности создателей мифов.

В мире Постмодерна технологии формирования сознания упрощаются и удешевляются до такой степени, что они становятся практически общедоступными. Благодаря присущим эпохе Постмодерна информационным технологиям, наиболее эффективным родом деятельности стало преобразование человеческого сознания: индивидуального, группового и массового. Причем этим видом деятельности может заниматься не только государство, но и негосударственные акторы, и даже отдельный индивид (через Интернет), что ведет к формированию системы глобальных рисков.

Идеологическая мощь — полноправный компонент современных войн. Перевес получает та сторона, которая имеет возможность довести до мирового сообщества сведения о вооруженном конфликте под выгодным для себя углом зрения. В частности, вооруженные конфликты, вызванные сепаратистскими устремлениями, могут длиться десятилетиями, в том числе и по той причине, что сепаратисты умело применяют психологический террор и давление на мировое общественное мнение посредством СМИ. Напомним в связи с этим, что российское государство начала 90-х гг. XX в. проиграло идеологическую борьбу с чеченскими сепаратистами, возглавлявшуюся «чеченским Геббельсом» М. Удуговым. В результате Россия вынуждена была фактически предоставить Чечне независимость по Хасавюртовским соглашениям.

Идеологическая мощь, как уже утверждалось выше, коррелирует с экономической мощью. Упадок экономической мощи обычно приводит к упадку идеологической мощи. Примером может служить распад СССР и мировой системы социализма. Экономический застой в странах социализма и неспособность выиграть экономическое соревнование «двух систем» продуцировали сомнение в ценностях коммунистической идеологии и образа жизни. Справедливости ради надо отметить, что экономическим провалам социализма не в последнюю очередь способствовала именно коммунистическая идеология с ее догмами планового централизованного хозяйства.

Информационно-психологические войны велись на протяжении всего XX в., но с приходом к власти в США президента Р. Рейгана информационно-идеологическое воздействие стало принципиально иным: началась эра глобальной борьбы за сознание целых народов с использованием новейших информационно-психологических технологий на основе координации деятельности всех государственных структур и спецслужб США. При Рейгане государственные органы стали в возрастающей степени использоваться

в качестве координационных и направляющих центров информационно-психологического воздействия. Центральную роль в процессе стратегического анализа и координации деятельности информационно-психологических структур США приобрел Совет национальной безопасности.

Во второй половине XX в. информационные (идеологические) воздействия способны изменить главный геополитический потенциал государства: национальный менталитет, культуру и моральное состояние людей. Тем самым вопрос о роли символического капитала в геополитическом процессе приобрел стратегическое значение. Национальная психология в современном мире может незаметным для нации образом изменяться ее геополитическими противниками. Итак, с 80-х годов XX в. задача защиты идеологических границ государства и общества стала выходить на передний план в структуре деятельности по обеспечению национальной безопасности.

Защита идеологической границы, в отличие от защиты границы географической, является исключительной функцией элиты: как элиты политической, так и элит в сфере науки, культуры и образования. Угрозы для ментальной безопасности общества и государства могут быть осознаны только на уровне социальных групп, обладающих для этого соответствующими знаниями и квалификацией. В «горячих» войнах [1], которые ведутся исключительно в географическом пространстве, основным комбатантом является народ. Ресурсы географического пространства — природные (сырье, территория), природно-социальные (народонаселение) — материальны, наглядны, и возможность их утраты воспринимается как угроза для физического выживания общества. В таких обстоятельствах, при наличии материальной, видимой угрозы, народ быстро психологически мобилизуется на ее отражение. Для осуществления отпора врагу в материальной форме ему только нужно адекватное данной угрозе лидерство со стороны политической элиты данного общества. Таковое, как правило, и обретается под давлением общественного мнения извне и изнутри элиты, испытывающей примерно те же эмерджентные эмоции (назначение Кутузова вместо Барклая де Толли, выдвижение Рокоссовского и Жукова для руководства ключевыми фронтами Великой Отечественной войны).

[1] «Горячая» война — тип геополитического противостояния государств, основным содержанием которого является вооруженная борьба за стратегическое доминирование в географическом пространстве на региональном или глобальном уровне. Противостояние глобального уровня носит название «мировая война», регионального — «локальная война».

В войнах, называемых «холодными», преобладают угрозы и разрушающие воздействия психолого-идеологического и экономического характера, в значительной степени скрытые от массового сознания. То, что реально представляет собой угрозу существованию данного общества как целостной экономической, социально-психологической и идеологической системы, под влиянием пропаганды противника по большей части воспринимается массовым сознанием как возможность освобождения от определенных социальных комплексов: несвободы, бедности и т. п., т. е. как социальное благо. Основным оружием «холодных войн» являются не пушки, а интеллектуальные и социально-психологические аберрации, «социальные перевертыши», создаваемые в процессе подрывной пропагандистской деятельности, направленной на разрушение и замещение базовых ментальных ценностей данного общества. В связи с этим функция выявления и ликвидации угроз разрушительного характера в идеологическом пространстве принадлежит главным образом элите, поскольку именно она имплицитно обладает соответствующим образованием, квалификацией и опытом, позволяющим отличить социальную угрозу от социального блага. Необходима также патриотическая мотивация действий элиты для противостояния неизбежным попыткам ее разложения, предпринимаемым извне.

Нужно отметить, что любое общество имеет как достоинства, так и недостатки развития. В данном случае под достоинствами подразумеваются адекватные ответы на вызовы времени, под недостатками — неадекватность реагирования на требования цивилизационного мейнстрима. Агрессоры, инициирующие «холодную войну» в отношении противостоящего центра силы, стремятся всемерно усилить и проявить для массового сознания главным образом недостатки и затушевать или вообще свести на нет достоинства развития общества-противника. Но само наличие, «количество и качество» недостатков, на базе которых и образуются социально-психологические комплексы массового сознания, конечно, в значительной мере зависит от качества управления данным обществом. Стратегию развития общества определяет его политическая элита, особенно если это общество так называемого альтернативного Модерна, каковым и являлось советское общество. К основным характеристикам альтернативного Модерна принадлежат централизованная директивная экономика, авторитарный политический режим и отсутствие контроля над государством со стороны гражданского общества. В обществах альтернативного Модерна преобладает общественная (государственная) собственность, что делает политическую элиту не только основным

реальным собственником-распорядителем львиной доли общественного богатства, но и возлагает на нее исключительную ответственность за результаты управления обществом, ведь реального противовеса ей в виде действенной политической оппозиции нет. Являясь по сути дела единственным актором в экономическом и информационно-идеологическом пространстве общества альтернативного Модерна, политическая элита, в том числе, имплицитно берет на себя и исключительную функцию защиты данных пространств, что делает ее также фактически единственным комбатантом в экономическом и психолого-идеологическом противостоянии с либеральными обществами «прямого» Модерна. Отсутствие системного гражданского общества отнимает у людей возможность структурированного социального действия. Это, в свою очередь, не дает возможности канализировать импульсы реального недовольства или негативных социально-политических предчувствий, существующих в обществе, и предъявить их политической элите в качестве социального аргумента для необходимого изменения стратегии и тактики общественного развития. Данный фактор становится фатальным в случае информационной войны, факт ведения и структуру которой невозможно распознать на уровне массового сознания. Если же политическая элита общества, ставшего объектом информационной войны, не имеет достаточной квалификации для выявления агрессии этого рода и организации адекватного отпора, то такое общество обречено на сокрушительное геополитическое поражение, что и произошло с СССР. Таким образом, идеологическая граница государства и общества проходит в глубине как массового, так и индивидуального сознания, а ее защитники — это, прежде всего, гуманитарии, создающие и сохраняющие ментальные ценности, а также представители политической элиты, непосредственно занятые формированием и отстаиванием положительного имиджа данного государства и общества.

Раздел II.
Информационные угрозы и информационно-психологическая безопасность в глобальном измерении

Глава 1. Четвертая промышленная революция и глобальная геополитика — вызовы глобальной безопасности

Влияние новой промышленной революции на формирование полицентричного мироустройства. В истории индустриальной цивилизации принято выделять четыре сменяемые друг друга промышленные революции и соответствующие им технологические уклады (табл. 2):

Таблица 2

Век	Промышленная революция	Технологический уклад
XVIII	1-я	механизация производства на основе теплоэнергетики
XIX	2-я	механизация производства на основе электроэнергетики
XX	3-я	автоматизация производства на основе информатики
XXI	4-я	«технологии сливаются и границы материального, цифрового и биологического миров стираются» (К. Шваб)

Первая и вторая промышленные революции характеризовались односторонней структурно-функциональной зависимостью между сферой материального производства и другими сферами человеческого бытия (социальной, политической, духовной): «Способ производства материальной жизни обусловливает социальный, политический и духовный процессы жизни вообще» [1]. Структура материального производства

[1] *Маркс К.* К критике политической экономии. Предисловие // Маркс К., Энгельс Ф. Соч. М.: Политиздат, 1959. Т. 13. С. 7.

определялась формирующейся системой машин — энергетических, транспортных, обрабатывающих и информационно-управляющих. В свою очередь, функции материального производства получали воплощение в создании различного рода механических, электрофизических и электрохимических и др. технологий. Но тогда же стала формироваться и своеобразная обратная связь, заключающаяся в воздействии духовной деятельности на материальное производство. Это, как доказал К. Маркс, проявилось в процессе превращения науки в непосредственно производительную силу общества: «Природа не строит ни машин, ни локомотивов, ни железных дорог, ни электрического телеграфа, ни сельфакторов и т. д. Все это — продукты человеческого труда, природный материал, превращенный в органы человеческой воли, властвующей над природой, или человеческой деятельности в природе. Все это — *созданные человеческой рукой органы человеческого мозга*, овеществленная сила знания. Развитие основного капитала является показателем того, до какой степени всеобщее общественное знание [Wissen, knowledge] стало *непосредственно производительной силой*, и отсюда — показателем того, до какой степени условия самого́ общественного жизненного процесса подчинены контролю всеобщего интеллекта и преобразованы в соответствии с ним; до какой степени общественные производительные силы созданы не только в форме знания, но и как непосредственные органы общественной практики, реального жизненного процесса» [2]. В свое время эти слова К. Маркса трактовались применительно к анализу процесса становления науки как непосредственно производительной силы специфически капиталистического способа производства. В контексте наших рассуждений хотелось бы подчеркнуть, что из «всеобщего общественного знания» именно научное знание, могущее быть овеществленным непосредственно в средствах труда, противопоставляется живому труду как сила капитала. При этом живому труду по-прежнему принадлежит всеобщее общественное знание в широком смысле, но ему противопоставляется систематизированное научное знание, овеществленное в технических средствах, технологии, методах организации производства [3]. Присущее науке имманентное свойство выступать силой капитала воплотилось в создании не только производственной техники, но и техники военной, в том числе предназначенной для совершения операций в информационной

[2] *Маркс К.* Экономические рукописи 1857–1861 гг. (Первоначальный вариант «Капитала»). В 2-х ч. Ч. 2. М.: Политиздат, 1980. С. 217.

[3] *Кефели И. Ф.* Автоматизация: методологические и социальные проблемы. Л.: Изд-во ЛГУ, 1987. С. 59–61.

сфере. Наука, будучи «всеобщим духовным продуктом общественного развития», создает прибавочную стоимость, поскольку она, — по меткому замечанию Маркса, — «выступает здесь как нечто непосредственно *включенное в* капитал (а применение ее как науки, отделенной от знаний и умения отдельного рабочего, в процессе материального производства проистекает только из *общественной* формы труда), как силы природы как таковые и как природные силы самого́ *общественного* труда» [1]. Так на протяжении первых двух промышленных революций наука в статусе «непосредственно производительной силы» была включена в систему капиталистического способа производства и тем самым обеспечивала его устойчивость, несмотря на многочисленные социальные и политические перевороты.

С тех пор промышленно развитые страны стали выступать центрами экономического и военного могущества, генератором которого стал растущий потенциал естественных, технических и гуманитарных наук. Рэй Клайн еще в середине 70-х гг. XX в. определял военное могущество как основу национальной мощи государства, которая, в свою очередь, представляет собой совокупность материальных и военно-политических факторов влияния и властвования за пределами национальных границ. В мировой политике национальная мощь государства представляется ее лидерами, военно-политическим руководством. Именно это руководство утверждает и претворяет в жизнь стратегические цели государства на перспективу. Клайн предложил рассматривать национальную мощь государства следующим образом: $\boldsymbol{P} = (\boldsymbol{C} + \boldsymbol{E} + \boldsymbol{M}) \times (\boldsymbol{S} + \boldsymbol{W})$, где: $\boldsymbol{P}$ — воспринимаемая национальная мощь государства; $\boldsymbol{C}$ — «критическая масса», определяемая отношением численности населения государства к величине его территории; $\boldsymbol{E}$ — экономический потенциал государства; $\boldsymbol{M}$ — военный потенциал государства; **S** — стратегические цели; $\boldsymbol{W}$ — политическая воля к реализации национальной стратегии. В своей совокупности $(\boldsymbol{C} + \boldsymbol{E} + \boldsymbol{M})$ означает «мощь государства», а $(\boldsymbol{S} + \boldsymbol{W})$ — «обязательства государства» [2]. Общая формула расчета геополитического статуса имеет следующий вид:

$$\boldsymbol{S(t) = FA(t) \cdot G(t)}, \text{ где:}$$

$\boldsymbol{S(t)}$ — статус в определенный период времени $\boldsymbol{t}$;

[1] *Маркс К.* Экономическая рукопись 1861–1863 годов // Маркс К., Энгельс Ф. Соч. Т. 48. М.: Политиздат, 1980. С. 39.

[2] *Cline R. S.* World power assessment: a calculus of strategic drift. Boulder: Westview Press, 1977. P. 34.

FA — «функция влияния» указанных выше факторов, не связанных непосредственно с геополитическим потенциалом;

G(t) — геополитический потенциал, значение которого определяется по следующей формуле:

$$G(t) = 0,5\left(1 + X_M^{0,43}\right) X_T^{0,11} \cdot X_D^{0,19} \cdot X_E^{0,27}, \text{ где}$$

X_i ***(i = T, D, E, M)*** — доли государства в общемировых показателях соответственно в территориальной, демографической, экономической и военной сферах.

В случае признания целью государства повышения своего геополитического статуса величина ***S(t)*** может быть использована в качестве целевой функции при стратегическом планировании внешней политики государства[3]. Данные для расчета геополитического статуса по приведенным выше формулам следует брать, исходя из сопоставления численности населения и вооруженных сил, места государств в мировых рейтингах, данных по ВВП отдельных блоков и стран мира. Геополитический статус государства определяется состоянием его транспортной инфраструктуры, которая развивается в соответствии с определенными геополитическими закономерностями.

Приведенная выше аналитика геополитического потенциала и геополитического статуса государства применима и к межгосударственным союзам и при прогнозировании геополитических сдвигов и потрясений в 2012–2025 гг. В этот период с большой вероятностью предполагается осуществление в ряде промышленно развитых стран, в т. ч. и в России, коренных экономических, политических и социальных реформ.

Вопрос о влиянии новой промышленной революции на формирование полицентричного мироустройства следует рассматривать именно в контексте анализа геополитических статусов как отдельных государств, так и коалиций государств, выступающих в качестве самостоятельных акторов мировой политики. В данном случае отдельные компоненты новой промышленной революции оказывают мультипликативное влияние на составляющие геополитического потенциала этих акторов ***T, D, E*** и ***M***.

О наступлении четвертой промышленной революции заявил Клаус Шваб на экономическом форуме в Давосе в январе 2016 г. Рассмотрим кратко ход его рассуждений:

---

[3] *Винокуров Г. Н., Коняхин Б. А., Подкорытов Ю. А.* Геополитический статус Китая как фактор российской политики ядерного сдерживания Соединенных Штатов // Стратегическая стабильность. 2008. № 2. С. 49–53.

— отличительной особенностью этой революции является постепенное стирание граней между физической, цифровой и биологической сферами;
— она, по сравнению с промышленными революциями прошлых лет, развивается по экспоненте, а не линейно, затрагивает практически все сферы жизни во всех странах и предвещает трансформацию всей системы производства, управления и руководства;
— имущественное неравенство, будучи наиболее важным экономическим показателем, начинает устойчиво ассоциироваться с Четвертой промышленной революцией;
— революция существенным образом изменит саму систему национальной и международной безопасности, оказывая влияние на природу конфликтов и их виды, поскольку «современные межгосударственные конфликты все чаще являются гибридными по своей природе, совмещая боевые действия на поле боя с элементами, которые ранее рассматривались как негосударственные. Граница между войной и миром, военнослужащим и гражданским, и даже между насилием и ненасилием становится пугающе нечеткой»;
— революции в биотехнологиях и искусственном интеллекте заставят нас переосмыслить само понятие человека;
— мы «должны направить Четвертую промышленную революцию в то русло, которое отвечает нашим общим целям и ценностям. Чтобы это сделать, нам необходимо выработать глобальную систему взглядов на то, как технологии влияют на нашу жизнь, экономику, общество, культуру и человека» [1].

Итак, вопрос о влиянии Четвертой промышленной революции на формирование полицентричного мироустройства необходимо анализировать, опираясь, в первую очередь, на математическую геополитику (коалиционное взаимодействие акторов полицентричного мира) и глобальную технологию преобразования реального и виртуального миров.

Геополитический ракурс информационно-психологического противоборства в киберпространстве. Философское осмысление геополитического знания о путях формирования полицентричного мироустройства не может обойти стороной процессы информационно-психологического противоборства в киберпространстве, возникновение которых обусловлено переходом к новому технологическому укладу. Так, еще в 1954 г.

---

[1] *Клаус Шваб*. Четвертая промышленная революция: Что она собой представляет и как на нее реагировать // Геополитика и безопасность. 2016. № 1(33). С. 122–126.

Поль Лайнбарджер (1913–1966), американский специалист-психолог, разведчик, консультант Пентагона по организации подрывной пропаганды, в книге «Психологическая война» вполне откровенно заявил следующее: «Психологическая война не является каким-то волшебным средством. Это вспомогательное оружие современной войны и полезная составная часть современной стратегии. Если определенный политический курс разработан достаточно разумно и служит действенным средством сдерживания войны, то мероприятия психологической войны, подкрепляющие эту стратегию, также будут служить делу предотвращения войны… Психологическая война своим оружием стремится привлечь на свою сторону живого солдата противника, чтобы затем отпустить его домой как своего друга. Никакое другое оружие не обладает подобными свойствами»[2]. Стоит обратить внимание на весьма «скромное» замечание: психологическая война привлекает противника, который становится другом организатора этой самой психологической войны, вернувшись домой. По сути дела, психологическая война той поры сводилась к самой изощренной пропаганде, основанной на лжи и дезинформации, разжигании межнациональной и межконфессиональной вражды, манипуляции общественным сознанием и идеологических диверсиях.

Томас Рона в 1976 г. ввел в научный оборот военных аналитиков термин «информационная война»[3], тем самым положив начало «оцифровке» методов и способов ведения психологической войны, прежде носившей преимущественно пропагандистский характер. Информация стала посредником в субъект-объектных отношениях в военных действиях, орудием стратегического информационного противоборства. Пожалуй, первые формулировки принципов борьбы с системами управления в качестве орудия стратегического информационного противоборства в военной области можно найти в разработанной и введенной в действие в 1996 г. министерством обороны США «Доктрине борьбы с системами управления». Принципы эти сводятся к совместному использованию «приемов и методов

---

[2] *Лайнбарджер П.* Психологическая война. М.: Военное издательство МО СССР, 1962. С. 335–336. Следует отметить, что в 2013 г. книга П. Лайнбарджера была переиздана: *Лайнбарджер П.* Психологическая война. Теория и практика обработки массового сознания. М.: Центрполиграф, 2013. 445 с.

[3] *Thomas P. Rona.* Weapon Systems and Information War / Office of the secretary of defense Washington DS. Yar. Boeing Aerospace Company Seattle, Washington 98124. 1 July 1976. P. 31. URL: http://www.dod.mil/pubs/foi/Reading_Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf.

безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также воспрепятствование противнику делать то же самое» [1]. От доктрины борьбы с системами управления к признанию разделения театра военных действий на две составляющие — традиционное пространство (земля, вода, воздух и ближний космос) и киберпространство — всего один шаг. Совершая его, полковник ВВС США Дж. Уорден разработал концепцию «пяти колец», согласно которой целями воздействия выступают следующие объекты противника, выбираемые по степени важности: в центре — политическое руководство, затем следуют система жизнеобеспечения; социальная и техногенная инфраструктура; гражданское население и, в последнюю очередь, вооруженные силы. Поскольку воздействие на указанные объекты осуществляется с помощью сетевых технологий и методов, такое противоборство получило название «гибридная война», основой которой является массированное воздействие на морально-психологическое состояние руководства и населения страны-противника.

Итак, пятым измерением войны выступает киберпространство (глобальное информационное пространство) как ключевое звено гибридной войны (hybrid warfare).В киберпространстве используются военные и невоенные инструменты в «интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, использующих дипломатические возможности; масштабные и стремительные информационные, электронные и кибероперации; прикрытие и сокрытие военных и разведывательных действий; в сочетании с экономическим давлением» [2]. Более того, гибридная война по своей сути носит глобальный характер — цивилизационный и геополитический, представляя собой череду конфликтов, в которых противник способен применять одновременно все способы ведения войны, соединяя их «для удовлетворения собственных стратегических

---

[1] Joint Pub 3–13.1. Joint Doctrine for Command and Control. Warfare (C2W). 7 February 1996. URL: http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf.

[2] Игорь Панарин: Гладиаторы гибридной войны // Экономические стратегии. 2016. № 2. URL: URL: http://www.nooov.ru/statya/statya-igor-panarin-gladiatory-gibridnoj-vojny.

культурных и географических целей» [3]. Начало XXI века ознаменовалось растущей интенсивностью кибератак и их выходом за пределы сферы ведения разведывательной деятельности. Киберпространство становится доступным для ведения боевых действий — наравне с землей, морем, воздухом и космосом [4]. Киберпространство — пятое измерение войн глобального масштаба — заключает в себе предпосылки как информационных боевых операций, так и информационной безопасности, которые «опредмечиваются»:

— в технико-технологических и организационных средствах ее обеспечения;
— в инновационном тренде расширения пространства ведения боевых действий;
— в национальных военных и оборонных доктринах и стратегиях.

Кибервойна (точнее, операции в киберпространстве, проводимые в ходе войны, а в мирное время — это диверсии, теракты, идеологическая обработка гражданского населения) является одним из магистральных направлений революции в военном деле, приведшим к появлению гибридных войн (их еще называют многомерными нелинейными войнами). Современное и перспективное кибероружие, используемое в гибридных войнах, подразделяется на пять основных групп:

— ***сетевое кибероружие***, обеспечивающее доступ многофункциональных компьютерных программ в закрытые внутренние военные и гражданские сети противника, включающие критические объекты;
— ***коммуникационное кибероружие***, которое представляет собой программный код, способный искажать и блокировать обмен сигналами между удаленным оператором и боевым роботом;
— ***предустановленное кибероружие***, в элементную базу которого производителем закладывается управляющий софт с различного рода «логическими бомбами», способными выводить из строя кибероружие под воздействием внешних сигналов;
— ***проникающее кибероружие***, базирующееся на целенаправленном изменении различных физических сред (акустической, оптической и др.), которое приводит к модификации сигналов, поступающих на внешние сенсорные датчики высокотехнологичных вооружений и приводящих к их выходу из строя;

---

[3] *Хоффман Ф. Г.* Гибридные угрозы: переосмысление изменяющегося характера современных конфликтов // Геополитика. Информ.-аналит. изд. Выпуск XXI. 2013. С. 45–62.

[4] Department of Defense Strategy for Operating in Cyberspace. July 2011 / US Department of Defense. URL: http://www.defense.gov/news/d20110714cyber.pdf.

— ***электромагнитное оружие***, полностью выводящее из строя в ходе превентивного удара боевую технику, «выжигая» элементную базу наступательного вооружения противника [1].

С полным основанием следует заявить о «шестом измерении» глобальной войны и глобальной безопасности в формате информационно-психологической войны и информационно-психологической безопасности. Если первые пять «измерений» определяют объектную сторону военной деятельности в различных физических средах окружающего мира, то «шестое измерение» охватывает внутренний мир человека, его инстинкты, психику, чувства, эмоции, мысли, мировоззрение, индивидуальное и общественное сознание. В гибридных войнах, с одной стороны, в полной мере используются организационные методы, технологии и средства информационно-психологического воздействия на личный состав и гражданское население противника, а с другой — информационно-психологические операции армии «сильных мира сего» нацелены на то, чтобы «дать урок» превосходства своих ценностей, силы, аппетитов всему остальному миру. Эти «уроки» буквально «вываливаются» на нас из всех СМИ. Недаром бывший министр обороны США Р. Гейтс как-то «изящно» заявил по поводу утверждения принципа глобального господства Америки: «Соединенные Штаты не могут позволить себе роскошь отказа от участия в конфликтах, потому что эти сценарии не соответствуют предпочтительным для Америки понятиям о войне».

Мы явно или неявно переживаем все детали информационно-психологических операций в реальном масштабе времени и только спустя какое-то время начинаем осмысливать их геополитические и социальные последствия. По прошествии многих лет люди начинают понимать, что прежнее их восприятие текущих событий было ложным, но изменить последствия этого уже невозможно («Но время шло, и старилось, и глохло», писал Б. Пастернак). Средства и технологии информационно-психологической войны, действующие и в мирное время, способны нанести противнику не меньший ущерб, чем средства вооруженного нападения, а информационное оружие, построенное на базе технологий психологического воздействия, обладает значительно большей поражающей, проникающей и избирательной способностью.

«Шестое измерение» глобальной войны и глобальной безопасности следует анализировать, по крайней мере, в двух аспектах — геополитическом и цивилизационном. В рамках глобальной геополитики

[1] *Ларина Е., Овчинский В.* http://topwar.ru/36839-pyatoe-izmerenie-voyny.html 04.12.2013.

информационно-психологическая война и информационно-психологическая безопасность предстают как две грани захватившего информационное пространство геополитического противоборства, для которого, как писал еще в 1964 году Г. Маклюэн, «земной шар теперь — не более чем деревня» [2]. Для цивилизационного подхода информационно-психологическая война и информационно-психологическая безопасность представляют научный интерес в той мере, в какой акторы цивилизационного противоборства (ими выступают в современном мире сложившиеся геоцивилизации — западная и славяно-православная, китайская и индская, арабо-мусульманская и тропически-африканская, латиноамериканская) смогут предложить символический капитал культуры, выражающий образ национальной или наднациональной (цивилизационной) идеи. Цивилизационный код, образцы материальной, духовной и социальной культуры каждого из этих акторов в первую очередь находятся под информационно-психологическим воздействием.

С точки зрения глобальной динамики развития процесс противоборства в информационно-психологической войне предстает разновидностью «большой» игры, в которой участвуют множество участников, ведущих борьбу за реализацию своих интересов, и, соответственно, может быть исследован с помощью теории игр. В таком случае мы должны ввести весь ход рассуждений о диалектической связи глобальной войны и глобальной безопасности шестого измерения в русло математической геополитики, одним из разделов которой, наряду с системным анализом и моделированием мировой динамики (А. А. Акаев, В. А. Садовничий и др.), является разработка игровых моделей в глобальной геополитике [3].

Выражая согласие с суждением И. А. Василенко относительно того, что в соответствии с новой информационной парадигмой судьба пространственных отношений между государствами все более определяется превосходством в киберпространстве, а в информационном противоборстве деформируется главный геополитический потенциал государства, т. е. упомянутый выше символический капитал культуры [4], следует отметить, во-первых, перспективность моделирования геополитической динамики на основе методов теории игр (в частности, теории кооперативных игр), а во-вторых — своевременность включения в геополитический дискурс

---

[2] *Маклюэн Г. М.* Понимание Медиа: Внешние расширения человека. М.; Жуковский: КАНОН-пресс-Ц, Кучково поле, 2003. С. 6.

[3] *Кефели И. Ф., Малафеев О. А.* Математические начала глобальной геополитики. СПб., 2013. 204 с.

[4] *Василенко И. А.* Геополитика современного мира. М.: Гардарики, 2006. С. 7–8.

представлений о глобальном информационном поле (пространстве), которое выступает не только сферой военного, но и информационно-психологического противостояния. Рассмотрим это подробнее.

Слово математической геополитике. Повторим сказанное выше, но более определенно: современная, глобальная геополитика характеризуется двумя особенностями. Во-первых, в ее недрах получает развитие информационная геополитика, утверждающая в своем развитии тезис о том, что главным геополитическим потенциалом государства (и коалиции государств) начинают выступать национальный менталитет, культура и моральное состояние людей, а императив «главного геополитического закона» — «тот, кто контролирует источники информации на данной территории, — тот контролирует и саму территорию» [1]. Вследствие этого мы должны признать, что весь комплекс проблем обеспечения информационно-психологической и когнитивной безопасности относится к предметному полю информационной геополитики. Во-вторых, стратегия конфликта, опирающаяся на математическую теорию игр, по сути своей инвертивна, т. е. выступает и как стратегия безопасности. Теория игр занимается изучением конфликтов, то есть ситуаций, в которых акторам необходимо выработать какое-либо решение, удовлетворяющее их всех. В теории кооперативных игр изучается круг вопросов об условиях и достижимых результатах взаимодействия акторов. Основными характеризующими признаками кооперативной игры как математической модели ситуации выступают:

1. Наличие нескольких акторов.
2. Неопределенность поведения акторов, связанная с наличием у каждого из них нескольких вариантов действий.
3. Различие (несовпадение) интересов акторов.
4. Взаимосвязанность поведения акторов, поскольку результат, получаемый каждым из них, зависит от поведения всех акторов.
5. Правила поведения, которым должны следовать все акторы.

Кооперативные игры относятся к классу игр с ненулевой суммой, в которых акторы принимают согласованные друг с другом решения и создают коалиции (частным условием кооперативных игр может быть отсутствие коалиций). Любая коалиция (союз государств) представляет собой объединение двух или более акторов кооперативной игры на основе определенных договорных обязательств (раздел выигрыша, обмен информацией и др.). Далее будем рассматривать игры с переменным составом

[1] Там же. С. 7, 73.

коалиций, что соответствует реальному положению дел. Примером тому служат растущий состав участников ЕАЭС, расширение круга задач участников ШОС (объединение ЕАЭС и «Экономического пояса Шелкового пути»), созревание качественно новых характеристик БРИКС — *ценностных*, предлагающих миру историческую альтернативу миропорядку эпохи холодной войны в виде модели, в равной степени привлекательной как для развивающихся, так и для развитых стран [2]. В каждом из этих случаев проблемы информационно-психологической и когнитивной безопасности должны рассматриваться в общем контексте информационной геополитики и теории игр.

Рассмотрим ряд конкретных примеров кооперативных игр, которые получаются в тех случаях, когда в игре n акторов разрешается образовывать определенные коалиции. Обозначим через N множество всех акторов, $N = \{1, 2, \ldots, n\}$, а через S любое его подмножество. Пусть акторы из S договариваются между собой о совместных действиях в формате одной коалиции. Очевидно, что число таких коалиций, состоящих из r акторов, равно числу сочетаний из n по r, т. е., а число всевозможных коалиций равно:

$$\sum_{r=1}^{n} C_n^r = 2^n - 1.$$

Из этой формулы следует, что число возможных коалиций растет в зависимости от числа всех акторов в данной игре. Для исследования этих игр необходимо учитывать все возможные коалиции, и поэтому трудности исследований возрастают с ростом n. Образовав коалицию, множество акторов S действует как один актор против всех остальных, и выигрыш этой коалиции зависит от применяемых стратегий каждым из n акторов.

Характеристической функцией игры называется функция υ, ставящая в соответствие каждой коалиции S наибольший, уверенно получаемый его выигрыш $\upsilon(S)$. Так, например, для бескоалиционной игры n акторов $\upsilon(S)$ может получиться, когда акторы из множества S оптимально действуют как один актор против остальных $N\backslash S$ акторов, образующих другую коалицию. Характеристическая функция υ называется *простой*, если она принимает только два значения: 0 и 1. Если характеристическая функция υ простая, то коалиции S, для которых

[2] *Давыдов В. М.* Миссия БРИКС в геополитическом пространстве XXI в. // Перспективы и стратегические приоритеты восхождения БРИКС. Научный доклад к VII саммиту БРИКС / Под ред. В. А. Садовничего, Ю. В. Яковца, А. А. Акаева. М.: МИСК–ИНЭС–НКИ БРИКС, 2014. С. 26–28.

$\upsilon(S) = 1$, называются *выигрывающими*, а коалиции S, для которых $\upsilon(S) = 0$, — *проигрывающими*. Если в простой характеристической функции υ выигрывающими являются только те коалиции, которые содержат фиксированную непустую коалицию R, то характеристическая функция υ, обозначаемая в этом случае через υ_R, называется *простейшей*. Для примера, простые характеристические функции возникают, например, в условиях голосования, когда коалиция является выигрывающей, если она собирает более половины голосов (простое большинство) или не менее двух третей голосов (квалифицированное большинство). Простейшая характеристическая функция появляется, когда в голосующем коллективе имеется некоторое «ядро», голосующее с соблюдением правила «вето», а голоса остальных участников оказываются несущественными.

После того как коалиции образованы, возникает вопрос: как делить общий выигрыш с учетом веса каждой коалиции между ее членами? В таком случае применяется принцип оптимальности в форме С-ядра, т. е. принципа оптимального распределения максимального выигрыша $\upsilon(S)$ между сторонами $i \in S$. Реализация этого принципа приводит к рассмотрению С-ядра, т. е. множества недоминируемых «вполне устойчивых» дележей кооперативной игры. Вектор $x = (x_1, \ldots, x_n)$, удовлетворяющий условиям индивидуальной и коллективной рациональности, называется *дележом* в условиях характеристической функции υ. Распределение выигрышей (дележ) акторов должно удовлетворять следующим условиям: если обозначить через x_i выигрыш i-го актора, то, во-первых, должно удовлетворяться условие *индивидуальной рациональности* $x_i \geq \upsilon(i)$, для $i \in N$, т. е. любой актор должен получить выигрыш в коалиции не меньше, чем он получил бы, не участвуя в ней (в противном случае он не будет участвовать в коалиции).

Во-вторых, должно удовлетворяться условие *коллективной рациональности* $\sum_{i \in N} X_i = \upsilon(N)$, т. е. сумма выигрышей акторов должна соответствовать возможностям (если сумма выигрышей всех акторов меньше, чем $\upsilon(N)$, то им незачем вступать в коалицию. Если же потребовать, чтобы сумма выигрышей была больше, чем $\upsilon(N)$, то это значит, что акторы должны делить между собой сумму большую, чем у них есть).

Наличие доминирования $x > y$ означает, что в множестве игроков N найдется коалиция, для которой x предпочтительнее y. Соотношение доминирования возможно не для всякой коалиции. Так, невозможно доминирование в коалиции, состоящей из одного актора или из всех акторов. Любой дележ из С-ядра устойчив, в том смысле, что ни одна из коалиций не имеет ни желания, ни возможности изменить исход игры. Для того чтобы дележ x принадлежал С-ядру кооперативной игры с характеристической функцией υ, необходимо и достаточно, чтобы для любой коалиции S выполнялось неравенство $\upsilon(S) \le \sum_{i \in S} x_i$. С-ядро может оказаться пустым, например, когда есть слишком сильные коалиции. Если С-ядро пусто, то требования всех коалиций одновременно не могут быть удовлетворены. В качестве примера можно рассмотреть ситуацию выбора С-ядра в кооперативной игре трех акторов, если максимальные гарантированные выигрыши всевозможных семи коалиций $\sum_{r=1}^{3} C_3^r = 7$ следующие:

$$\upsilon(1, 2, 3) = 9,\ \upsilon(2, 3) = 7,\ \upsilon(1, 3) = 4,\ \upsilon(1, 2) = 4,\ \upsilon(1) = \upsilon(2) = \upsilon(3) = 0.$$

Решение будет выглядеть следующим образом: воспользуемся утверждением, раскрывающим метод построения С-ядра как множества недоминируемых дележей, т. е. для того, чтобы дележ $x(S)$ принадлежал С-ядру, необходимо и достаточно выполнения неравенств:

$$\upsilon(S) \le \sum_{i \in S} x_i,$$

$$S \subset N,$$

где x_i — доля i-го актора; $i \in S$, должна соответствовать требованию:

$$\boldsymbol{x}_i \ge \upsilon(i),\ i = 1, 2, 3.$$

Оставляя в стороне математические расчеты, укажем на то, что в случае, когда какой-либо актор не является существенным, т. е. не принадлежит

коалиции S — носителю игры, возникает необходимость конструирования принципа оптимальности как принципа справедливого дележа. В этом случае необходимо применить подход Шепли, который формируется на основании аксиом, отражающих справедливость дележей. *Носителем игры* с характеристической функцией υ называется такая коалиция T, при которой $\upsilon(S) = \upsilon(S \cap T)$ для любой коалиции S. Назначение T заключается в том, что любой актор, не принадлежащий T, является нейтральным, он не может ничего внести в коалицию и ему ничего не следует выделять из общих средств.

Пусть υ — характеристическая функция кооперативной игры n акторов, π — любая перестановка множества N акторов. Через $\pi\upsilon$ обозначим характеристическую функцию, содержательный смысл которой состоит в том, что если в игре с характеристической функцией υ поменять местами акторов согласно перестановке π, то получим игру с характеристической функцией $\pi\upsilon$. В данном случае необходимо применить аксиомы Шепли.

1. ***Аксиома симметрии***. Для любой перестановки π и $i \in N$ должно выполняться $(\pi\upsilon) = \varphi_{\pi(i)}(\upsilon)$, т. е. акторы, одинаково входящие в игру, должны «по справедливости» получать одинаковые выигрыши.
2. ***Аксиома эффективности***. Если коалиция S — любой носитель игры с характеристической функцией υ, то $\sum_{i \in S} \varphi_i(\upsilon) = \upsilon(S)$.

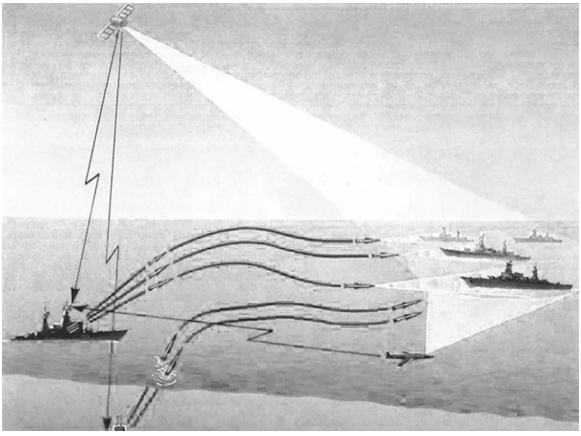
Иными словами, «справедливость требует», чтобы при разделении общего выигрыша носителя игры ничего не выделять на долю посторонних, не принадлежащих этому носителю, равно как и ничего не взимать с них.

3. ***Аксиома агрегации.*** Если есть две игры с характеристическими функциями υ' и υ'', то $\varphi_i(\upsilon' + \upsilon'') = \varphi_i(\upsilon') + \varphi_i(\upsilon'')$, т. е. ради «справедливости» необходимо считать, что при участии акторов в двух играх их выигрыши в отдельных играх должны складываться.

Приведенные примеры и решения могут быть использованы при разработке игровых моделей объективно складывающихся процессов коалиционного взаимодействия в указанных выше объединениях с целью принятия политических решений по обеспечению эффективности их деятельности, укрепления мер доверия при установлении полицентричного мира и устойчивого развития мирового сообщества. Вместе с тем, в контексте всех предшествующих рассуждений мы с уверенностью должны утверждать, что информационно-психологическое

противоборство в киберпространстве не только подвластно гуманитарной экспертизе, но и на основе теоретико-игрового моделирования взаимодействия государств и их коалиций будет разрешаться благодаря математическому объяснению справедливости, индивидуальных и общих интересов.

Глобальное информационное поле. Еще в 1973 г. с целью разработки, совершенствования и сопровождения военно-космических информационно-управляющих систем различного назначения под руководством А. И. Савина (1920–2016) были разработаны и переданы на вооружение комплекс противокосмической обороны «ИС–М» и первая в мире система морской космической разведки и целеуказания (МКРЦ «Легенда»). Высокая эффективность системы МКРЦ была продемонстрирована в 1982 г. в реальной обстановке в период англо-аргентинского вооруженного конфликта у Фолклендских островов. Система позволяла полностью отслеживать обстановку в Мировом океане (рис. 1). В 1982 г. институтом была создана и передана в эксплуатацию космическая система раннего обнаружения ракет «УС–КС». Эти уникальные системы были основаны на комплексном использовании принципиально новых технологий и передовых достижений в области радиотехники, микрофотоэлектроники, схемотехники, создания новых видов оптических материалов и технологических процессов, вычислительной техники, цифровой обработки информации и построения системы распознавания [1].



[1] Отечественный военно-промышленный комплекс и его историческое развитие / Под ред. О. Д. Бакланова, О. К. Рогозина. Изд. 2-е. М., 2013. С. 549.

Рис. 1. Инфографика: пресс-служба концерна ПВО «Алмаз-Антей»

Что следовало далее и какое отношение эти разработки имеют отношение к нашей теме, можно почерпнуть из ряда интервью, которые в последние годы жизни дал академик А. И. Савин.

«Надо было заменить земное мышление космическим, — вспоминал по этому поводу Анатолий Иванович. — Эпопея началась в 1960 году. Система должна быть глобальной: ведь надо контролировать весь земной шар. Как это делать, никто представить не мог. Одна система — это поражение спутников, для этого необходимы Центр контроля за космическим пространством и сложные наземные структуры, а также спутник, который будет уничтожать аппараты противника. К боевому спутнику нужны ракета, системы обеспечения, бортовая аппаратура и головка самонаведения. Мы всё делали до десяти тысяч километров. Потом наш проект вырастал до 42 тысяч километров. К началу программы СОИ (известной еще и под названием "звездные войны") в космосе уже было уничтожено нашей системой до десятка объектов… Опыт подтвердил, что создать ее в полном объеме нельзя, так как оборонительные средства не успевают за развитием средств нападения. И по стоимости они несопоставимы: защищаться во много раз дороже, чем нападать. В инфракрасном диапазоне снимали всю планету, чтобы найти участок, где факел стартующей ракеты был бы виден. И нашел этот участок — на границе светло-голубой атмосферы Земли и черного звездного космоса!.. Сейчас я, в частности, работаю над такой системой, которая делает войну бессмысленной… Я должен иметь информационное поле, которое давало бы время, чтобы поднять наши баллистические ракеты до того, как противник сможет их уничтожить на земле. Это уже глобальное мышление, да и масштабы планетарные. Основная цель — это предотвращение возможной войны». Так Савин опередил заокеанских коллег-конструкторов на 15 лет! СССР реально мог вести космические войны. Именно созданные под его руководством космические информационно-управляющие системы (глобальные по охвату территорий и масштабу задач) позволили уже в 1970-м году достичь и по настоящее время сохранить военно-стратегический паритет с США и всем блоком НАТО (рис. 2, 3).

«Нам удалось, — продолжает далее Савин, — разработать уникальный, даже по нынешним меркам, автоматизированный комплекс, связанный с защитой наших и уничтожением, при военной необходимости, спутников вероятного противника. Тогда это не афишировалось по той причине, что СССР ни при каких условиях не начал бы войну в космосе первым. Мы разрабатывали средства, которые и сегодня относятся

к Воздушно-космической защите. Защите, а не нападению…

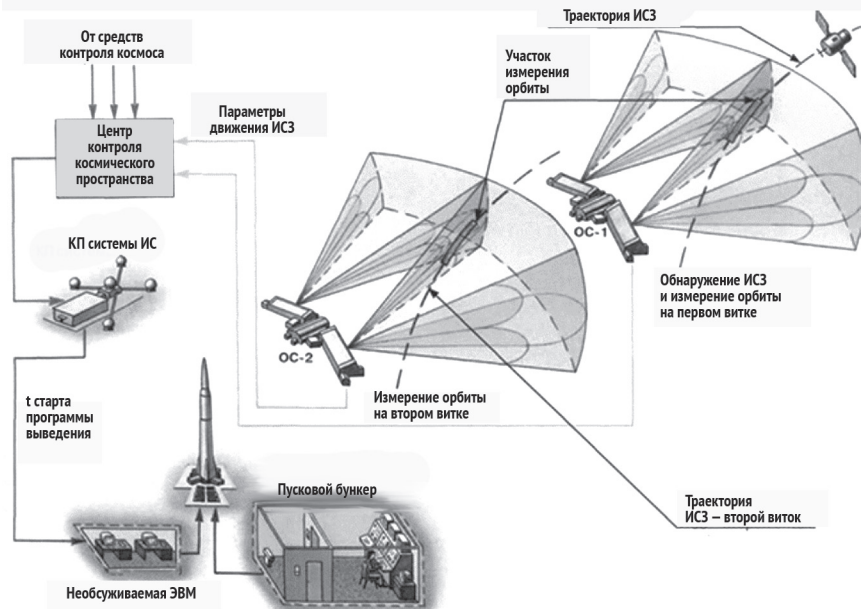


Рис. 2. Инфографика: пресс-служба концерна ПВО «Алмаз-Антей»

Пока за океаном шумно рекламировали и пытались создать свою СОИ, СССР уничтожил в космосе до десятка спутников-мишеней. Вот тогда-то меня и стали называть “отцом космических войн”… Мы стали держать под постоянным наблюдением практически всю акваторию Мирового океана. Причем данные, получаемые космической разведкой, использовались не только в военных, но и в научных целях. Мы наблюдали и наблюдаем развитие природных стихий, миграцию рыб, многое другое. Сейчас такое наблюдение называется дистанционным зондированием земли…С В. Н. Челомеем мы начали делать две системы. Еще до меня он выступал с предложениями по ним, но сам сделать не мог, так как у него были только ракеты, а в такого рода системах главную роль играет информационное поле. Цель создания такой системы — поражение спутников вероятного противника. Система должна быть глобальной, ведь надо контролировать всё околоземное космическое пространство.

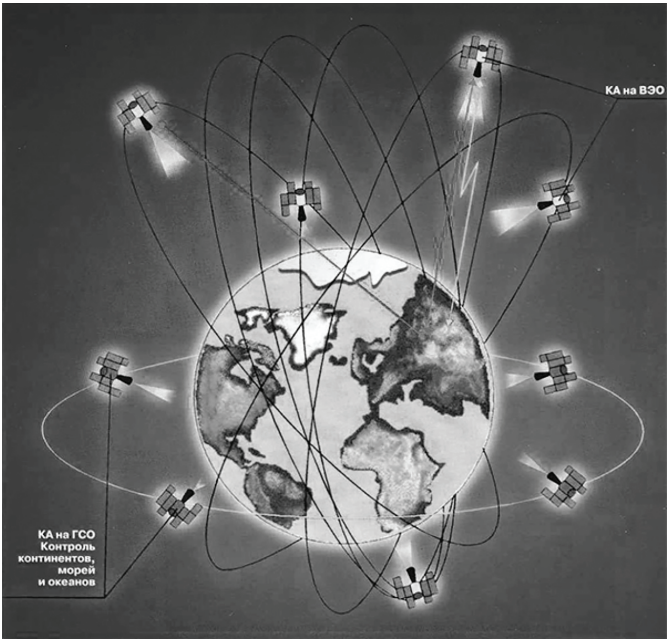


Рис. 3. Инфографика: пресс-служба концерна ПВО «Алмаз-Антей»

Переход на сознание глобального типа дается любому человеку очень трудно. Человек привык мыслить конкретно, но в настоящее время этого недостаточно. Мне удалось преодолеть и этот барьер… Под моим руководством — а я тогда был генеральным конструктором Концерна ПВО "Алмаз-Антей" — разработана концепция поддержания стратегического равновесия и ракетно-ядерного сдерживания агрессии на основе глобальных информационно-управляющих систем. На ней основывается современная оборонная концепция стратегического равновесия в мире»[1]. Как эта идея глобального информационного поля трансформировалась в теоретические разработки инфокоммуникационных и НБИК-технологий, речь пойдет в следующей главе.

Глава 2. Информационная революция в контексте глобального мироустройства и нового технологического уклада

Этапы развития цифровой технологии в информационном обществе. Социальным следствием информационной революции, начиная со второй половины XX века, явилось формирование информационного общества, в развитии которого следует выделять три этапа реализации цифровых технологий обработки и распространения данных [1]:

- ***компьютеризация***, положившая начало автоматизации управленческого труда в соответствии с концепцией построения автоматизированных систем управления (АСУ);
- ***телекоммуникация***, обеспечившая создание новой среды для массового информационного взаимодействия людей в процессе деятельности;
- ***инфокоммуникация***, реализовавшая возможность конвергенции цифровых технологий сохранения, распространения и обработки данных с целью построения глобального информационного поля для обеспечения различных видов социальной деятельности.

Первый этап был нацелен на создание социальных, экономических и технических условий формирования и начального удовлетворения информационных потребностей людей. Для этого этапа было характерно:

[1] *Верзун Н. А., Колбанёв М. О., Михайлов С. В.* Информационные технологии в периодизации истории // Ученые записки Международного банк. ин-та. 2015. Вып. 13. С. 150–161.

— опережающее развитие научно-технических и информационно-технологических направлений, непосредственно обеспечивающих эффективное применение компьютерных технологий;
— модернизация конструкторской, технологической и промышленной баз производства информационных средств и их элементов;
— экстенсивное распространение вычислительной техники на различные области человеческой деятельности;
— организация системы образования, обеспечивающей всеобщую компьютерную грамотность как основу информационной культуры населения.

Техническую базу информатизации на этом этапе создавали мейнфреймы. Они появились в 50-х гг. XX в. и были единственным, дорогим, доступным только крупным организациям, типом компьютеров. Создание мейнфреймов в их современном понимании связано со стандартизацией аппаратного и программного обеспечения в 60-х гг. и с появлением IBM System/360 в 1964 г. В СССР аналогом вычислительных машин IBM была серия ЕС ЭВМ.

Совершенствование технологий построения мейнфреймов никогда не прекращалось. Многие идеи автоматизации управленческой деятельности, особенно в экономике, созданные для мейнфреймов, используются и сегодня. В основном это АСУ, представляющие собой совокупность аппаратно-программных средств и персонала для управления деятельностью в рамках технологических процессов (АСУТП), предприятий (АСУП), отраслей экономики (ОАСУ) или реализации отдельных этапов процессов управления, таких как проектирование, материально-техническое снабжение, бухгалтерский учет и т. п. Внедрение АСУ способствовало повышению эффективности управления объектами деятельности, принятию рациональных управленческих решений.

Переход ко второму этапу обеспечил широкое распространение цифровых телекоммуникационных технологий и связан с изобретением в 90-е гг. XX в.:

— персональных компьютеров, которые существенно превзошли мейнфреймы как по вычислительной мощности, так и по экономическим возможностям массового распространения;
— цифровой сети связи (Интернет), которая объединила многие тысячи персональных компьютеров в корпоративные, научные, правительственные, домашние и другие локальные сети; а затем эти локальные сети были объединены при помощи стека протоколов TCP/IP.

В основе этой цифровой технологии передачи данных лежит коммутация пакетов — блоков данных, на которые разбивается сообщение пользователя. На цифровых сетях коммутационные узлы были заменены маршрутизаторами, которые обеспечивают автоматическую коммутацию, исходя из IP-адресов получателей пакетов [1]. IP-протокол стал мощным инструментом информационной глобализации, поскольку образовал единое адресное пространство в масштабах всего мира. При этом в каждой отдельной сети существует собственное адресное подпространство, которое выбирается, исходя из класса сети. Такая организация IP-адресов позволяет маршрутизаторам однозначно определять дальнейшее направление распространения данных для каждого пакета данных. В итоге данные передаются из сети в сеть, и между локальными сетями Интернета не возникает конфликтов.

Любая локальная или глобальная сеть передачи цифровых данных, для которой существует стандарт инкапсуляции (вложения) в нее IP-пакетов, может передавать и трафик Интернета. Компьютеру или маршрутизатору достаточно знать тип сетей, к которым он непосредственно присоединен, и уметь работать только с этими сетями, не учитывая состояние сети в целом.

Благодаря интуитивно понятным человеко-машинным интерфейсам персональных компьютеров, все слои населения, даже далекие от глубоких знаний компьютерной техники, были вовлечены в повседневной жизни в информационную среду общения. Число постоянных пользователей Интернет продолжает расти и сегодня, а число пользователей, периодически подключающихся к сети, приближается к 90%.

Совместное использование технологии цифровой телекоммуникации с цифровыми технологиями обработки данных в персональных компьютерах и серверах существенно изменило не только способ управления экономикой, но и общественные отношения при реализации процессов производства, распределения, обмена и потребления. Видоизменилась форма реализация человеком своих гражданских прав, возникли новые методы и формы воспитания и образования. Они оказали определяющее влияние на социальную структуру общества, экономику, политику, развитие общественных институтов и служат основой развития общества [2]. Следует утверждать, что

[1] *Кожанов Ю. Ф., Колбанёв М.* О. Технология инфокоммуникации. — Курск: Науком, 2011. 260 с.

[2] *Советов Б. Я., Колбанёв М. О., Татарникова Т. М.* Информационное общество: современные состояние, проблемы, технологии и перспективы // Инновации

в первом десятилетии XXI века второй этап становления цифрового информационного общества, начатый в 90-е гг. XX в., был завершен.

Третий этап развития информационного общества характеризуется лавинообразным ростом объемов данных, сопровождающих человеческую деятельность. Например, за один 1999 год в мире было произведено от 2 до 3 Экзабайт данных. В 2002 году уже от 3 до 5 Экзабайт, а в 2011 году объем цифровой информации в 10 раз превысил объем 2006 года. По прогнозам, к 2020 г. объем информации достигнет 40 Зеттабайт. Такие процессы наблюдаются практически во всех сферах деятельности человека: культуре, экономике, политике, науке, образовании и других. Возрастающий объем информационного ресурса вовлекает в информационную индустрию все большее количество людей. Доля людей, занятых в сфере производства и распространения информации в XXI в., значительно выше, чем в других видах человеческой деятельности. Более того, свыше 60% новых рабочих мест в развитых странах связаны сегодня с той или иной формой преобразования информации.

Технологической базой реализации третьего этапа стали информационные технологии, обеспечивающие развитие информационной инфраструктуры каждой страны и условия для включения ее в состав мировой структуры информационного общества. Тем самым открывается доступ к новым информационным ресурсам, представленным в цифровом виде в глобальном информационном пространстве [1]. Третий этап формирования информационного общества характеризуется конвергенцией услуг систем хранения, распространения и обработки данных, благодаря которой появляется возможность не только пользоваться, но и непосредственно пополнять государственные и мировой информационный фонды. Конвергенция информационных технологий породила качественно новую технологию инфокоммуникации (рис. 4) в виде интегрированной инфокоммуникационной среды, «накрывающей» цифровой сетью все информационные системы и ресурсы. Информационный фонд человечества, ставший достоянием практически каждого человека, превратился в основной ресурс развития общества.

В настоящее время накоплены настолько большие объемы информационного ресурса, что проблемой стала сложность доступа к данным в процессе

в информационно-аналитических системах. 2015. Вып. 11. URL: http://www.iias.ru/index.php/sborniki/vypusk-11.

[1] *Верзун Н. А., Колбанёв М. О., Татарникова Т. М.* Технологическая платформа четвертой промышленной революции // Геополитика и безопасность. 2016. № 2(34). С. 73–78.

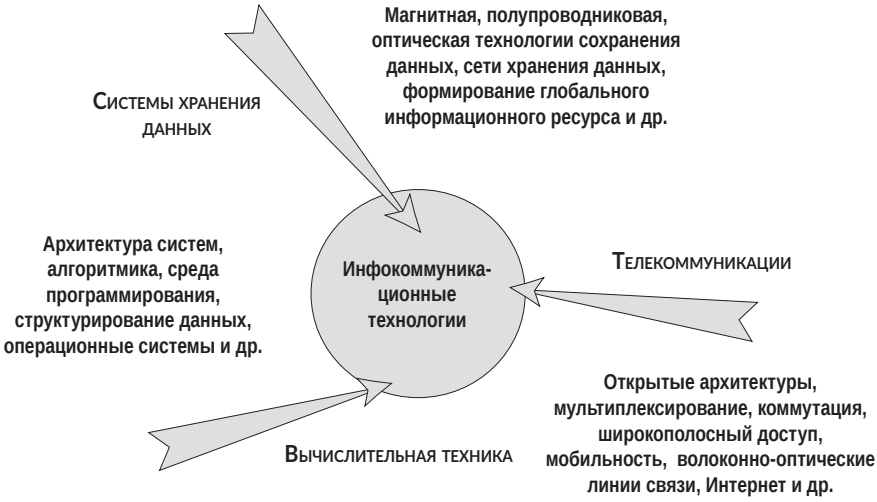


Рис. 4. Интегрированная инфокоммуникационная среда

удовлетворения информационных потребностей людей. Основная задача технологии информационного общества на текущем этапе развития, соответственно, заключается в повышении эффективности процедур доступа к данным[2].

В глобальном информационном пространстве ведутся тысячи международных, национальных, региональных и местных проектов поддержки развития информационного общества. Государства, имеющие стратегии информационных обществ, выполняют строгие политические обязательства в этом направлении с учетом национальной безопасности своих стран. Доктрина информационной безопасности Российской Федерации относит, по сути, к таким угрозам возможность использования информационного потенциала зарубежных стран:

— для воздействия на критическую информационную инфраструктуру РФ и технической разведки;
— в качестве инструмента для подрыва суверенитета и территориальной целостности РФ, распространения необъективной и предвзятой информации;

[2] *Колбанёв М. О., Татарникова Т. М.* Информационный объем базовых информационных процессов // Информационно-управляющие системы. 2014. № 4. С. 42–47.

— для поддержки компьютерной преступности в кредитно-финансовой сфере и нарушения неприкосновенности персональных данных;
— для препятствия развитию в РФ конкурентоспособных информационных и коммуникационных технологий и продукции на их основе;
— для достижения экономического и геополитического преимущества за счет технологического доминирования в глобальном информационном пространстве.

В основе этих угроз лежит оценка роли информации в современном обществе, из которой следует, что информация превратилась в важный политический и экономический ресурс, что доступ к информации уже невозможен без развитых инфокоммуникационных технологий и др. Достижение целей указанной выше доктрины невозможно без обеспечения безопасности базовых технологий цифрового общества и цифровых рынков. Таким образом, все более широкое применение цифровых информационных технологий на указанных выше этапах ***компьютеризации***, ***телекоммуникации*** *и* ***инфокоммуникации*** привело к появлению принципиально нового типа угроз информационного характера (примером чему может служить Интернет вещей, несущий многочисленные риски и угрозы), защиту от которых необходимо создавать на технологическом, экономическом и политическом уровнях.

Ожидаемые последствия внедрения технологий цифровой экономики. На этапе инфокоммуникации стали доступны процедуры преобразования объектов разной природы в цифровую модель и обратно, что позволяет, в частности, представить модель деятельности в условиях функционирования цифровой экономики (рис. 5).

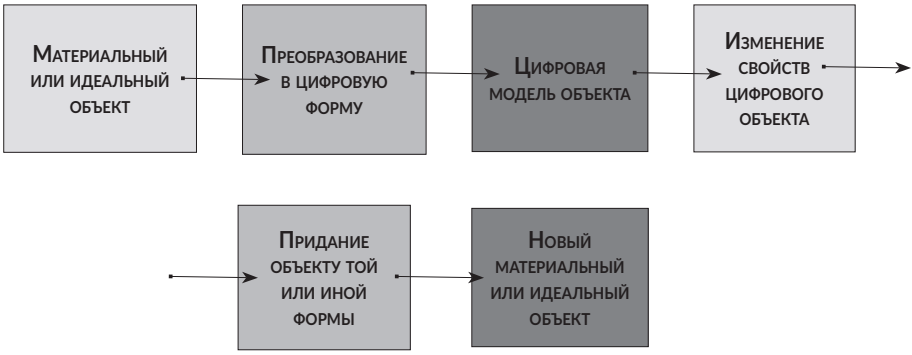


Рис. 5. Обобщенная модель деятельности в цифровой экономике

Реализация этой модели предполагает, что общество, помимо опоры на цифровые информационные технологии, обладает рядом признаков:

— опора на цифровые информационные технологии;
— сетевая архитектура и цифровая коммуникация;
— цифровая форма представления объектов деятельности;
— виртуализация цифровых технологий работы с объектами;
— ориентация на знания, представленные в цифровом виде;
— инновационная движущая сила развития;
— интеграция и глобализация за счет стандартизированной формы цифровых объектов;
— конвергенция и высокая динамика изменений;
— трансформация всех видов деятельности и др.

Соответственно возникают цифровая экономика, цифровая политика, цифровое образование, цифровая медицина, цифровые культура и спорт, цифровое государство, цифровое сельское хозяйство, цифровой транспорт, цифровая безопасность, цифровая энергетика, цифровая экология и т. д. Одно из центральных мест в цифровом обществе занимает цифровая экономика. В своем послании к Федеральному Собранию 2016 г. Президент России В. В. Путин сформулировал задачу перехода к цифровой экономике как политическую цель развития государства. Он, в частности, заявил следующее: «Одной из самых быстроразвивающихся отраслей стала у нас <…> ИТ-индустрия… — Уверен, уже в ближайшее десятилетие есть все возможности сделать ИТ-индустрию одной из ключевых экспортных отраслей России». Далее: «Будем увеличивать число бюджетных мест по инженерным дисциплинам, по ИТ-специальностям…, которые определяют развитие экономики… В следующем году на базе ведущих вузов, в том числе региональных, будут созданы центры компетенции. Они призваны обеспечить интеллектуальную, кадровую поддержку проектам, связанным с формированием новых отраслей и рынков». И наконец: «Правительству Российской Федерации разработать совместно с Администрацией президента Российской Федерации и утвердить программу "Цифровая экономика", предусмотрев меры по созданию правовых, технических, организационных и финансовых условий для развития цифровой экономики в Российской Федерации и ее интеграции в пространство цифровой экономики государств — членов Евразийского экономического союза» [1].

---

[1] http://sosedgeorg.livejournal.com/490683.html.

Что же такое «цифровая экономика»? Синонимами этого понятия являются: в США — API-экономика (Application Programming Interface — интерфейс для программирования приложений) [1]; Gartner — программируемая экономика [2]; экономика приложений; электронная (транзисторная) экономика и др. Общим местом всех этих определений является обозначение экономики, переход к которой инициируется развитием цифровых информационных технологий.

В проекте «Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» (декабрь 2016 г.) дается такое определение: цифровая экономика — это «деятельность, в которой ключевыми факторами производства являются данные, представленные в цифровом виде, а их обработка и использование в больших объемах, в том числе непосредственно в момент их образования, позволяет по сравнению с традиционными формами хозяйствования существенно повысить эффективность, качество и производительность в различных видах производства, технологий, оборудования, при хранении, продаже, доставке и потреблении товаров и услуг» [3]. В этом определении выделяют признаки экономической деятельности, основанной на цифровых информационных технологиях:

1) наличие цифровых данных,
2) формирование больших объемов этих цифровых данных,
3) возможность обработки этих данных в реальном масштабе времени для реализации экономических процессов,
4) достижение лучших экономических показателей за счет такой обработки.

Анализируя последствия перехода к цифровой экономике, необходимо помнить, что каждый крупный технологический прорыв в прошлом приводил к опасным последствиям, в том числе и к мировым войнам. Индустриальный аспект цифрового общества выделяет Клаус Шваб, президент Всемирного экономического форума в Давосе. С его точки зрения переход к цифровой экономике происходит в результате четвертой промышленной революции, о чем речь шла в предыдущей главе.

---

[1] Экономика API. URL: http://www.ibm.com/middleware/integration/ru-ru/api-economy.html.

[2] Gartner Symposium/ITxpo, 1–5 October 2017 Orlando FL. URL: http://www.gartner.com/us/symposium.

[3] Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (проект). URL: http://d-russia.ru/wp-content/uploads/2016/12/2016-strategia_IO_proekt_dec.pdf.

Обсуждению последствий революционных изменений в сфере производства посвящена статья Шваба[4]. Ее главный мотив: «Мы стоим на пороге технической революции, которая полностью изменит наш образ жизни, работы и коммуникации. Нас ожидает величайшая за всю историю человечества трансформация — величайшая по масштабу и сложности». Отталкиваясь от особенностей промышленного производства, К. Шваб строит периодизацию исторического процесса индустриализации следующим образом (рис. 6).

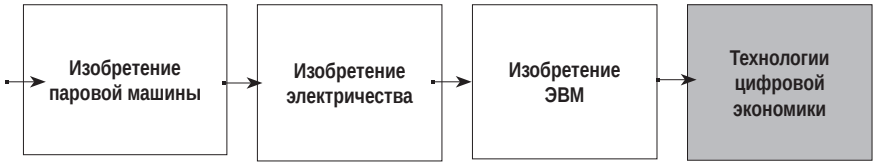


Рис. 6. Технологические основания промышленных революций

Четвертая промышленная революция, как отмечалось в предыдущей главе, опирается на третью, поскольку ее база — это по-прежнему цифровые технологии, но нового типа. Революционные возможности новых технологий являются следствием «скорости, масштаба и системных последствий технологических изменений». «Четвертая революция влияет на каждую индустрию каждой страны в мире. Глубина и широта вызванных ей изменений требуют трансформации целых систем производства, менеджмента и управления». Примером новых информационно-технологических достижений могут служить такие области, как «искусственный интеллект, робототехника, Интернет вещей, автономный транспорт, 3D-печать, нанотехнологии, материаловедение, новые батареи, квантовые компьютеры».

Одним из самых важных признаков технологий четвертой промышленной революции является сопряжение информационных и физических объектов, стирающих границы между реальными и виртуальными процессами. Благодаря новым информационно-технологическим достижениям, без преувеличения, любая деятельность человека становится информационной не только по своей форме, но и по содержанию. Шваб признает, что помимо новых возможностей цифровые технологии приведут и к новым трудностям, которые способны «усилить финансовое

[4] *Klaus Schwab*. The Fourth Industrial Revolution. URL: https://www.foreign affairs.com/articles/2015–12–12/fourth-industrial-revolution.

и социальное неравенство, нарушить работу рынков, вытеснить с рынка труда множество людей и увеличить разрыв между прибыльностью капитала и прибыльностью труда». Общее мнение всех исследователей заключается в том, что четвертая промышленная революция будет иметь серьезные последствия для людей, государства и бизнеса.

Технологический аспект цифровой экономики также стоит во главе угла исследований ученых, изучающих экономические циклы. В частности, академик С. Ю. Глазьев указывает на переход ведущих экономик мира на 6-й технологический уклад, который принципиально меняет комплекс технологий и инноваций и лежит в основе количественного и качественного скачка в развитии производительных сил общества [1]. При этом информационные технологии, которые являлись локомотивом 5-го технологического уклада, сохраняют свою роль и при переходе к 6-му укладу благодаря конвергенции Нано-Био-Инфо-Когно и формированию НБИК-технологий (рис. 7).

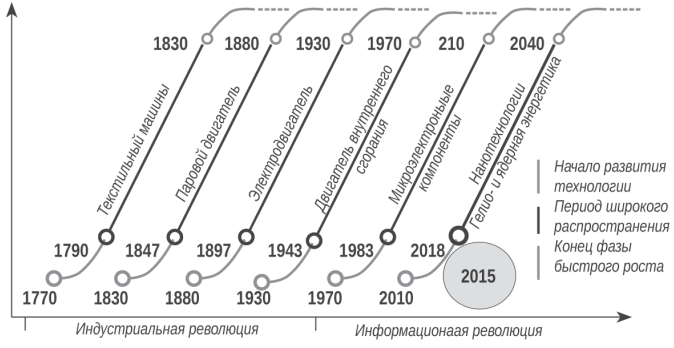


Рис. 7. Смена технологических укладов экономики

Помимо информационных технологий, рассмотренных выше, в состав НБИК-технологий входят нано-, био- и когнитивные технологии. Особенности новых технологических направлений заключаются в следующем. Нанотехнологии выделяются в соответствии с линейными размерами элементов систем. Если при уменьшении объема какого-либо

[1] *Глазьев С. Ю.* Уроки современной революции: крах либеральной утопии и шанс на «экономическое чудо». М., 2011. 572 с.

вещества по одной, двум или трем координатам до размеров нанометрового (10^{-9} м) масштаба возникает новое качество, то эти образования следует отнести к наноматериалам, а технологии к нанотехнологиям. Примеры таких технологий: наноэлектроника, экраны с высокой разрешающей способностью, нанотрубки и др.

Биотехнологии предполагают использование живых организмов, их систем или продуктов их жизнедеятельности для решения технологических задач, а также создание живых организмов методом генной инженерии. Примерами могут служить: создание новых сочетаний генов, производство человеческого инсулина путем использования генно-модифицированных бактерий, клонирование и др.

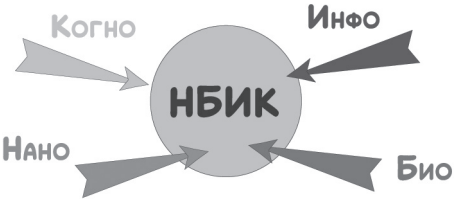


Рис. 8. Образование НБИК-технологий

Технологии, которые объединяют достижения когнитивной психологии, педагогики, исследований в сфере искусственного интеллекта, нейробиологии, нейропсихологии, нейрофизиологии, лингвистики, математической логики, неврологии, философии и других наук, называются когнитивными технологиями, в числе которых — интеллектуальные допинги для мозга, «заглядывание» в мозг, излечение слепых и глухих, мозго-машинные интерфейсы и др. (рис. 8).

По мнению многих специалистов, благодаря развитию инфокоммуникационных и НБИК-технологий, в течение ближайших 7–10 лет окажутся невостребованными многие специалисты физического и рутинного интеллектуального труда, поскольку их заменят программные роботы. Примером соответствующих специальностей могут служить бухгалтеры, юрисконсульты, нотариусы, логисты, журналисты, туристические агенты, специалисты call-центров, экскурсоводы, таксисты, переводчики, пекари, мясники, бурильщики, фармацевты, страховые агенты, продавцы, врачи, системные администраторы и многие другие профессии. Востребованными останутся профессии, требующие интуиции, сопереживания и социального взаимодействия. Такие как, например, психологи, социальные

работники, медсестры, артисты, спортсмены, священнослужители и т. п. В то же время цифровой экономике требуются специалисты новых профилей. Например, на одном из сайтов можно найти перечень новых профессий для области информационных технологий [1]:

- дизайнер виртуальных миров создает концептуальные решения для виртуального мира: философию, законы природы и общества, правила социального взаимодействия и экономики, ландшафт, архитектуру, ощущения (запахи, вкус, звуки и др.), живой мир;
- сетевой юрист занимается формированием нормативно-правового взаимодействия в сети (в т. ч. в виртуальных мирах), разрабатывает системы правовой защиты человека и собственности в Интернете (включая виртуальную собственность);
- проектировщик нейроинтерфейсов занимается разработкой совместимых с нервной системой человека интерфейсов для управления компьютерами, домашними и промышленными роботами, с учетом психологии и физиологии пользователей;
- организатор интернет-сообществ организует и моделирует электронные форумы, игровые и образовательные площадки;
- ИТ-проповедник организует коммуникации с конечными пользователями, продвигает новые решения в консервативно настроенные группы, осуществляет обучение людей новым программам и сервисам для сокращения цифрового разрыва среди населения;
- цифровой лингвист разрабатывает лингвистические системы семантического перевода (с учетом контекста и смысла), обработки текстовой информации (в том числе семантический поиск в Интернете) и новые интерфейсы общения между человеком и компьютером на естественных языках;
- разработчик моделей BigData проектирует системы сбора и обработки больших массивов данных, получаемых через Интернет, разрабатывает модели их анализа.

Обращает на себя внимание та ситуация, что в своем большинстве новые профессии связаны с сугубо смысловой стороной информационное деятельности — проповедник и лингвист, сетевой юрист и дизайнер, проектировщик и организатор и др.

Угрозы, порождаемые базовыми технологиями цифровой экономики. В соответствии с изложенными выше представлениями о принципах функционирования цифровой экономики, ее архитектура может быть

[1] Сколково. URL: http://atlas100.ru.

представлена как сеть, содержащая совокупность разнообразных по функциям и масштабу центров преобразования цифровых данных, которые:

— реализуют ту или иную часть общего процесса, общая схема которого была представлена выше на рис. 5 (с. 110);
— связаны друг с другом при помощи цифровых сетей.

Цифровая экономика включает в себя и киберпространство, и информационный контент, и средства работы с этим контентом, поэтому ее следует рассматривать не только как элемент цифрового общества, но и как часть единого глобального информационного пространства (инфосферы).

Цифровая экономика позволяет формировать виртуальную действительность, меняет формы общественных отношений и дает возможность человеку действовать независимо:

— от часовых поясов,
— от географического расположения объектов,
— от социальной значимости объектов.

С информационно-технологической точки зрения цифровая экономика создает интегральное информационное поле (рис. 9).

Это понятие ввел академик А. И. Савин, работая над противоспутниковой обороной и занимаясь науками о Земле, о чем речь шла в предыдущей главе. В его интерпретации это такая часть инфосферы, которая обладает следующими свойствами:

1) это искусственная система;
2) это глобальная система, охватывающая весь Земной шар и околоземное космическое пространство;
3) это мощный технологический инструмент геополитики;
4) эта система максимально приближает друг к другу три момента времени: а) возникновение некоторых событий в произвольных точках пространства, б) начало анализа последствий, к которым могут привести эти события, в) принятие решения о варианте реагирования на эти события;
5) информационное поле следует рассматривать как интегральную информационную систему, которая включает в себя информацию, накопленную во всех областях человеческой деятельности. Информационное поле интегрирует все знания и возможности;
6) интегральная информационная система имеет, по крайней мере, два входа:

— для получения данных от сенсоров и датчиков, распределенных на Земле, в космосе, киберпространстве и замеряющих различные физические параметры,

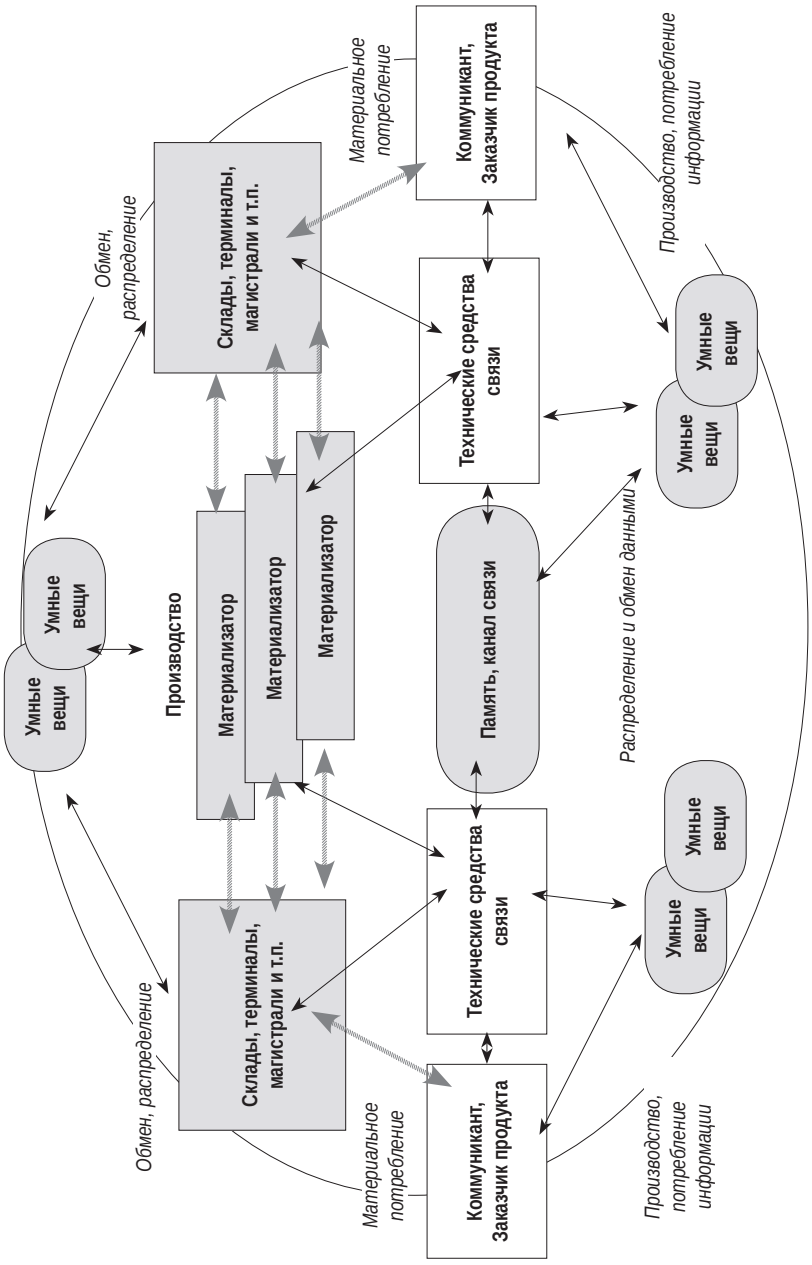


Рис. 9. Модель интегрального информационного поля цифровой экономики

— для подключения терминалов пользователей, через которые имеется возможность проводить исследования, моделировать природные процессы и процессы деятельности людей.

7) Эта система должна иметь три уровня:

— уровень смысла и архитектуры, который формируется специалистами разных областей знания путем создания метаданных на основе определения и классификации понятий. Метаданные дают возможность специалисту ориентироваться в информационном поле, превращают информацию в информационный ресурс, пригодный и доступный для использования;

— уровень информационных технологий, который образуется распределенными в пространстве центрами, способными реализовать комплексную интеграцию сенсоров, датчиков-измерителей, инструментальных средств, систем хранения и другого оборудования и программ, с одной стороны, и больших объемов цифровых данных, с другой стороны. Такая интегрированная система намного сложнее, чем данные, объединенные в системах хранения отдельно от измерительных и вычислительных мощностей сами по себе;

— уровень сетевой архитектуры, обеспечивающий взаимодействие между центрами при помощи коммутируемых высокоскоростных потоков цифровых данных.

В качестве модели интегрального информационного поля определена коммуникационная сеть. Она комплексно описывает инфокоммуникационные, производственные, логистические системы, как и цифровые системы любого другого назначения в виде элементов единой коммуникационной сети, доставляющей в автоматическом режиме материальные и информационные объекты любого вида до пункта назначения с заданными вероятностно-временными и энергетическими характеристиками [1].

Со стороны пользователя инфокоммуникационная и материальная инфраструктуры превращаются в «розетку доступа», через которую можно как получить любую информационную услугу, так и заказать сохранение, изготовление и доставку нужного материального изделия.

Наряду с понятием «облачная услуга», которое уже широко используется в информационных технологиях, появилось понятие «облачное

---

[1] *Колбанёв М. О., Татарникова Т. М., Воробьёв А.* И. Модель балансировки нагрузки в вычислительном кластере центра обработки данных // Информационно-управляющие системы. 2012. № 3. С. 37–41.

производство»[1] — полностью автоматизированное производство, которое обеспечивает доступ к производственным, логистическим и информационно-технологическим ресурсам дистанционно через коммуникационные сети[2]. Примером облачных производств могут служить[3]: аддитивное производство, производство на основе промышленных роботов, новая логистика и др. Благодаря этим достижениям место интернет-магазинов в скором времени начнут занимать интернет-заводы.

Новые возможности мобильного широкополосного доступа являются источником новых угроз информационной безопасности. Все они в основном связаны с внедрением в мобильные устройства вредоносных программ как на этапе собственно изготовления устройства, так и в процессе эксплуатации. В результате таких атак появляется возможность:

- несанкционированного доступа к конфиденциальным данным, сохраненным в устройстве, к почтовой переписке, паролям используемых программ, системам работы с денежными средствами и т. п.;
- включения микрофона без ведома пользователя и, тем самым, прослушивания конфиденциальных переговоров;
- получения данных от GPS-навигатора о местонахождении пользователя, его присутствии или отсутствии в определенных местах;
- отслеживания всех контактов пользователя и изучения истории совершенных звонков.

Владелец зараженного мобильного устройства оказывается под полным круглосуточным контролем. Особенно опасны такие атаки на устройства представителей государственной власти и крупного бизнеса. Для защиты мобильного устройства не годятся методы защиты персональных компьютеров, поскольку, как и в случае облачных вычислений, отсутствует граница сети, на которой можно было бы блокировать атаки. Это означает, в частности, что значительная часть ответственности за информационную безопасность лежит на владельце устройства.

Важной особенностью технологий третьей платформы информатизации (ТПИ) являются широкие возможности организации наложенных

---

[1] *Зеленков Ю. А.* На пути к облачному производству // Открытые системы. СУБД. 2015. № 3. С. 42–44.

[2] *Колбанёв А. М., Татарникова Т. М., Яковлева Е. А.* Систематизация базовой терминологии в области информационных технологий // Ученые записки Междунар. банк. ин-та. 2015. № 13. С. 162–171.

[3] *Верзун Н. А., Колбанёв М. О., Татарникова Т. М.* Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности: сборник статей сотрудников кафедры ИСиТ. — СПб., 2016. С. 52–56.

сервисов, когда новые информационные услуги создаются за счет наложения нового оборудования и программного обеспечения на уже существующую информационную инфраструктуру. OTT (Over the top, наложенный сервис) — метод (формат), с помощью которого набор данных (цифровой контент, файлы) разбивается на IP-пакеты и доставляется от одного компьютера к другому по сетям сторонних операторов связи от источника к получателю. Принципиальное отличие OTT заключается в том, что оператор связи не контролирует OTT-сервис, а OTT-сервис не контролирует сеть оператора и не гарантирует качество обслуживания[4].

Примером OTT-сервисов служат, в частности, социальные сети — это информационная платформа, которая предназначена для построения, отражения и организации социальных (общественных, межличностных) отношений. Свойства Интернета позволяют реализовать такую платформу в виде OTT-сервисов, и тогда социальная сеть (как часть Интернет) — это WEB-сайт, который за счет персонализации пользователей и путем объединения их в виртуальные группы с общими интересами для общения и (или) работы создает возможность социальных отношений в цифровом пространстве. Создать WEB-сайт для современной социальной сети можно только при помощи технологий облачных вычислений, высокоскоростного мобильного доступа и больших данных, поскольку он должен обладать особыми свойствами:

— работа с большими объемами плохо структурированных данных (сотни терабайт в день);
— обслуживание трафика очень большого объема (миллионы посещений в сутки);
— обеспечение режима реального времени, причем и времени отклика, и скорости обмена.

Социальные сети способны обеспечить всевозможные способы индивидуального и массового общения — электронная почта, форумы, блоги, социальные закладки, чаты, онлайн-игры, WEB-конференции, интернет-сообщества и др.

Об экономической эффективности социальных сетей от предприятий аналоговой экономики свидетельствует такой факт. Штат сотрудников мессенджера WhatsApp, который был продан за $19 млрд составлял 55 человек. При этом он обслуживал около 1 млрд пользователей по всему миру и обеспечивал передачу 30 млрд сообщений и 200 млн голосовых заметок каждый день. Принцип создания наложенных сервисов применим

[4] http://www.minsvyaz.ru/ru/events/33396.

и по отношению к услугам связи. Наложенные сети, как правило, образованы множеством равноправных узлов, каждый из которых может либо отсутствовать в сети, либо присутствовать, выполняя, в зависимости от условий распространения трафика, роль клиента или роль сервера. Такое свойство сетей называют самоорганизацией.

Наложенные сервисы являются еще одним каналом рисков и угроз, особенно если их использование является частью процессов принятия решений на государственном уровне или элементом реализации бизнес-процессов компании. Риск утечки конфиденциальной информации повышается из-за невнимательных или нелояльных сотрудников. Еще одна угроза — это «маскарад», или возможность подмены личности, т. к. в социальной сети никогда не известно, кто доподлинно скрывается под тем или иным именем. Необходимо учитывать, что процессы и тематика общения в социальных сетях могут быть намеренно организованы противником, использующим средства социальной инженерии. Поскольку наложенные сервисы представляют собой надстройку над Интернет, им свойственны и все традиционные угрозы, такие как Web-атаки, воровство паролей или фишинг.

Анализ возможностей технологий ТПИ показывает, что, без преувеличения, любая деятельность человека в XXI веке становится информационной не только по своему содержанию, но и по форме, поскольку немыслима без использования информационных технологий. Это обстоятельство прямо отражается в возникновении новых угроз информационной безопасности личности, общества и государства. Мрачную картину результатов внедрения незащищенных инновационных технологий ТПИ можно представить следующим образом:

— облачные вычисления. Затребованные нами вычисления производит в произвольный момент времени виртуальная машина, которая расположена в облаке в неизвестной нам точке информационного пространства, не контролируется нами и, возможно, контролируется другими лицами;
— интернет-вещи. Вещи стали элементами киберпространства. Мы окружены множеством сенсоров, таких как камеры видеонаблюдения, датчики движения, температуры или банковские карты, которые непрерывно информируют облако о нашем состоянии и состоянии окружающего нас мира;
— мобильный доступ. Смартфон, который сопровождает нас повсюду, непрерывно передает информацию в облако о нашем местоположении, наших контактах и способен самостоятельно вести прослушивание наших разговоров;

— наложенные сервисы. В социальных сетях, в том числе и без нашего участия, постоянно обновляется информация о нашей приватной жизни, и, возможно, сразу несколько наших двойников поддерживают контакты с известными или неизвестными нам людьми от нашего имени;
— большие данные. При помощи специальных алгоритмов и суперкомпьютеров весь объем подобной информации о нас и миллионах наших сограждан обрабатывается для получения статистического досье нашего общества.

Множество угроз безопасности, вызванных инновационными свойствами технологий ТПИ, с одной стороны, и невозможность отказа от этих технологий без потери эффективности деятельности, с другой стороны, позволяет выделить новый объект исследования — информационно-технологическую безопасность в приложении ко многим предметным областям, например:

— в области критической инфраструктуры: информационно-энергетическую и информационно-транспортную безопасность,
— в социальной сфере: информационно-медицинскую и информационно-психологическую безопасность,
— в государственном управлении: информационно-политическую и информационно-экономическую безопасность.

Особое значение в системе безопасности информационного общества принадлежит взаимодействию двух предметных областей: экономической безопасности и информационной безопасности.

Цифровые рынки и безопасность. Практическим инструментом движения России к цифровой экономике является Национальная технологическая инициатива — НТИ — это долгосрочная комплексная программа по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках, которые будут определять структуру мировой экономики в ближайшие 15–20 лет [1]. Постановлением Правительства РФ № 317 от 18.04.2016 г. утверждены правила разработки и реализации планов мероприятий («дорожных карт») НТИ. Дорожные карты должны содержать [2]:

---

[1] *Песков Д. Н.* Стратегия национальной технологической инициативы. Режим доступа: свободный. http://ftp-www.bsu.edu.ru/Skolkovo/Д.%20 Песков_Национальная%20технологическая%20инициатива.pdf.

[2] *Ливанов Д. В.* Национальная технологическая инициатива. URL: Режим доступа: свободный. http://www.government.ru/media/files/ipgQAHH3Lz30OzqLEIPbreX1mCG63sjz.pdf.

1) результаты форсайта (foresight — взгляд в будущее), обоснованность выбора рынков и групп технологий;
2) оценку состояния рынков до 2035 г., в том числе со смежными рынками и оценку вероятной доли лидеров;
3) необходимые ресурсы и их источники:
— требования к уровню технологического развития. Критические точки по доступности ключевых технологий,
— требования к научной и инновационной инфраструктуре, формирование опережающего задела,
— потребность в человеческом капитале и требования к системе образования и подготовки кадров,
— необходимая интеллектуальная собственность и опережающее патентование ключевых технологий,
— необходимые инвестиции, включая модификацию деятельности и ресурсы институтов развития,
— общественная поддержка трансформации. Развитие системы дополнительного образования;
4) инструменты поддержки реализации дорожной карты:
— стандарты и регламенты,
— система государственного регулирования,
— нормативное обеспечение трансформации рынков и развития технологий;
5) ожидаемые результаты реализации дорожной карты.

Ведущие университеты страны в рамках НТИ в 2015 г. уже получили более 5 млрд руб.

К числу критериев для выбора рынков будущего относятся [1]:
— рынок станет значимым и заметным в глобальном масштабе: объем составит более $100 млрд к 2035 г.;
— на текущий момент рынка нет, либо на нем отсутствуют общепринятые/устоявшиеся технологические стандарты;
— рынок в первую очередь ориентирован на потребности людей как конечных потребителей (приоритет B2C над B2B);
— рынок важен для России с точки зрения обеспечения базовых потребностей и безопасности;
— в России есть условия для достижения конкурентных преимуществ и занятия значимой доли рынка;

[1] О Национальной технологической инициативе. URL: Режим доступа. свободный. https://www.leader-id.ru/upload/file/get/3109.

— в России есть технологические предприниматели с амбициями создать компании-лидеры на данном высокотехнологичном новом рынке;

— рынок будет представлять собой сеть, в которой посредники заменяются на управляющее программное обеспечение.

В настоящее время в активной проработке находятся дорожные карты по развитию 9-ти перспективных рынков и 3-х инфраструктурно-технологических направлений (ИТН):

— AeroNet — рынок распределенных систем беспилотных летательных аппаратов;
— MariNet — рынок распределенных систем морского транспорта без экипажа;
— AutoNet — рынок распределенной сети автотранспорта без водителя;
— HealthNet — рынок систем, базирующихся на достижениях в науках о жизни и обеспечивающих рост продолжительности жизни, а также получение новых эффективных средств лечения тяжелых заболеваний;
— NeuroNet — рынок средств человеко-машинных коммуникаций, основанных на передовых разработках в нейротехнологиях и повышающих продуктивность человеко-машинных систем, производительность психических и мыслительных процессов;
— EnergyNet — рынок энергии, основанный на технологических решениях, обеспечивающих интеллектуализацию и распределенный характер энергетических сетей (smart grid);
— FoodNet — рынок продовольствия, обеспеченный интеллектуализацией, автоматизацией и роботизацией технологических процессов на всем протяжении жизненного цикла продуктов от производства до потребления, а также развитием биотехнологий;
— SafeNet — рынок безопасных и защищенных компьютерных технологий, решений в области передачи данных, безопасности информационных и киберфизических систем;
— FinNet — рынок децентрализованных финансовых систем и персонифицированных сетевых финансовых сервисов;
— TechNet –разработка технологий цифрового проектирования и моделирования, производства новых материалов, аддитивных технологий;
— группа «Университетские города НТИ» — создание открытой платформы для генерации профессий, компетенций и технологий будущего;

— группа «Кружковое движение» — создание среды возможностей, которая поощряет организационное разнообразие и выращивание команд для исследований и новых бизнесов.

Новые рынки формируются на отрицании всех базовых принципов аналоговой экономики. Это можно проиллюстрировать на примере рынка AutoNet (табл. 3) [1].

Приоритетные группы технологий НТИ составляют:

— большие данные;
— искусственный интеллект;
— системы распределенного реестра;
— квантовые технологии;
— новые и портативные источники энергии;
— новые производственные технологии;
— сенсорика и компоненты робототехники;
— технологии беспроводной связи;
— технологии управления свойствами биологических объектов;
— нейротехнологии, технологии виртуальной и дополненной реальностей.

Таблица 3

Сравнение аналогового и цифрового автомобильных рынков

Аналоговая экономика	Цифровая экономика
Автомобильная отрасль	Не отрасль, а рынок
Автомобиль как изделие	Оказание услуги по передвижению
Материал – сталь	Композитные материалы
С двигателем внутреннего сгорания	Без двигателя внутреннего сгорания
Делается на комплексе заводов (от металлургических, до сборочных)	Производится в «гараже» с необходимым оборудованием
Автомобили выпускаются серийно	Автомобили кастомизированы, учитывают требования каждого заказчика
Управление человеком	Беспилотное управление
Продается дилерами	Продается без посредников
Стоит дорого	Не платный, оплачивается пакет услуг

[1] Форум стратегических инициатив 2016. *Песков Д. Н.* Мир 2035 безусловно шизофреничен // Форум стратегических инициатив 2016. URL: Режим доступа: свободный. http://www.json.tv/ict_news_read/forum-strategicheskih-initsiativ-2016-dmitriy-peskov-mir-2035-bezuslovno-shizofrenichen-20160802024543.

Развитие этих групп технологий позволит создать глобально конкурентоспособные высокотехнологичные продукты и сервисы, необходимые рынкам будущего. Исследования в этих направлениях обеспечат университетам востребованность на рынке труда со стороны высокотехнологичных отраслей отечественной экономики на протяжении примерно 20 лет. Процесс цифровизации человеческой деятельности, а значит, и движение человечества к цифровому обществу и цифровой экономике является объективным процессом. Гуманитарным преимуществом такого движения должно стать увеличение продолжительности и качества жизни людей, но только в одном случае — обеспечения безопасности используемых технологий. Применимы ли методы обеспечения безопасности личности, общества и государства, разработанные и апробированные в аналоговом обществе, для цифрового общества? Достаточно ли соблюдения принципов построения систем информационной безопасности, разработанных в эпоху мейнфреймов и классического Интернета, для обеспечения безопасности цифрового общества?

На оба эти вопроса следует дать отрицательный ответ, в первую очередь потому, что меняется форма представления объектов, с которыми имеет дело экономика.

Сравним экономическую и информационную деятельности. И в одном, и в другом случае субъектом деятельности является человек. Объектом же экономической деятельности, в общем случае, является благо, т. е. то, что способно удовлетворить жизненные потребности людей, приносить пользу, то, что имеет ценность. В аналоговой экономике таким благом являются полезные товары и услуги.

В свою очередь, объектом информационной деятельности является информация, т. е. смыслы, созданные человеком и представленные им в виде данных на каком-либо языке взаимодействия как последовательность знаков, имеющих физическую реализацию. По определению цифровая экономика переводит благо в цифровой вид или, что то же самое, благо становится информацией или смыслом. Совпадение объектов деятельности цифровой экономики и информатики поддерживается совпадением предметов их деятельности. В табл. 4 приведены определения ряда понятий, связанных с предметной деятельностью человека, к которой отнесены общественные отношения при реализации процессов производства, распределения, обмена и потребления блага и информации для экономической и информационной деятельностей соответственно. В табл. 5 сравниваются экономическая и информационная деятельности, из чего можно сделать такие выводы:

— традиционный аналоговый способ реализации процессов экономической деятельности в принципе не оптимален из-за субъективизма,

ручного труда, неэффективности конкурентных процедур и ограничений при производстве и потреблении;

— процессы информационной деятельности реализуются автоматически при помощи цифровых технологий, которые строятся оптимально с точки зрения объема потребляемых ими ресурсов. Ограничения эффективности информационной деятельности связаны только с психофизиологией человека. Эти обстоятельства и определяют целесообразность перехода к цифровой экономике.

Таблица 4

Содержание предмета экономической и информационной деятельности

Предмет деятельности	Экономическая деятельность (аналоговая экономика)	Информационная деятельность и цифровая экономика
Процесс производства	Создание из природных и других экономических ресурсов продуктов и услуг, имеющих, соответственно, материальную и информационную основу	Создание человеком новых смыслов и их представление на каком-либо языке, цифровые модели аналоговых объектов
Процесс распределения	Деление всей совокупности созданных продуктов и услуг на части, каждая из которых предназначена определенному потребителю	Деление всей совокупности доступной информации на части по ее смысловому содержанию или другим признакам для использования определенным кругом пользователей
Процесс обмена	Превращение продуктов и услуг в товар путем согласования их товарной ценности и замена владельцами принадлежащих им товаров на товары других владельцев	Превращение информации в данные и передача их адресатам через физическую среду взаимодействия во времени (сохранение), в пространстве (распространение) и через изменение физической формы (обработка)
Процесс потребления	Удовлетворение определенных потребностей за счет использования блага (произведенных и приобретенных продуктов и услуг)	Удовлетворение определенных потребностей за счет использования доступной информации

Итак, процесс деятельности в цифровой экономике может быть описан как процесс информационного взаимодействия субъектов деятельности, результатом которого становится благо, представленное в виде тех или иных смыслов[1]. Выделим в нем интеллектуальный и материальный метауровни[2]:

[1] *Воробьёв А. И., Колбанёв М. О., Татарникова Т. М.* Оценка вероятностно-временных характеристик процесса предоставления информационно-справочных услуг // Изв. высш. учеб. заведений. Приборостроение. 2014. Т. 57. № 9. С. 15–18.

[2] *Колбанёв М. О., Татарникова Т. М., Микадзе С. Ю.* Модель информационного взаимодействия для предприятий сервиса // Приборостроение. № 9. 2014. С. 10–14;

— идеальный метауровень является продуктом мышления людей. Здесь рождается смысл, т. е. мысль, содержание некоторого высказывания. Процессы идеального метауровня — это процессы мышления;
— материальный метауровень обеспечивает обмен данными, т. е. материальными объектами, представляющими знаки языка взаимодействия.

Таблица 5

Сравнение процессов деятельности аналоговой и цифровой экономики

Процесс деятельности	Особенности экономической деятельности	Особенности информационной деятельности
Производство	Ограничения – природные и другие экономические ресурсы. Эффективность – соотношение результатов (выпуска продукции и услуг) и затрат	Ограничения – психофизиология человека, уровни развития науки и образования. Эффективность – соотношение известных и новых результатов, фактически достигнутых с помощью новой информации
Распределение	Способ реализации – сочетание властных решений и конкуренции Ограничения – человеческий фактор	Способ реализации – создание технологий для свободных распространения и поиска информации Ограничения – ресурсы для технологий
Обмен	Способ реализации – создание денег и инфраструктуры для их оборота	Способ реализации – создание стандартных форматов данных и инфраструктуры для хранения, распространения и обработки Ограничения – ресурсы для технологий
Потребление	Ограничено возможностями приобретения тех или иных товаров	Свободное, если только существует свободный доступ к информации Ограничения – психофизиология человека, ресурсы для технологий

Процессы материального метауровня — это процессы обмена данными, имеющими физическую форму сообщений и сигналов (рис. 10, а).

В соответствии с этой моделью методы обеспечения безопасности процессов информационного взаимодействия могут быть разделены на 3 группы (рис. 10, б):

Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Диалектика информационных процессов и технологий // Информация и Космос. 2014. № 3. С. 98–106.

— на идеальном метауровне обеспечивается защита смыслов с учетом человеческого фактора. Человек, обладающий секретным знанием, рассматривается как часть системы и одно из уязвимых мест в системе безопасности. Разрабатываются мероприятия, блокирующие такие ошибки людей, которые могут привести к успешным информационным атакам, имеющим цель раскрыть секретные смыслы противнику;
— на техническом уровне материального метауровня обеспечивается защита логических свойств сообщений, составленных на том или ином языке информационного взаимодействия, например, математическими методами криптографии путем перевода смыслов на язык, который закрыт от противника;
— на уровне физической среды материального метауровня обеспечивается защита сигнала и физических законов его существования, например, от попыток разрушить или модифицировать память, от перехвата побочных излучений или наводок медного кабеля, от воздействия на сигналы программным путем и др.

В условиях цифровой экономики при повсеместном использовании цифровых технологий и свободном обмене информацией безопасность физической среды и контента будут обеспечивать роботы. Например, на автомобильных дорогах, построенных на рынке AutoNet, безопасность дорожного движения уже не будет зависеть от поведения людей. Она будет полностью определяться программными агентами, сопровождающими движение беспилотного автомобиля. То же самое касается любых других физических процессов, включая процессы защищенного распространения данных [1] или систем долговременного хранения данных [2]. Они будут выполнены роботами строго в соответствии с заданием, в срок и с оптимальными затратами энергии.

Проблемой цифрового общества остается защита смыслов на верхнем идеальном метауровне модели информационного взаимодействия.

Формально смысл в этом случае можно охарактеризовать набором персональных данных коммуниканта. Эти персональные данные состоят из двух частей. Первая — это те данные, которые, по мнению коммуниканта, не подлежат распространению. Вторая должна быть передана

[1] *Верзун Н. А., Колбанёв М. О., Колбанёв А. М.* Энергетическая эффективность помехоустойчивого кодирования в беспроводных сетях Интернета вещей // Приборостроение. № 2. 2017. С. 143–149.

[2] *Верзун Н. А., Колбанёв М. О., Пойманова Е. Д.* Энергетические характеристики процесса долговременного хранения данных // Приборостроение. № 2. 2017. С. 158–164.

Рис. 10. а) обобщенная модель информационного взаимодействия, б) уровни обеспечения информационной безопасности

системе, т. к. без этого она не сможет предоставить требуемую услугу. Данными второго типа может быть, например, только адрес для определения направления перемещения на беспилотном автомобиле. Однако для получения более удобной услуги системе можно дополнительно сообщить количество пассажиров, вид перевозимого груза, их уникальные идентификаторы, время предполагаемой поездки в обратном направлении и другие данные. Ограничивающими факторами здесь является возможность использования данных, переданных системе для контроля пользователя. Чем больше персональных данных открыл коммуникант, тем проще организовать жесткий контроль за ним со стороны системы. С другой стороны, уменьшение числа данных, переданных системе, ухудшает качество получаемой услуги.

Следует утверждать, что в цифровой экономике усиливается противоречие между удобством и безопасностью, давно знакомое пользователям информационных технологий. Например, для повышения безопасности информационной деятельности следует использовать сложные пароли, чаще менять эти пароли, использовать шифрование, хотя оно задерживает обработку, и т. д. Все это затрудняет, делает менее комфортной работу с техникой. Принципиально существуют две полярные возможности, обеспечивающие разный уровень информационной безопасности субъекта цифровой деятельности:

1) использование открытых программных систем. Тогда пользователь может контролировать систему и самостоятельно принимать решения о распространении тех или иных персональных данных по сети;
2) использование закрытых программных систем. В этом случае систему контролирует не пользователь, а кто-то другой, знакомый с программным кодом. Этот «кто-то» имеет возможность распространять персональные данные пользователя, не сообщая ему об этом.

Следовательно, мир цифровой экономики, основанный на интегральном информационном поле, противоречив. С одной стороны, он способен предоставить самую удобную и качественную услугу, но с другой — в качестве платы за эти удобства он ограничивает личное пространство человека. Посмотрим на практику использования современных информационных систем. Социальная сеть Facebook — это пример закрытой системы. Она с 2015 года приняла по отношению к пользователям новую политику конфиденциальности. Эти «правила игры» распространяются на пользователей автоматически, если они продолжают пользоваться сервисами Facebook: «Используя наши сервисы,… вы соглашаетесь с… политикой использования данных…, а также с просмотром рекламы

на основании приложений и сайтов, которые вы используете». Эта политика социальной сети дала ей возможность без разрешения владельца передавать имеющиеся у нее данные третьим лицам [1].

Проведенный анализ позволяет сделать следующие выводы:

— схожесть субъектов, объектов и предметов цифровой экономики и информатики изменяет принципы защиты от угроз в процессе деятельности по сравнению с аналоговой экономикой;
— главным объектом защиты цифровой экономики является смысл деятельности, т. е. набор персональных данных, которые пользователь хочет сохранить как конфиденциальные;
— единственным способом обеспечения конфиденциальности является использование открытых информационных систем;
— современные системы не отвечают этому требованию.

[1] Facebook. Обновление наших правил и условий. URL: Режим доступа: свободный. https://www.facebook.com/about/terms-updates/?notif_t=data_policy_notice.

Глава 3. Целевой мониторинг глобального информационного пространства: информационно-психологические аспекты

Глобальное информационное пространство как среда информационно-психологического мониторинга. Сложившееся понимание информационного пространства связано сугубо с антропогенными источниками информации — информационными ресурсами, а также средствами информационного взаимодействия и информационной инфраструктурой. Так, например, под информационным пространством часто понимают совокупность результатов семантической деятельности человечества. Эти результаты могут пониматься как в переносном смысле, так и в идеалистическом, последний подход развивается в философии, а также в пара- и псевдонаучных исследованиях, тогда информационное пространство может пониматься как «мир имен и названий, сопряженный к онтологическому». В соответствии с Концепцией формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов единое информационное пространство представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей. Иными словами, единое информационное пространство складывается из следующих главных компонентов:

- информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации;
- организационные структуры, обеспечивающие функционирование и развитие единого информационного пространства, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации;
- средства информационного взаимодействия граждан и организаций, обеспечивающие им доступ к информационным ресурсам на основе соответствующих информационных технологий, включающие программно-технические средства и организационно-нормативные документы.

Из этого определения следует, что информационное пространство состоит из двух основных частей: информационной оболочки и организационно-технической части (рис. 11).

Рис. 11. Состав информационного пространства

Информационная оболочка в данном представлении информационного пространства занимает особое место, т. к. именно она создает среду применения организационно-технических средств. Информационную оболочку, как основу информационного пространства можно определить в виде специфической конструкции, представляющей собой множество каких-либо объектов, которые называют его точками: ими могут быть различные информационные источники. Отношения между этими точками определяют «геометрию»

пространства. При аксиоматическом ее построении основные свойства этих отношений выражаются в соответствующих аксиомах. Исходя из этого определения, *первичными (простыми) элементами* информационной оболочки информационного пространства являются элементы содержания существующих объектов (явлений): составные части объекта (явления) наблюдения, в том числе свойства, противоречия, тенденции развития и т. д. На этом уровне информационная оболочка состоит из двух частей (рис. 12):

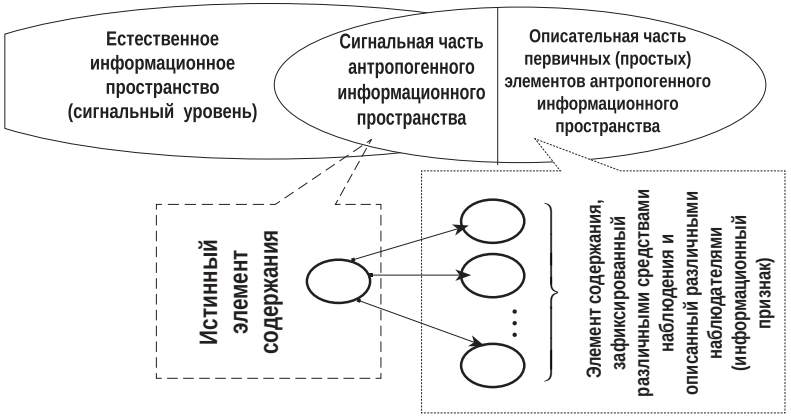


Рис. 12. Общая структура информационной оболочки на уровне первичных элементов

естественного информационного пространства, включающего элементы содержания, распространяющиеся в пространстве и времени при помощи объективно существующих носителей (сигналов) различной природы (сигнальный уровень). При этом часть этих элементов, зафиксированных антропогенными средствами приема информации, представляет собой подпространство естественного информационного пространства (*сигнальную часть антропогенного информационного пространства*);

описательной части антропогенного информационного пространства, включающей в себя различные описания (информационные признаки) одного и того же истинного элемента содержания. При этом следует понимать, что число описаний может быть сколь угодно большим, в зависимости от того, сколько человек интересуются объектом (явлением) действительности, подлежащим изучению.

Формирование сигнальной части антропогенного информационного пространства осуществляется приемниками при сканировании ими естественного информационного пространства. В его состав входят все те элементы содержания объектов (явлений), которые могут быть зафиксированы существующими приемными устройствами, функционирующими на различных физических (химических, биологических и т. п.) принципах, в том числе и органами чувств человека. При обнаружении известного (или неизвестного) сигнала осуществляется его интерпретация и последующее описание. Это описание представляет: а) численное значение и размерность принятого сигнала; б) его номер (шифр); в) какую-либо качественную оценку; г) название объекта (явления), к которому этот сигнал принадлежит; д) различного рода пояснения. Каждый из элементов описания назовем *элементарным (простым) текстовым элементом* антропогенной части информационного пространства. Он может быть представлен в *информационном продукте (источнике антропогенной информации) в виде* отдельного текста (или фрагмента текста), или текстом с графиками, изображениями и т. п. (заметка, статья, брошюра, книга, отчет о НИР и т. п.), отдельными изображениями, схемами. Таким образом, информационный продукт представляет собой один из сложных элементов (описаний) информационной оболочки. Правила формирования таких описаний (сложных конструкций) соответствуют правилам (грамматике) языка, на котором создается продукт, или правилам оформления соответствующих документов. Исходя из данных предположений, процесс формирования информационных ресурсов, циркулирующих в глобальном информационном пространстве, схематично может быть представлен так, как показано на рис. 13.

Структуризация этой части глобального информационного пространства осуществляется при помощи таких известных схем систематизации, как языки классификационного, словарного или дескрипторного типа. В дальнейшем подисточником информации будем понимать условное обозначение какого-либо документа или издания, которые служат не только важнейшими источниками, но и средством передачи целевой информации в пространстве и времени. Кроме того, к источникам информации относятся также люди (одушевленные источники), элементы предметно-вещественной среды и средства массовой информации (СМИ). Среди документов и изданий выделяют первичные и вторичные.

В *первичных* источниках информации по преимуществу содержатся новые сведения или новое осмысление известных идей и фактов. К ним относятся книги, за исключением справочников, периодические

Рис. 13. Процесс формирования информационных ресурсов

и продолжающиеся издания, специальные виды тематических изданий, экономические, финансовые, научно-технические и иные отчеты, диссертации, информационные карты и т. п. Особый вид источников информации представляют собой нормативно-правовые акты, которые:

— принимаются компетентным (уполномоченным на то) органом государственной власти или иной организацией при обязательной санкции государства. Нормативно-правовой акт всегда отражает волю государства, это властный и официальный документ;
— занимают определенное место в иерархической системе права. В частности, любой нормативно-правовой акт не должен входить в противоречие с вышестоящими нормативно-правовыми актами;
— характеризуются определенной процедурой вступления в силу (официальное опубликование, определенный срок с момента принятия);
— всегда облекаются в специально предусмотренную документальную форму, имеют установленную структуру, определенные реквизиты.

Во *вторичных* источниках информации содержатся главным образом сведения из первичных документов или о них. К ним относятся справочная литература, обзоры, реферативные журналы, библиотечные каталоги, библиографические указатели и картотеки и т. п. Важным источником информации этого типа является система депонирования неопубликованных источников. Она состоит в том, что рукописи статей, книг и т. п., представляющие интерес для небольшого числа специалистов, по решению издательств и редакций передаются на хранение в органы информации. Сведения об этих рукописях публикуются в информационных изданиях, а копии самих рукописей высылаются по запросам специалистов.

Человек является носителем информации сам по себе, он может выступать генератором информации (источником) или ее ретранслятором. Человек — самый сложный и в то же время весьма доступный источник информации. Он может быть и первоисточником, и вторичным источником информации, и источником дезинформации. Предметно-вещественная среда является носителями порой весьма ценной информации. Например, образцы продукции, произведенные за рубежом, обладающие привлекательными свойствами и импортируемые в значительных объемах, могут создавать впечатление о несовершенстве образа жизни в собственной стране.

К *средствам массовой информации* (СМИ) относятся все периодические издания, телевидение, радиовещание и Internet. В мире огромное количество самых разнообразных *периодических изданий*. Все они имеют свои особенности. Но всех их объединяет то, что они имеют бумажную основу.

Эта их особенность является причиной некоторой задержки в подаче информации. Она связана: во-первых, с необходимостью редактирования материала, печати и распространения; во-вторых, с зависимостью от конкретной типографии, осуществляющей выпуск материала. Поэтому, в настоящее время, данный тип СМИ ориентируется не столько на подачу оперативной информации, сколько на аналитику, рассуждения и т. п.

Радио и телевидение с точки зрения оперативности можно рассматривать как аналогичные источники, поскольку их общая черта и основная особенность — это донесение информации до конечного пользователя посредством электромагнитных колебаний. Вместе с тем, работать с данным источником несколько труднее — необходимо фиксировать полученные данные и переводить их в вид, удобный для дальнейшего анализа и обобщения. Основными особенностями *Internet* как хранилища информации являются:

— Internet — это распределенное хранилище информации, то есть информация разнесена по разным хранилищам, в том числе и физически;
— только часть, причем меньшая часть информации, выложенной в Internet, индексируется поисковыми машинами;
— в индексы поисковых машин информация попадает далеко не сразу;
— поисковые машины покрывают разные части Internet;
— алгоритм работы поисковиков разный.

В Internet информация хранится несколькими, интересными для деловой разведки, способами: общедоступно на сайте; общедоступно, но на отдельном сервере; в закрытых зонах (на закрытых страницах сайта и в закрытых серверах). Та информация, что выложена на общедоступном сайте, доступна и поисковым роботам и видна любому посетителю этого сайта. Именно эта информация выводится после запроса в поисковый сервер. Сложнее обстоит дело с общедоступной информацией, находящейся не на сайте, а на отдельном сервере (например, в базе данных). Эту информацию поисковик не видит и соответственно не выдаст по запросу, хотя она и общедоступна. Практически недоступна информация, находящаяся в закрытых зонах.

Сущность и содержание целевого (информационно-психологического) мониторинга глобального информационного пространства. *Информационно-психологический мониторинг глобального информационного пространства представляет собой* постоянный процесс добывания (сбора), накопления, структурирования, анализа и обобщения информации о направлениях, степени развития и эффективности

информационно-психологического воздействия на население в целом, отдельные социальные группы, руководящий состав системообразующих элементов политической и хозяйственной структуры общества, его политическое и военное руководство со стороны зарубежных государств и отдельных структур внутри страны. Необходимость проведения такого мониторинга связана с расширением масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Как отмечается в Доктрине информационной безопасности Российской Федерации, в настоящее время наблюдается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации [1]. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности. Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

Основное содержание информационно-психологического мониторинга глобального информационного пространства сводится к тому, что он является специально организованной и непрерывно проводимой системой мероприятий. Понятием специально организованной системы подчеркивается специфичность этого вида деятельности, утверждается необходимость создания специальной организации и применения для

[1] Доктрина информационной безопасности Российской Федерации // Российская газета. 6 декабря 2016 г.

выполнения задач деловой разведки особых методов и приемов, учитывающих частные закономерности, свойственные процессам мониторинга. В этой части определения устанавливается положение о том, что информационно-психологический мониторинг является системой действий, т. е. вскрытие информационно-психологических операций (ИПО) является не частными, изолированными актами, а единым процессом, который слагается из закономерно увязанных действий, направленных на достижение определенной цели. Сформулированные положения указывают также *конечную цель* информационно-психологического мониторинга — своевременное выявление угроз, уязвимостей, возможностей и иных факторов влияния на информационно-психологическое состояние общества и обеспечение руководства информацией, необходимой для принятия эффективного управленческого решения по устранению негативного влияния информационно-психологических операций.

Основными *принципами* информационно-психологического мониторинга, реализация которых обеспечивает достижение его цели, являются целеустремленность, непрерывность, активность, оперативность, скрытность, достоверность. *Целеустремленность* мониторинга заключается в строгом подчинении мероприятий по вскрытию замысла информационно-психологических операций, сосредоточении ее усилий на решение важнейших задач. Она достигается:

- правильным определением цели, задач, районов и объектов информационно-психологического воздействия на основе глубокого знания закономерностей информационной борьбы, взглядов на ее ведение, состояния и возможностей органов и средств информационно-психологических операций;
- комплексным ведением мониторинга по единому плану, оптимальным распределением усилий по задачам и объектам и целесообразным сочетанием централизованного и децентрализованного управления силами и средствами мониторинга.
- *Непрерывность* информационно-психологического мониторинга заключается в постоянном его ведении в любых условиях обстановки и достигается:
- обоснованным планированием по задачам, районам, объектам и времени;
- комплексным применением разнородных сил и средств с тщательным согласованием их действий между собой;
- целесообразной периодичностью мониторинга деятельности основных объектов;

— готовностью органов мониторинга к действиям в любых условиях обстановки, устойчивым управлением ими;
— наличием достаточно подготовленного резерва сил и средств мониторинга, современным его выполнением и правильным использованием.

Активность мониторинга заключается в настойчивом стремлении органов управления, сил и средств добыть необходимые сведения в любых условиях обстановки и всеми возможными способами. Она достигается:
— творческой и умелой организацией применения сил и средств мониторинга;
— проявлением сотрудниками мониторинга разумной инициативы, смелости и решительности действий, основанных на правильном понимании задач и реальных условий конкурентной обстановки.

Оперативность мониторинга заключается в добывании достоверных сведений в установленные сроки, быстрой их обработке, своевременном докладе руководству для немедленного использования. Она достигается:
— предвидением развития информационно-психологической обстановки;
— своевременной постановкой задач исполнителям;
— проведением мероприятий, обеспечивающих сокращение затрат времени на ввод в действие (перенацеливание) сил и средств мониторинга, добывание, сбор, обработку и доведение специальной информации;
— устойчивым и непрерывным управлением силами и средствами мониторинга;
— широким применением средств автоматизации.

Скрытность мониторинга заключается в сохранении в тайне всех проводимых руководством мероприятий по его проведению, введении противостоящей стороны в заблуждение относительно расположения и характера действий органов мониторинга. Она достигается:
— привлечением к планированию мониторинга строго ограниченного круга лиц;
— скрытными действиями сил и средств мониторинга;
— исключением шаблона во времени и способах проведения мероприятий по добыванию информации;
— умелым проведением мероприятий по маскировке своих действий.

Достоверность мониторинга заключается в добывании информации, полностью соответствующей фактической информационно-психологической обстановке, выявлении и правильной оценке истинных, демонстративных

и ложных объектов и действий органов информационной борьбы. Она достигается правильным выбором и распределением сил и средств мониторинга по задачам и объектам в соответствии с их возможностями, а также получением информации от различных источников, тщательным ее анализом, перепроверкой и при необходимости проведением доразведки.

Механизм информационно-психологического мониторинга глобального информационного пространства. В условиях стремительного развития информационного общества, информация становится не только стратегическим ресурсом, обеспечивающим общественно-политическое развитие общества, но и мощным средством воздействия на население в целом и на отдельных лиц в частности. В зарубежной и отечественной науке такое воздействие обычно называют информационно-психологическими операциями [1]. При этом чаще всего исследователи, говоря об ИПО, имеют в виду воздействие на общественное сознание или поведение военнослужащих (представителей силовых структур) какой-либо страны в целом. Это объясняется, в первую очередь, масштабом осуществляемых информационно-психологических действий, масштабом привлекаемых сил и средств и масштабом ожидаемых операций. Такой подход является справедливым с той точки зрения, что в соответствии с принятой в отечественной военной науке системой категорий и понятий термин «операция» предполагает именно масштабные действия участвующих в ее проведении сил и средств.

Широкомасштабные информационно-психологические действия предполагают применение в рамках общественно-политических, профессионально-деловых, социокультурных, семейно-родственных, социально-бытовых, дружеских и случайных социальных связей таких способов, как ознакомление, аргументация, суждение, убеждение, очевидность, хитрости, разочарование, отравление сознания, контринформирование, контрпропаганда, дезинформация, развенчание слухов, пропаганда, индокринация, подрывная деятельность, террор и другие. При этом личность рассматривается, как правило, как абстрактный элемент социального общества, а не конкретное должностное лицо [2]. Начало и ход проведения ИПО такого рода достаточно легко идентифицируется, так как основными средствами и формами их осуществления являются

---

[1] *Манойло А. В.* Информационно-психологическая война как средство достижения политических целей. URL: http://www.ict.edu.ru/ft/002468/manoylo.pdf; *Грачев Г. В., Мельник И. К.* Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: Эксмо, 2003. 112 с.

[2] *Грачев Г. В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС, 1998. 125 с.

имеющие публичный и массовый характер средства массовой коммуникации: печатные и электронные СМИ, Internet, а также различные массовые мероприятия: совещания, конференции, брифинги, тренинги, митинги и т. п. Кроме того, к таким формам относятся:

— литература (в том числе художественная, научно-техническая, общественно-политическая, специальная);
— искусство (в том числе различные направления так называемой массовой культуры);
— образование (в том числе системы дошкольного, среднего, высшего и среднего специального государственного и негосударственного образования, система так называемого альтернативного образования);
— воспитание (все разнообразные формы воспитания в системе образования, общественных организаций — формальных и неформальных, система организации социальной работы).

Информационно-психологические действия в отношении конкретного лица, особенно наделенного важными государственными, экономическими или иными полномочиями, характеризуются:

во-первых, задействованием для достижения цели (например, превращение лица в так называемого «агента влияния», его дискредитации) ресурсов, часто сравнимых с проведением классических ИПО;

во-вторых, длительным, как правило, сроком воздействия;

в-третьих, масштабом последствий при изменении мировоззрения таких лиц, что должно привести к нарушению нормального функционирования органов власти и управления, общественно-политических и экономических организаций и других сложных социальных субъектов.

В связи с этим такие ИПО относятся к классу угроз дестабилизирующего концентрированного воздействия и дестабилизирующей операции, представляющих совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени, разнородных единичных и массированных угроз, которые формируются как одновременно, так и последовательно, в соответствии с единым планом и замыслом, и которые в рассматриваемом случае нацелены на дискредитацию или подчинение ключевых представителей руководства страны, других системообразующих общественно-политических, экономических, военных и т. п. структур [3].

[3] *Левкин И. М., Левкина С. В., Галкова Е.* А. Угрозы национальной безопасности и их информационно-признаковые модели // Геополитика и безопасность. 2015. № 1(29). С. 88–94.

Главной особенностью информационно-психологических операций в отношении должностного лица является использование наряду с открытыми видами информационно-психологического воздействия (пропаганда, агитация, слухи, дезинформирование, двойные стандарты, мнимые прогнозы, конъюнктурные оценки) широкого спектра скрытого принуждения людей (манипулятивное воздействие, нейролингвистическое программирование, психологическое давление, рефлексивное управление, подкуп, шантаж, обман). Это, в свою очередь, приводит к особенностям построения и использования информационно-признаковых моделей ИПО, к основным из которых относятся следующие.

Привязка элементов информационно-признаковых моделей ИПО во времени к графику деятельности должностного лица. Данная особенность связана с тем, что скрытые виды информационного воздействия наиболее эффективны при непосредственном контакте должностного лица с источником воздействий. Это может происходить, в первую очередь при осуществлении международных саммитов, визитов различного рода (официальных, рабочих, культурных), проведении переговоров, неофициальных встреч. Кроме того, организаторы ИПО, как правило, хорошо осведомлены о графике работы должностного лица (хотя бы на ближайшую перспективу) и могут в преддверии этих мероприятий усиливать открытые информационно-психологические воздействия, как на социальную среду, так и на само должностное лицо и/или его ближайшее окружение.

Так, даже в период нормальных взаимоотношений РФ со странами Запада в 2005–2006 гг. мощная психологическая операция против лидеров РФ была приурочена к июльскому 2006 года саммиту руководителей стран G8 в Санкт-Петербурге, который впервые проводился под председательством России. Некоторыми признаками этой кампании стали:

- использование целого ряда неурегулированных, спорных проблем международных отношений (иранская ядерная программа, взаимоотношения со странами СНГ, «цветные революции» и «горячие точки» на постсоветском пространстве, проблемы энергетической безопасности и др.) в качестве информационного повода для наращивания давления на Россию и ее руководство в ходе подготовки и принятия решений;
- использование в качестве главного информационного посыла — сомнение в возможности и целесообразности проведения саммита 15–17 июля в Санкт-Петербурге;
- последовательность и целенаправленность проводимых акций информационно-психологического воздействия (публикация

в середине марта 2006 г. в США, новой «Стратегии национальной безопасности», фактически ужесточающей официальную позицию Вашингтона по отношению к России и совпадающую по времени публикации документа с подведением итогов парламентских выборов на Украине и президентских выборов в Белоруссии в марте 2006 г.; обнародование представителями Пентагона документа, в котором утверждалось, что российские разведструктуры, якобы, информировали С. Хусейна о передвижениях войск США во время вторжения в Ирак в 2003 г.; проведение в столице Литвы 4 и 5 мая 2006 года конференции «Общее видение добрососедства» организации стран Балтийского и Черноморского регионов);

- координация по времени осуществления пропагандистских акций;
- постепенное наращивание усилий в их организации и проведении [1].

Лавинообразное нарастание информационно-психологического давления на РФ произошло в связи с событиями в Украине в феврале 2014 года и последовавшими за ними возвращением Крыма в состав России и событиями в Новороссии. Возможность выявления отдельных элементов информационно-признаковых моделей — скрытых информационно-психологических воздействий ИПО по информационным признакам их результатов. Результатами таких воздействий могут быть: изменение мнения по важным вопросам государственного и военного строительства; увольнение перспективных руководителей, занимающих государственные позиции; принятие решений, способных нанести ущерб государству или его основным структурам. В конечном итоге эффективным результатом продолжительных скрытых информационно-психологических воздействий может стать формирование «агентов влияния», т. е. лиц, осуществляющих деятельность в интересах другого государства, с использованием для этого своего высокого служебного положения в верхних эшелонах власти — руководстве страны, политической партии, парламенте, средствах массовой информации, а также науке, искусстве и культуре.

Наиболее ярким примером формирования «агентов влияния» со стороны американских спецслужб явилась вербовка некоторых лиц из группы советских стажеров, находившихся в конце пятидесятых — начале шестидесятых годов в Колумбийском университете [2].

---

[1] Неадекватное понимание своих интересов или некоторые особенности антироссийского ПиАра в 2006 году. URL: http://www.wv2.vrazvedka.ru/index.php?option=com_content&view=article&id=36.

[2] *Доронин А.* Агенты влияния // Оборона и безопасность. 26.11.2002. URL: http://www.nomad.su/?a=5–200211260025; *Дроздов Ю. И.* Вымысел

Немало информационных признаков свидетельствует об эффективности информационно-психологического воздействия на Генерального секретаря ЦК КПСС М. С. Горбачева. Одна только фраза премьер-министра Великобритании М. Тэтчер: «Я думаю, Горбачев — это тот человек, с которым можно иметь дело» многого стоит [1].

Увеличение значимости информационных признаков, характеризующих деловые и личностные качества должностного лица, в структуре элементов информационно-признаковой модели ИПО. Наличие таких признаков позволяет:

во-первых, более точно определить перечень возможных видов информационно-психологического воздействия на конкретное должностное лицо;

во-вторых, повысить качество прогнозирования результатов скрытого информационно-психологического воздействия на него.

Так, например, такие свойства характера, как непомерные амбиции, нарциссизм, и ряд других качеств позволили использовать в отношении Горбачева такие виды информационно-психологического воздействия, как восхваление, поощрение [2].

Усиление взаимосвязи между результатами открытых и скрытых видов информационно-психологического воздействия. Повышение интенсивности открытых видов информационно-психологических в отдельные промежутки времени позволяют более точно определить круг должностных лиц, в отношении которых будут применяться отдельные виды скрытого воздействия.

Учет перечисленных особенностей предполагает при разработке информационных признаков ИПО с равным вниманием рассматривать все основные структурные элементы угрозы: объективно сложившаяся совокупность неблагоприятных условий и факторов (землетрясения, наводнения, природные пожары и т. п.); субъективные намерения (замыслы, желания), объективную возможность реализации субъективных намерений, наличие существующих сил и средств, наличие необходимых и достаточных условий, создаваемых субъектом и складывающихся без участия субъекта.

исключен. Записки начальника нелегальной разведки. URL: http://bungalos.ru/b/drozdov_vymysel_isklyuchen_zapiski_nachalnika_nelegalnoy_razvedki/34.

[1] Человек, с которым можно иметь дело. Визит М. С. Горбачева в Англию. URL: http://www.22–91.ru/etot-den-v-istorii-sssr/9/chelovek-s-kotorym-mozhno-imet-delo-vizit-ms-gorbacheva-v-angliju.

[2] *Леонов Н. С.* Агенты влияния. — URL: http://www.index43su.narod.ru/notes/agentsofimpact.htm.

Фрагмент алфавита агрегированных информационных признаков ИПО в отношении должностного лица как угрозы приведен в таб. 6.

Таблица 6

Алфавит агрегированных информационных признаков информационно-психологической операции (фрагмент)

Элементы угрозы	Информационные признаки угрозы
Объективно сложившаяся совокупность неблагоприятных условий и факторов, приводящих к снижению жизненного уровня населения страны	a_1 – землетрясения; a_2 – наводнения, сели; a_3 – природные пожары; a_4 – извержения вулканов; a_5 – засуха; a_6 – ураганы, смерчи; a_7 – климатические катастрофы
Субъективные намерения (замыслы, желания)	b_1 – публичные заявления высшего руководства ведущих зарубежных государств о необходимости изменения политики страны (взглядов на отдельные события международной жизни); b_2 – поддержка подобных заявлений другими странами; b_3 – публичные заявления действующих политиков ведущих зарубежных государств; b_4 – принадлежность политика к партии (группе), отрицательно относящейся к РФ; b_5 – публикации в средствах массовой информации; b_6 – инициирование в международных организациях мероприятий, наносящих вред стране; b_7 – визиты в зарубежные страны с целью поддержки антироссийских настроений или давления на руководство; b_8 – призыв к принятию различного рода санкций (политических, экономических, финансовых и т.п.); b_9 – создание коалиций, противостоящих РФ; b_{10} – проведение мероприятий по изучению должностного лица; b_{11} – подсказки в вопросах принятия решений; b_{12} – проведение мероприятий индивидуального информационно-психологического воздействия (убеждение, подкуп, шантаж и т.п.)
Объективная возможность реализации субъективных намерений	c_1 – наличие у должностного лица специфических черт характера (жадность, трусость, нарциссизм, властолюбие, склонность к злоупотреблению спиртными напитками, любвеобильность и т.п.); c_2 – возможность контактов с должностными лицами на официальных мероприятиях; c_3 – возможность проведения частных встреч; c_4 – развитие инфокоммуникационных технологий в стране; c_5 – возникшие трудности в развитии (военном, политическом, экономическом, финансовом и т.п.) страны; c_6 – возможность нанесения ущерба (военного, политического, экономического, финансового и т.п.) стране; c_6 – наличие пробелов в законодательстве страны, регламентирующего вопросы национальной (в том числе информационной) безопасности

Элементы угрозы	Информационные признаки угрозы
Наличие существующих сил и средств	d_1 – наличие доктрины информационной войны; d_2 – наличие опыта проведения информационно-психологических операций; d_3 – наличие органов информационной войны; d_4 – наличие высококвалифицированных специалистов в сфере информационно-психологических операций; d_5 – наличие средств информационно-психологического воздействия (печатные и электронные СМИ, Internet, психотронные генераторы и т.п.); d_6 – наличие подконтрольных организаций, ведущих политическую деятельность в РФ («иностранных агентов»); d_7 – выделение требуемого объема финансовых средств
Наличие необходимых и достаточных условий	e_1 – обострение борьбы за власть; e_2 – коррупция в верхних эшелонах власти; e_3 – несовершенство судебной системы; e_4 – несовершенство выборного законодательства; e_5 – высокий уровень преступности; e_6 – национализм; e_7 – наличие легальных экстремистских организаций; e_8 – снижение финансирования социальных сфер; e_9 – общее падение уровня образования, нравственности и т.п.; e_{10} –религиозная нетерпимость
Факторы, обусловленные деятельностью субъекта	g_1 – попытки принятия самостоятельных решений в международной политике; g_2 – возражения против незаконных действий зарубежных государств на международной арене; g_3 – предотвращение различных видов экспансии (экономической, финансовой, культурной и т.п.); g_4 – ужесточение политики в отношении некоммерческих организаций; g_5 – увольнение из высших руководящих органов сотрудников, исповедующих сомнительные экономические теории (неокейнсианство, монетаризм, нейроэкономика и т.п.)
Условия, складывающиеся без участия субъекта	h_1 – появление на международной арене новых акторов, претендующих на лидерство; h_2 – появление внутри страны новых акторов, претендующих на лидерство; h_3 – ухудшение международной обстановки; h_4 – высокая волатильность цен на стратегические виды сырья (в первую очередь на энергоносители); h_5 – рост разрыва между благосостоянием жителей РФ и развитых зарубежных стран; h_6 – создание за рубежом благоприятных условий для утечки капитала, специалистов высшей квалификации, перспективной молодежи и т.п.; h_7 – обострение борьбы за природные ресурсы, транспортные коммуникации и т.п.; h_8 – обострение идеологической борьбы

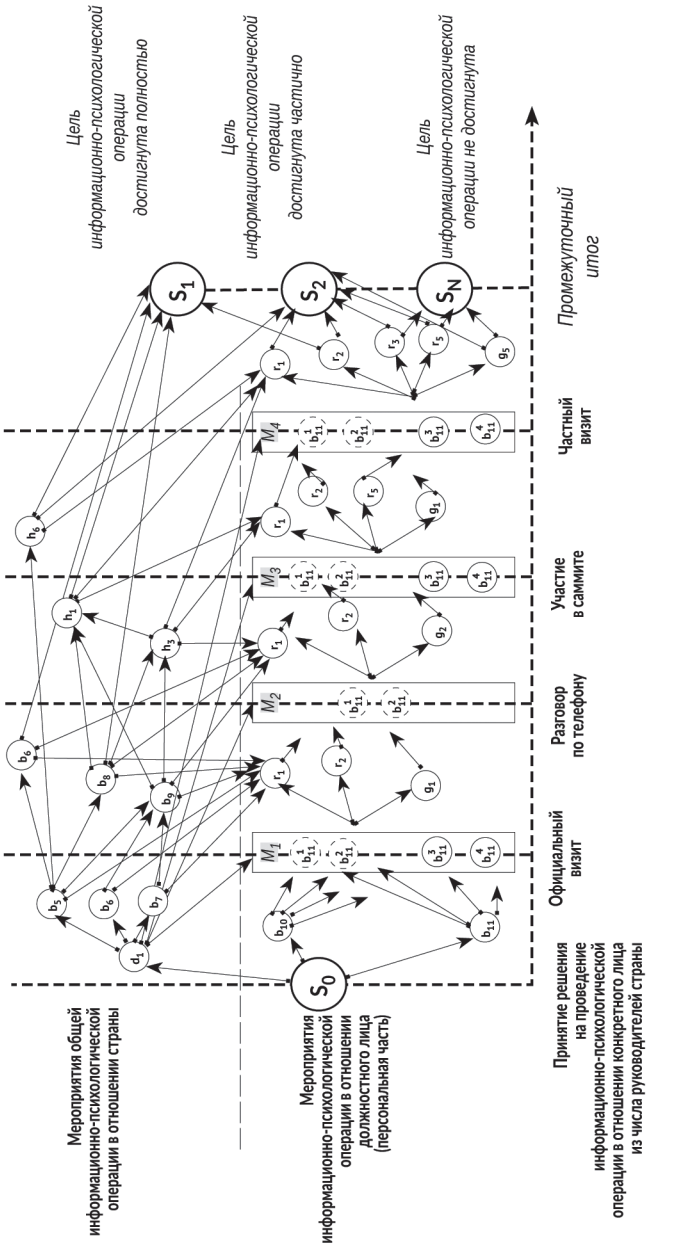


Рис. 14. Агрегированная информационно-признаковая операция в отношении руководства страны (фрагмент)

Наличие алфавита информационных признаков элементов угрозы типа ИПО и результатов информационно-психологического воздействия позволяет построить ее информационно-признаковую модель (ИПМ) в сетевой форме (фрейм-сценарий). С учетом ранее обозначенных особенностей построения таких моделей в рассматриваемом случае агрегированная ИПМ ИПО в терминах информационных признаков-мероприятий будет иметь вид, представленный на рис. 14.

На этом рисунке обозначено:

S_0 — принятие решения на проведение информационно-психологической операции в отношении представителя руководства страны;

S_1 — цель информационно-психологической операции достигнута полностью;

S_2 — цель информационно-психологической операции достигнута частично;

S_3 — цель информационно-психологической операции не достигнута;

b_{11}^i — виды информационно-психологического воздействия, $i = \overline{1, N}$;

скрытые мероприятия информационно-психологического воздействия обозначены штрих-пунктиром.

В этой модели каждое мероприятие, в свою очередь, может быть представлено информационно-признаковой моделью в виде иерархического взвешенного графа типа «корневое дерево» (рис. 15). Процесс вскрытия ИПО в отношении должностного лица в целом имеет следующие основные особенности.

Во-первых, в силу того, что информационно-психологическое воздействие в открытом виде ведется в любых формах политической (военной, экономической, финансовой и т. п.) борьбы, явные мероприятия могут идентифицироваться достаточно легко по совокупности соответствующих информационных признаков. В этом случае может быть использован типовой подход к работе с ИПМ: вскрытие мероприятия — прогнозирование наступления (усиления интенсивности) связанного с ним последующего (последующих) мероприятия — оценка эффективности проводимых мероприятий — выработка предложений по устранению негативных явлений выявленных мероприятий.

Рис. 15. Информационно-признаковая модель мероприятия информационно-психологической операции

Во-вторых, эффективность проведения скрытых мероприятии информационно-психологического воздействия на руководство страны (и иных должностных лиц) может быть оценена путем вскрытия информационных признаков их результатов, т. е. в обратном направлении развития ИПМ — характер результатов может свидетельствовать: во-первых, о виде проведенного мероприятия информационно-психологического воздействия; во-вторых, о возможности проведения подобных мероприятий в дальнейшем. Причем время и условия проведения таких мероприятий становятся известными, так как они привязаны к официальному графику деятельности должностного лица. Вскрытие факта проведения ИПО, в отношении высших руководителей страны при помощи предлагаемых информационно-признаковых моделей может быть осуществлено следующим образом.

В схеме проведения общей ИПО.

На первом этапе осуществляется сбор информационных признаков, свидетельствующих о проведении ИПО и выделение из них тех, которые

позволяют идентифицировать информационно-психологические операции в отношении конкретного должностного лица.

Вероятность того, что информационно-психологическое воздействие направлено на конкретное должностное лицо, может быть вычислена при помощи известной формулы:

$$P = 1 - (1 - a_i)(1 - b_j)...(g_s), \quad (1)$$

где $a_i, b_j, ...g_s$ – информационные признаки направленности открытых мероприятий ИПО на конкретное должностное лицо.

На втором этапе в соответствии с логикой ИПИ осуществляется прогнозирование наступления (усиления интенсивности) одного или нескольких мероприятий, связанных с выявленным. Это позволяет:

— нацелить средства мониторинга на выявление информационных признаков прогнозируемого мероприятия, которые должны появиться в ближайшей перспективе;
— при появлении этих признаков сделать вывод о том, что с вероятностью, рассчитанной при помощи выражения (1), проводится именно прогнозируемое мероприятие.

На третьем этапе по результатам выявленных мероприятий осуществляется прогнозирование варианта реализации ИПО в отношении должностного лица в схеме проведения персональной части ИПО.

На первом этапе вскрываются информационные признаки уязвимых индивидуально-психологических качеств должностного лица (нарциссизм, алчность, гордыня, любвеобильность, склонность к употреблению спиртных напитков, завышенная потребность в самоактуализации).

В схеме проведения ИПО в отношении конкретного должностного лица каждый следующий этап выявления информационных признаков информационно-психологического воздействия привязывается к проведению протокольных (частных) мероприятий в процессе выполнения этим лицом своих профессиональных обязанностей. При этом по окончании мероприятия производится анализ принимаемых решений на предмет их соответствия интересам соответствующей государственной структуры. Перечень информационных признаков, характеризующих ошибочные решения, свидетельствует:

во-первых, об использовании уязвимых качеств должностного лица при помощи проведения соответствующих скрытых мероприятий информационно-психологического воздействия;

во-вторых, о возможности использования этих мероприятий в процессе участия должностного лица в следующем протокольном (или частном) мероприятии.

Вычисление вероятности достижения цели ИПО в отношении должностного лица (наступления каждого из конечных состояний S_1, S_2,…, S_N на рис. 14) осуществляется следующим образом. При превышении вероятности проведения текущего мероприятия информационно-психологического воздействия некоторой заданной величины (например, 0,75) ему присваивается значение индикатора равным 1. Таким образом, предполагается, что это мероприятие представляет собой проявившийся информационный признак связанного с ним следующего мероприятия. По числу проявившихся таким образом информационных признаков с использованием выражения (1) вычисляется вероятность проведения связанного с ними следующего мероприятия. Таким образом, вычисляются индикаторы всех мероприятий построенной информационно-признаковой модели.

Так как конечные состояния ИПО представляют собой полную группу событий, апостериорная вероятность каждого из них может быть вычислена при помощи формулы Байеса [1]. Для модели, представленной на рис. 14, это будет выглядеть следующим образом:

$$P\left(S_i / f_j\right) = \frac{P\left(S_i\right) P\left(f_j / S_i\right)}{\sum_j P\left(S_i\right) P\left(f_j / S_i\right)}, \qquad (2)$$

— где априорная вероятность конечного результата ИПО; апостериорная вероятность конечного результата ИПО при проявлении информационного признака. Таким образом, информационно-признаковое моделирование информационно-психологических операций в отношении высшего руководства страны (и иных должностных лиц) позволяет:

— своевременно вскрыть факт нацеленности ИПО на конкретное должностное лицо (группу лиц);

---

[1] *Вентцель Е. С.* Теория вероятностей и ее инженерные приложения: учебное пособие / Е. С. Вентцель, Л. А. Овчаров. 5-е изд., стер. М.: КНОРУС, 2016. 480 с.

— определить вероятный перечень основных мероприятий открытого и скрытого информационно-психологического воздействия;
— обосновать вариант развития ИПО;
— получить численные оценки возможных результатов ИПО в отношении высшего руководства страны (и иных должностных лиц).

В общем виде методика использования информационно-признаковых моделей информационно-психологических операций для оценки направлений их развития представлена на рис. 16.

В соответствии с этой методикой на первом этапе выявляются информационные признаки как открытых, так и скрытых информационно-психологических воздействий. При этом выявление информационных признаков открытых информационно-психологических воздействий осуществляется по материалам СМИ, заявлениям ведущих зарубежных политиков (как действующих, так и отставных), документам государственных и общественных зарубежных и отечественных организаций. В свою очередь, выявление информационных признаков скрытых информационно-психологических воздействий осуществляется путем экспертизы управленческих решений, принятых как после плановых или внеплановых встреч с зарубежными партнерами (конкурентами), так и после них. По совокупности выявленных информационных признаков далее определяется:

во-первых, вероятность проведения соответствующих мероприятий информационно-психологических воздействий, а также прогнозируется вариант дальнейшего развития информационно-психологической операции;

во-вторых, вероятность проведения скрытого информационно-психологического воздействия и его характер.

Так, если бы во второй половине 80-х гг. XX в. были своевременно проанализированы такие задачи созданной под эгидой США Трехсторонней комиссии, как проведение согласованных мероприятий по организации международной поддержки перестройки, осуществляемой М. С. Горбачевым, а также учтена характеристика, данная этой комиссией Горбачеву как человеку неосторожному, внушаемому и весьма честолюбивому [1], то стали бы понятны многие решения, принимаемые Генеральным секретарем ЦК КПСС в самом начале его международной и внутриполитической деятельности.

---

[1] *Панарин И.* Первая мировая информационная война. Развал СССР. СПб.: Питер, 2010. 256 с.

Рис. 16. Методика использования информационно-признаковых моделей информационно-психологических операций для оценки направлений их развития

Выявленные информационные признаки позволяют сформировать исходные данные для расчета текущей интегрированной оценки состояния информационно-психологической безопасности и далее выработать практические рекомендации по устранению негативного влияния информационно-психологических воздействий. В основу методики интегральной оценки информационно-психологической безопасности страны (региона, объекта) может быть положена методика расчетов индексов политической, военной, экономической и других видов безопасности, разработанная ПИР-центром [1]. Предлагаемая методика предполагает расчет интегрального индекса информационно-психологической безопасности (*ИИИПБ* = I_{Ψ}) по следующей формуле [2]:

$$ИИИПБ = \frac{G_o}{N}\left[f_1(1-\beta_1) + f_2(1-\beta_2) + \ldots + f_N(1-\beta_N)\right] +$$

$$+\frac{G_{дл}}{K}\left[h_1(1-\gamma_1) + h_2(1-\gamma_2) + \ldots + h_K(1-\gamma_K)\right]\Delta_i,$$

где G_o – коэффициент масштаба информационно-психологического воздействия на общую информационно-психологическую обстановку; N – число открытых видов информационно-психологических воздействий; f_n — коэффициент важности *n*-го открытого вида информационно-психологического воздействия; β_n – вероятность использования (степень напряженности информационно-психологической безопасности) *n*-го открытого вида информационно-психологического воздействия в информационно-психологической операции; G_n – коэффициент масштаба информационно-психологического воздействия на конкретную систему управления; K – число высокопоставленных должностных лиц, на которых может быть осуществлено скрытое информационно-психологическое воздействие; h_k – коэффициент важности (значимости) *k*-го

[1] Методология iSi. URL: http://www.pircenter.org/static/isi-methodology. 30.11.2015.

[2] *Левкин Е. О.* Особенности построения информационно-аналитического фрагмента ситуационного центра мониторинга информационно-психологической безопасности // Материалы научно-практической конференции НИУ ИТМО, 3 ноября 2015 г.

высокопоставленного должностного лица в системе управления; γ_k – вероятность эффективного использования скрытого информационно-психологического воздействия на *k*-е высокопоставленное должностное лицо; Δ_i – коэффициент значимости *i*-го объекта управления.

Основными особенностями предлагаемой методики являются:

1. Определение вероятности использования *n*-го открытого вида информационно-психологического воздействия β_n как степени напряженности информационно-психологической обстановки при помощи метода «трех групп» [3] по модернизированной формуле:

$$\beta_n = \frac{4P_n + H_n}{4P_n + 4П_n + H_n},$$

где P_n – число положительных информационно-психологических событий, $П_n$ — число негативных информационно-психологических событий, H_n — число нейтральных информационно-психологических событий. Значения величин P_n, $П_n$, H_n могут быть определены методом ивент-анализа (или контент-анализа) [4].

2. Определение вероятности эффективного использования скрытого информационно-психологического воздействия на высокопоставленное должностное лицо как отношения числа принятых некачественных управленческих решений к их общему числу после каждой официальной (или частной) встречи с зарубежными партнерами (конкурентами).

3. Величины G_o, G_n, f_n, h_k и Δ_i определяются методами экспертного опроса.

Таким образом, построение информационно-аналитического фрагмента ситуационного центра мониторинга информационно-психологической безопасности предлагаемым способом позволит:

---

[3] *Левкин И. М.* Теория и практика информационно-аналитической работы. Курск, 2011. 389 с.

[4] Ивент-анализ. URL: http://www.all-politologija.ru/knigi/politicheskij-analiz-i-prognozirovanie-axremenko/ivent-analiz-sozdanie-metoda; Контент-анализ. URL: http://www.psyfactor.org/lib/content-analysis3.htm.

во-первых, своевременно вскрывать факты усиления интенсивности общего информационно-психологического воздействия на общественно-социальную среду;

во-вторых, выявлять взаимосвязи между скрытыми информационно-психологическими воздействиями на высокопоставленных должностных лиц и принимаемыми ими управленческими решениями после проведения официальных и частных мероприятий с зарубежными партнерами (конкурентами);

в-третьих, получать численные значения изменения уровня информационно-психологической безопасности страны (объекта) и вырабатывать предложения по снижению негативного влияния открытых и скрытых видов информационно-психологического воздействия;

в-четвертых, обеспечить рациональный обмен информацией в информационной структуре ситуационного центра мониторинга информационно-психологической безопасности.

Глава 4. Противодействие информационному вандализму, криминалу и терроризму

Современному обществу свойственен ряд устойчивых тенденций. Идет активное развитие различных информационно-телекоммуникационных систем и средств с глобальным охватом населения Земли. Чем дальше, тем выше становится уровень информатизации общества [1]. Непрерывно расширяются возможности по предоставлению государственным структурам, бизнесу, гражданам, социальным группам различных функций по обращению с информацией. К таким функциям относятся доступ к накопленным мировым информационным ресурсам (ИР), формирование собственных ИР и оперативное предоставление их широким слоям общества. На граждан различных стран, городов, других населенных пунктов через радио, телевидение, Интернет, газеты, журналы, книги, фильмы, компьютерные игры, обучение и общение идет нарастающий поток разнородной, зачастую противоречивой и недостоверной информации. Увеличивается зависимость поведения населения от содержания этого информационного потока. Такой поток на различных уровнях несет в себе как позитивную, так и деструктивную составляющую. В деструктивном плане он может приводить к нервозам, депрессии, страхам, фобиям людей, к различным конфликтам в обществе и попыткам их разрешить незаконным путем, реализацией асимметричных действий, наносящих существенный моральный и материальный ущерб населению. Можно сказать, что в последние годы наблюдается существенный

[1] *Юсупов Р. М., Заболотский В. П.* Концептуальные и научно-методологические основы информатизации. СПб.: Наука, 2009. 542 с.

рост информационно-психологических угроз для населения. В качестве деструктивных составляющих таких угроз могут выступать:

- широко тиражируемые ложные сведения о государственных, политических, религиозных деятелях, участниках различных выборных кампаний;
- ложные сообщения об авариях на предприятиях промышленности (атомных электростанциях, химических заводах и других), о заминированных домах, поездах, самолетах, о финансовых крахах компаний, провокации и слухи в политической сфере;
- различного вида информация, вызывающая страх, агрессию, недовольство, раздражительность, порождающая сомнения, призывающая к деструктивным действиям;
- информационные сигналы, изменяющие психофизическое состояние людей, повышающие их утомляемость, вызывающие головные боли, повышающие давление и другие;
- деструктивные программы, как отрицательно влияющие на людей, так и дезорганизующие различные системы управления, вычислительные сети и технические средства и так далее.

Известно много случаев таких деструктивных воздействий, получивших большой резонанс в мире:

- скандальные информационные события, связанные с выборными кампаниями в США и Европе в 2016–2017 гг.;
- множественные нарушения информационной безопасности и поражения сети Интернет различными компьютерными вирусами, программами-«шпионами», деструктивными закладками;
- передачи по отечественному телевидению специальных сигналов и видеоинформации в период перестройки и в настоящее время;
- показ по японскому телевидению одной из серий про покемонов, спровоцировавшей приступы эпилепсии у детей;
- случаи насилия с применением оружия детьми после просмотра агрессивных и провоцирующих фильмов, участия в негативных компьютерных играх в развитых странах;
- публикация скандальных карикатур на пророка Мухаммеда датской газетой Jyllands-Posten в сентябре 2005 г., перепечатанных позже в газетах Норвегии (Magazinet), Франции (FranceSoir, Liberation, LeMonde), Германии (DieWelt), Испании (ElPais), Бельгии (DeStandaard) и других;
- информационный вандализм и криминал со стороны различных сект;

- в какой-то мере, деструктивные информационные воздействия через средства массовой информации, спровоцировавшие мировой экономический кризис, и др.

По экспертным оценкам величина ущерба от этих воздействий ежегодно в мире исчисляется в миллиардах и триллионах долларов. Все эти деструктивные воздействия могут быть подразделены на **мероприятия информационного вандализма, криминала и терроризма**, которые можно рассматривать не только как угрозы информационно-технической (ИТБ), но и информационно-психологической безопасности (ИПБ). Напомним, что ИТБ и ИПБ определяют суть современного понятия «информационная безопасность».

Информационный вандализм (ИВ) — понятие довольно новое. Это одна из современных форм вандализма — умышленного и бессмысленного уничтожения, разрушения культурных, материальных ценностей и нематериальных активов. Под информационным вандализмом предлагается понимать деструктивные действия при обращении с различного рода информацией, не обусловленные террористическими и криминальными целями. Такой вандализм является следствием безграмотности, любопытства, безответственности, непродуманной рекламы, некорректных высказываний по радио и телевидению, необдуманных публикаций карикатур, недостоверных порочащих фактов.

Общая направленность ИВ — это разрушение имеющейся информационной среды. Несмотря, на первый взгляд, на безобидность информационного вандализма, по масштабности он существенно перекрывает информационный криминал (ИК) и информационный терроризм (ИТР) и наносит не меньший ущерб обществу, чем ИК и ИТР.

Информационный криминал — это действия отдельных лиц или групп, направленные на взлом систем защиты, на хищение, уничтожение, искажение информации, а также формирование (разработку) и распространение деструктивных информационных воздействий в корыстных или хулиганских целях. Он отличается от ИТР, прежде всего, целями. Формы реализации деструктивных действий у них практически одни [1].

Под **информационным терроризмом** понимается вид террористической деятельности, ориентированный на принуждение к реализации политических, экономических, религиозных, идеологических и других целей через деструктивные действия в сфере информации. Различают кибер-, телевизионный,

[1] *Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С.* Информационное оружие как геополитический фактор и инструмент силовой политики. М.: Ин-т систем. анализа РАН, 1997. 37 с.

телефонный, музыкальный и другие виды информационного терроризма. Одним из примеров современного кибертерроризма выступают события в Эстонии с 27 апреля по 18 мая 2007 г. В этот период сайты газет, основных банков и правительственных учреждений подвергались массированным бомбардировкам спамом или стали жертвами взломщиков. К телевизионному терроризму следует отнести освещение по соответствующим каналам выступлений террориста № 1 — Бен-Ладена. Телефонный терроризм — явление очень распространенное во всех странах мира. Терроризируют не только отдельных лиц, но крупные государственные и коммерческие структуры взрывами, физической расправой и другими угрозами. Музыкальный терроризм предусматривает достижение террористическими организациями целей через деструктивные музыкальные произведения.

Информационный терроризм при внешнем сходстве по форме и методам с информационным криминалом отличается от него целями и тактикой проведения. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия и получил широкий общественный резонанс. Как правило, требования террористов сопровождаются угрозой повторения террористического акта, обычно без указания конкретного объекта и места действия. Заметим, что способы и средства реализации мероприятий ИК и ИТР, как и ведения современной информационной войны, в настоящее время в мире, к сожалению, получили большое развитие [1]. Последствия ИВ, ИК и ИТР могут сказываться как на разрушении моральных устоев, поведении и конфликтности различных слоев населения, групп, отдельных лиц, так и на работе общественного транспорта, систем жизнеобеспечения, промышленных и социальных учреждений, телекоммуникационных и других сетей. Кроме этого скрытые деструктивные информационные воздействия на сознание широких

[1] *Расторгуев С. П.* Информационная война. М.: Радио и связь, 1999. 415 с.; *Прокофьев В. Ф.* Тайное оружие информационной войны: атака на подсознание. 2-е изд. М.: Сентег, 2003. 408 с.; *Астахов М. А., Ростовцев Ю. Г., Яфраков М. Ф.* Информационная борьба. М.: Изд-во ТОМ, 2007. 334 с.; *Бухарин С. Н., Цыганов В. В.* Методы и технологии информационных войн. М.: Академ. проект, 2007. 382 с.; *Лисичкин В. А., Шелепин Л. А.* Третья мировая (информационно-психологическая) война. Серия: История XXI века 2-е изд.: М.: Эксмо, 2003. 304 с.; *Цыганков В. Д.* Психотроника и безопасность России. М.: Синтег, 2003. 136 с.; *Смолян Г. Л., Зараковский Г. М. и др.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997. 52 с.; *Цыганов В. В., Бухарин С.* Н. Информационные войны в бизнесе и политике. Теория и методология. М.: Академический проект, 2007. 336 с.; *Осипов В. Ю., Ильин А. П. и др.* Радиоэлектронная борьба. Теоретические основы. Петродворец: ВМИРЭ им. А. С. Попова, 2006. 302 с.

слоев населения являются не только подпиткой уже сформированных асимметричных групп населения или отдельных граждан, но и порождением новых деструктивных структур. Все эти негативные предпосылки и проявления информационных асимметричных слабо контролируемых угроз уже не только существенно сказываются на состоянии всего человечества, но и чреваты для будущих поколений.

Состояние развития практики и теории противодействия. Анализ современных работ [2] по ИВ, ИК, ИТР свидетельствует о том, что исследования этих социальных явлений и мер противодействия им далеки от глубокой проработки. Имеются определенные результаты в области обеспечения информационной безопасности, прежде всего технических, в меньшей мере биологических систем. В целом, что касается населения, как объекта защиты от деструктивных информационных воздействий по различным каналам, здесь больше проблем, чем ответов.

В Российской Федерации в общем виде определены основные методы обеспечения информационной безопасности [3]. Отражены особенности ее в различных сферах общественной жизни (экономике, внутренней и внешней политике, области науки и техники, духовной жизни, общегосударственных информационных и телекоммуникационных системах, обороне). Однако реальное воплощение положений утвержденной доктрины информационной безопасности на практике связано с большими

---

[2] *Котенко И. В., Юсупов Р. М.* Информационные технологии для борьбы с терроризмом // Защита информации. ИНСАЙД. 2009. № 2(26). С. 74–79; *Вишняков Я. Д., Бондаренко Г. А. и др.* Основы противодействия терроризму / Под ред. Я. Д. Вишнякова. М.: Академия, 2006. 240 с.; *Афонин С. А. и др.* Современный терроризм и борьба с ним: социально-гуманитарные измерения / Под ред. В. В. Ященко. М.: МЦНМО, 2007. 216 с.; *Андреев О. О. и др.* Критически важные объекты и кибертерроризм. Часть 1, 2 / Под ред. В. А. Васенина. М.: МЦНМО, 2008. 398 с. (ч. 1). 607 с. (ч. 2); *Фролов Д. Б.* Информационная геополитика и вопросы информационной безопасности // Национальная безопасность. 2009. № 1. С. 72–79; *Пирумов В. С.* Стратегия выживания социума. Системный подход в исследовании проблем геополитики и безопасности. М.: Дружба народов, 2003. 544 с.; Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 05.12.2016 г. № 643. URL: http.://www.kremlin.ru/acts/bank/41460; *Астахов М. А., Ростовцев Ю. Г., Яфраков М. Ф.* Информационная борьба и знаковые системы. М.: Изд-во ТОМ, 2007. 334 с.; *Юсупов Р.* М. Наука и национальная безопасность. Монография. 2-е изд., перераб. и доп. СПб.: Наука, 2011. 369 с.

[3] Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 05.12.2016 г. № 643. URL: http.://www. kremlin.ru/acts/bank/41460.

трудностями и даже негативными аспектами. В частности, из-за обеспечения технологической независимости и возможных информационных угроз введены существенные ограничения на использование импортного программного обеспечения и элементной базы при разработке ряда отечественной радиоэлектронной техники. С одновременным повышением информационной безопасности эти ограничения не только замедлили темпы развития этой техники, но и существенно увеличили затраты на ее создание. Практика защиты информации на основе дорогих услуг не стимулирует прогресс. В то же время аспекты противодействия ИВ, ИК, ИТР, связанные с оперативной проверкой информации на предмет информационно-психологической безопасности, остаются без должного внимания. В определенной мере это обусловлено невысоким уровнем развития научной базы противодействия ИВ, ИК, ИТР не только в России, но и за рубежом. Известны научно-методические подходы к такому противодействию [1]. В основном это методы на основе мнений экспертов и упрощенных математических моделей. Выход на многофакторные количественные оценки, предусматривающие наличие более адекватных математических моделей, осуществляется редко, за исключением вопросов кибербезопасности, радиоэлектронной и криптозащиты. Традиционные методы цензурного характера в настоящее время существенно устарели из-за их инерционности и субъективности. В основном проблемами информационно-психологической безопасности по отношению к человеку, обществу занимались и продолжают заниматься специалисты в области социальных и общественных наук. Их техническая и методическая оснащенность несомненно возросла за последние годы. Разработаны специальные методики и стенды для анализа профессиональной психологической пригодности граждан и, в частности, для оценки влияния на них различного рода информационных воздействий. Однако методы и средства, позволяющие оперативно выявлять скрытую деструктивную информацию без непосредственного ее воздействия на людей, в настоящее время практически отсутствуют. Можно утверждать, что имеет место существенный разрыв между уровнем развития теории противодействия

[1] *Смолян Г. Л., Зараковский Г. М. и др.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997. 52 с.; *Афонин С. А. и др.* Современный терроризм и борьба с ним: социально-гуманитарные измерения / Под ред. В. В. Ященко. М.: МЦНМО, 2007. 216 с.; *Пирумов В. С.* Стратегия выживания социума. Системный подход в исследовании проблем геополитики и безопасности. М.: Дружба народов, 2003. 544 с.; *Юсупов Р. М.* Наука и национальная безопасность. 2-е изд., перераб. и доп. СПб.: Наука, 2011. 376 с.

ИВ, ИК, ИТР и потребностями практики. Способы и средства деструктивного информационного воздействия на население существенно обогнали в своем развитии теорию и практику противодействия этим угрозам.

Общая характеристика проблем противодействия. С учетом вышесказанного необходима, по нашему мнению, разработка теории процессов противодействия отмеченным угрозам, новых математических моделей и методов, позволяющих:

- эффективно прогнозировать деструктивные действия групп и лиц в условиях разнородной, неполной и зачастую недостоверной информации о них;
- оперативно выявлять и пресекать опасные информационные воздействия на население, передаваемые (переносимые) посредством различных носителей и средств, в том числе через средства массовой информации.

В перспективе это позволит разработать эффективные системы и средства оперативной проверки разнородной, прежде всего семантической информации по требованиям безопасности, тем самым снизить возможные риски от информационного вандализма, криминала и терроризма, а также вырабатывать рекомендации по разрешению многих широкомасштабных конфликтов в обществе. В интересах устранения имеющихся противоречий между уровнем развития науки и потребностями практики противодействия ИВ, ИК, ИТР предлагается решить ряд частных проблем:

1. Сформировать концептуальные модели ИВ, ИК, ИТР как современных угроз человечеству. Необходимо уточнить понятия и категории, характерные ИВ, ИК, ИТР, глубже проанализировать цели, задачи, возможности и условия проявления этих явлений в Российской Федерации и в мире. Следует систематизировать возможные методы, средства и объекты, а также вскрыть причинно-следственные связи, порождающие ИВ, ИК, ИТР. В определенной мере при решении этой частной проблемы можно опереться на известные результаты анализа террористических угроз[2]

---

[2] Report on Terrorism. USA. National Counterterrorism Center. 2008. 30 April. 96 p.; *Иванов М. Н., Васильченко А. В., Юсупов Р. М.* Склонность к терроризму: психофизиологический, этнический анализ (стратегии управления и мониторинга групп риска в этническом регионе) // Взаимопонимание культур, проблемы национальных идентичности (к 125-летию М. Гафури): Сборник научных статей. Уфа, 2009. С. 148–153; *Ильясов Ф. Н.* Терроризм — от социальных оснований до поведения жертв // Социологические исследования. 2007. № 6. С. 78–85; *Жаринов К. В.* Терроризм и террористы: Исторический справочник / Под общ. ред. А. Е. Тараса. Минск, 1999. 606 с.

с учетом человеческого фактора [1], методы традиционной радиоэлектронной борьбы [2] и ведения информационной войны [3].

2. Разработать теоретические основы противодействия ИВ, ИК, ИТР. Желательно определить цели, задачи, методы и потенциальные средства такого противодействия. Нужна разработка соответствующей системы показателей и критериев оценки эффективности. Требуется математически сформулировать основные задачи противодействия, разработать методы их решения. В основу этих исследований могут быть положены теоретические положения радиоэлектронной борьбы [4], комплексного технического контроля [5], компьютерной безопасности [6].

3. Получить приемлемые для практики подходы к математическому моделированию поведения населения, социальных слоев, групп и конфессий, как объектов защиты от ИВ, ИК, ИТР. Необходимо разработать формализмы, отражающие основные свойства объектов защиты в условиях деструктивных информационных воздействий. Требуются математические модели, учитывающие структурную сложность, саморазвитие и перестройку этих объектов во времени, не только в зависимости от этих информационных воздействий, но и других факторов. В частности, для моделирования поведения объектов защиты можно использовать относительно-конечные операционные автоматы [7], которые являются моделями перестраиваемых, перепрограммируемых систем. Отличие их от традиционных автоматов в том, что все их параметры, в том числе

---

[1] *Osipov V., Ivakin Y.* Terrorists: Statistical Profile / Information Fusion and Geographic Information Systems. Proceedings of the Fourth International Workshop, 17–20 May 2009. Springer-Verlag Berlin Heidelberg, 2009. P. 241–250.

[2] *Осипов В. Ю., Ильин А. П. и др.* Радиоэлектронная борьба. Теоретические основы. — Петродворец: ВМИРЭ, 2006. 302 с.

[3] *Расторгуев С. П.* Информационная война. М.: Радио и связь, 1998. 415 с.; *Бухарин С. Н., Цыганов В. В.* Методы и технологии информационных войн. М.: Академический проект, 2007. 382 с.

[4] *Осипов В. Ю., Ильин А. П. и др.* Радиоэлектронная борьба. Теоретические основы. Петродворец: ВМИРЭ, 2006. 302 с.

[5] *Осипов В. Ю., Ильин А. П. и др.* Указ. соч.; Технические методы и средства защиты информации / Ю. Н. Максимов, В. Г. Сонников, В. Г. Петров и др. СПб.: Полигон, 2000. 320 с.

[6] *Андреев О. О. и др.* Критически важные объекты и кибертерроризм. Часть 1, 2 / Под ред. В. А. Васенина. — М.: МЦНМО, 2008. 398 с. (ч. 1), 607 с. (ч. 2).

[7] *Цыганов В. В., Бухарин С. Н.* Информационные войны в бизнесе и политике. Теория и методология. М.: Академический проект, 2007. 336 с.; *Осипов В. Ю.* Информационная безопасность: синтез управляющих программ. Петродворец: ВМИРЭ, 2001. 64 с.

множества функций переходов и выходов, конечны относительно предыдущего шага. Возможны и другие подходы.

4. Разработать модели формирования информационных вандалов, криминальных элементов, террористов и модели угроз населению через современные каналы информационного воздействия. Получение первых моделей предусматривает формализацию среды их порождения, мотиваций при принятии асимметричных решений. Создание вторых моделей включает формализацию типовых способов деструктивных воздействий на объекты защиты, исследование самовоспроизводящихся и невоспроизводящихся, психологически, биологически и социально опасных информационных воздействий на население, прежде всего, через средства массовой информации. Для моделирования этих процессов могут быть использованы методы искусственного интеллекта [8], теории вероятностей, автоматные подходы и другие. Для синтеза и анализа самовоспроизводящихся структур применимы предложенные ранее методы [9].

5. Развить теорию мониторинга информационных угроз населению со стороны ИВ, ИК, ИТР, методы оперативного их вскрытия и прогнозирования. Это развитие предполагает совершенствование методов наблюдения за потенциально опасными каналами деструктивных информационных воздействий и контроля безопасности имеемых информационных ресурсов. Нужны новые, более совершенные, методы распознавания статичных и динамичных информационных угроз, оценки достоверности информации, прогнозирования развития анализируемых процессов. При таком развитии следует принять во внимание результаты работ [10].

---

[8] *Поспелов Д. А.* Ситуационное управление: теория и практика. М.: Наука, 1986. 288 с.; Искусственный интеллект. В 3-х кн. Кн. 2 Модели и методы: Справочник / Под ред. Д. А. Поспелова. М.: Радио и связь, 1990. 304 с.; *Рассел С., Норвиг П.* Искусственный интеллект: современный подход, 2-е изд. / Пер. с англ. М.: Вильямс, 2006. 1408 с.; *Хайкин С.* Нейронные сети: полный курс, 2-е изд. / Пер. с англ. М.: Вильямс, 2006. 1104 с.

[9] *Осипов В. Ю.* Информационная безопасность: синтез управляющих программ. Петродворец: ВМИРЭ, 2001. 64 с.; *Осипов В. Ю., Ильин А. П. и др.* Радиоэлектронная борьба. Теоретические основы. Петродворец: ВМИРЭ, 2006. 302 с.

[10] *Осипов В. Ю., Ильин А. П. и др.* Радиоэлектронная борьба. Теоретические основы. Петродворец: ВМИРЭ, 2006. 302 с.; *Поспелов Д. А.* Ситуационное управление: теория и практика. М. Вильямс, 1986. 288 с.; *Городецкий В., Карсаев О., Самойлов В.* Многоагентная система оценки ситуаций на основе асинхронного потока распределенных гетерогенных данных // Труды Междунар. конф. «Искусственные интеллектуальные системы», Дивноморское, Россия, сентябрь 3–9, Физматгиз, 2004. С. 294–300; *Кулешов С. В.* Аналитический мониторинг Интернет ресурсов с целью выявления потенциально опасного содержания // Перспективные системы и задачи управления:

6. Разработать методы оперативного синтеза и реализации целесообразных мероприятий противодействия ИВ, ИК, ИТР. Желательно совершенствовать методы автоматического извлечения знаний из наблюдений за процессами ИВ, ИК, ИТР. Требуют дальнейшего развития методы автоматического синтеза структурно-сложных программ противодействия угрозам с учетом возможностей их реализации на практике в приемлемые сроки. В интересах этого рекомендуется опираться на известные методы интеллектуальной обработки данных [1], дедуктивного синтеза программ [2]. Для доказательства существования результативных программ при дедуктивном синтезе на знаниях можно использовать прямой логический вывод, а для извлечения этих программ из вывода — обратный вывод.

7. Разработать принципы построения средств мониторинга и автоматической проверки телевизионных и радиопередач, информации, получаемой через Интернет, социальные и другие сети, цифровых фильмов и музыки, компьютерных игр, газет, журналов, учебной, художественной и технической литературы по требованиям безопасности для населения. Необходимы поиск методов обоснования современных требований к характеристикам, составу и структуре этих средств, а также разработка универсальных технологий их построения с обеспечением защиты от программных деструктивных воздействий.

8. Совершенствовать теорию построения глобальных систем защиты населения от информационного вандализма и терроризма. Следует

Материалы четвертой научно-практической конференции. Таганрог, 2009. С. 255; *Александров В. В., Кулешов С. В.* Аналитический мониторинг INTERNET-контента. Инфологический подход // Системные проблемы надежности, качества, математического моделирования, информационных и электронных технологий в инновационных проектах (Инноватика — 2007): Материалы Междунар. конф. и Рос. научной школы. Часть 2, Т. 1. М., 2007. С. 80–83.

[1] *Городецкий В., Самойлов В., Малов А.* Технология обработки данных для извлечения знаний: Обзор состояния исследований // Новости искусственного интеллекта. 2002. № 3–4; *Jiawei Han, Micheline Kamber*. Data Mining: Concepts and Techniques, 2nd ed. The Morgan Kaufmann Series in Data Management Systems, Jim Gray, Series / Editor Morgan Kaufmann Publishers, March 2006; *Багдесян А. А., Куприянов М. С., Степаненко В. В.* Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP. 2-е изд. СПб.: БХВ-Петербург, 2007. 384 с.

[2] *Осипов В. Ю.* Информационная безопасность: синтез управляющих программ. Петродворец: ВМИРЭ, 2001. 64 с.; Искусственный интеллект. В 3-х кн. Кн. 2 Модели и методы: Справочник / Под ред. Д. А. Поспелова. М.: Радио и связь, 1990. 304 с.; *Осипов В. Ю.* Синтез результативных программ управления информационно-вычислительными ресурсами // Приборы и системы управления. 1998. № 12. С. 24–27.

совершенствовать нормативную основу такой защиты, разработать международные требования к информации глобального распространения по безопасности. Необходимо развить методы синтеза и анализа таких систем, управления информационной безопасностью на различных уровнях иерархии общества.

Практические пути решения проблем. Решение сформулированных проблем возможно только при объединении усилий ученых различных областей знаний, формировании специальной государственной целевой программы на проведение этих исследований и разработок. Все возможности у Российской Федерации для этого есть, необходима, прежде всего, интеграция и координация усилий ведущих институтов страны, в том числе институтов РАН, и, несомненно, финансовая поддержка этих работ. В результате могут быть получены инновационные результаты, позволяющие существенно снизить риски от ИВ, ИК, ИТР, повысить информационную безопасность Российской Федерации. На основе этих результатов, наряду с запретительными мерами, может быть широко реализован рекомендательный подход при предоставлении различного рода информации населению. Суть этого подхода в том, чтобы при предоставлении населению информации, прежде всего через средства массовой информации и Интернет, шло сопровождение ее рекомендациями по безопасности применения. Несомненно, вручную (старыми методами) выработка таких рекомендаций в современных условиях практически нереальна. Для этого нужны специальные методы и средства автоматической оперативной проверки информации по основным требованиям безопасности и генерации рекомендаций населению. Получив такие рекомендации человек сам должен принимать решение, использовать эту информацию или нет. При таком подходе не нарушаются конституционные права граждан на пользование информацией, не ограничивается свобода слова, в то же время существенно снижаются риски деструктивных информационных воздействий на население. Заметим, что оперативная проверка информации по требованиям безопасности позволит выявлять не только деструктивные, но и позитивные воздействия на людей, превратить информацию в эффективное «лекарство». Планируемые результаты также могут дать возможность: количественно обосновывать системные решения, принимаемые на различных уровнях государственного и военного управления, как по вопросам внутренней, так и внешней информационной безопасности; своевременно прогнозировать и предотвращать возможные информационные «катаклизмы» в обществе.

В целом они позволят:

• совершенствовать существующую систему информационной безопасности Российской Федерации;

• устранить имеющиеся перекосы, сосредоточить внимание на ключевых позициях, снизить необоснованные затраты на решение проблем информационной безопасности;

• стимулировать гармоничное, сбалансированное развитие экономики и самого общества за счет совершенствования управления современным информационным потоком.

Рекомендации по использованию информационных технологий при противодействии угрозам. Для противодействия ИВ, ИК и ИТР могут использоваться различные информационные технологии (ИТ). Основная цель использования ИТ в этом случае — повышение у соответствующих органов их способности эффективно вести профилактическую работу, обнаруживать подготовку деструктивных действий со стороны информационных вандалов, преступников и террористов, идентифицировать их, не допускать совершения этих действий, устранять последствия. В простейшем случае все эти информационные технологии противодействия ИВ, ИК и ИТР могут быть подразделены на технологии сбора данных, их анализа и принятия решений. Технологии сбора данных в основном представляются технологиями реализации различных аппаратных и программных средств обнаружения признаков и фактов проявления угроз, слияния информации от различных источников. К ключевым технологиям анализа данных и принятия решений относятся технологии взаимодействия лиц, принимающих решения, выбора и обоснования решений, анализа текстов, обработки естественного языка, распознавания и анализа образов, прогнозирующего моделирования возможных событий и т. д.

Указанные информационные технологии помогают аналитикам создавать модели образов деятельности информационных вандалов, преступников, террористов. Они позволяют вести поиск и использовать большое количество различных мультимедийных данных, многоязычной речи и текста, извлекать объекты и связи между ними из больших массивов данных. С использованием ИТ можно сотрудничать, делать заключения и совместно использовать информацию, выдвигать гипотезы и проверять возможные действия информационных злоумышленников вырабатывать стратегии и меры противодействия. К наиболее важным информационным технологиям, используемым для противодействия ИВ, ИК, ИТР, можно отнести технологии:

— выбора и обоснования решений;
— поддержки взаимодействия лиц, принимающих решения;
— имитационного и математического моделирования событий, в том числе для их прогнозирования;
— интеллектуального анализа данных;
— управления и обработки информации в базах данных;
— управления потоками работ;
— мониторинга событий и оповещения;
— интеллектуального поиска информации в различных средах;
— управления знаниями;
— дешифрования и стегоанализа;
— биометрии;
— распознавания и анализа образов (изображений, текстов, сигналов);
— обработки речи (естественного языка);
— сенсорных сетей;
— технологии радиочастотной идентификации;
— геоинформационные, «космические» информационные технологии и др.

Информационные технологии в той или иной мере могут применяться на различных этапах противодействия информационным и психологическим угрозам:

— мониторинг, сбор и накопление информации;
— прогнозирование ситуаций;
— профилактика угроз;
— выявление угроз (деструктивных действий, террористических актов);
— пресечение угроз;
— расследование;
— ликвидация последствий;
— информационно-психологическое обеспечение.

Привязка информационных технологий к этапам противодействия таким угрозам была обоснована, в свое время, Р. М. Юсуповым и В. П. Заболотским [1].

Итак, на основе анализа событий последних лет можно утверждать, что наблюдается рост и совершенствование видов информационно-психологических угроз для населения. Все чаще население сталкивается

[1] *Юсупов Р. М., Заболотский В. П.* Концептуальные и научно-методологические основы информатизации. — СПб.: Наука, 2009. 542 с.

с такими социальными явлениями, как информационные вандализм, криминал и терроризм. Несмотря на ряд проведенных исследований этих явлений, проблемы противодействия им далеки от глубокой проработки. Активное решение их позволит стимулировать дальнейшие исследования по противодействию ИВ, ИК и ИТР. Успешное решение сформулированных проблем возможно только при объединении усилий ученых различных областей знаний.

Глава 5. Защита от нежелательной и вредоносной информации в глобальных информационных сетях

В настоящее время глобальные информационные сети, наиболее ярким представителем которых является Интернет, содержат огромное количество информации, доступной пользователям по всему миру. При этом доступ к этой информации может получить любой человек. Это является несомненным преимуществом использования глобальных информационных сетей в нашей повседневной жизни. В то же время, несмотря на положительные стороны использования глобальных информационных сетей, необходимо заметить, что огромные потоки и массивы данных, доступные для просмотра и анализа каждому пользователю Интернета, могут содержать информацию, которая может быть нежелательной либо вредоносной для определенных групп лиц. К такому виду информации можно отнести, например, контент, содержащийся на веб-сайтах организаций, запрещенных на территории Российской Федерации, а также на веб-страницах, которые распространяют нелицензионную продукцию либо пропагандируют насилие и употребление наркотических веществ. Не менее важным является ограждение несовершеннолетних от информации, способной причинить вред их здоровью и развитию. Следовательно, в настоящее время в глобальных информационных сетях наряду с проблемой защиты информации остро встает и другая проблема — защита пользователей сетей от нежелательной и вредоносной информации. Актуальность этой проблемы не вызывает сомнения, и необходимость ее скорейшего разрешения существенно возрастает. Поэтому целью исследований, результаты которых представлены в настоящем разделе,

являлось рассмотрение сущности заявленной проблемы, возможных подходов к ее решению, обсуждение предлагаемого подхода и результатов его экспериментальной оценки.

Анализ проблемы защиты от информации. Прежде всего, следует отметить, что в России проблема защиты от нежелательной и вредоносной информации стала упоминаться на законодательном уровне. В частности, эта проблема находит отражение в «Доктрине информационной безопасности», в Федеральном законе «Об информации, информационных технологиях и о защите информации» [1], а также в Федеральном законе «О защите детей от информации, причиняющей вред их здоровью и развитию» [2]. Это говорит о том, что на государственном уровне данной проблеме уделяется достаточно большое внимание.

В соответствии с требованиями упомянутых выше законов, организацию защиты от нежелательной и вредоносной информации можно разделить на два основных направления:

1) ограждение несовершеннолетних от нежелательных материалов;

2) блокировка контента, нарушающего законодательство.

Однако реализация данных мероприятий осложняется, в первую очередь, следующими факторами:

1) большими объемами информации в сети Интернет;

2) высокой изменчивостью содержимого сайтов;

3) сложностью структуры этих сайтов.

Основным направлением решения поставленной проблемы, позволяющим получить высокое качество распознавания нежелательной и вредоносной информации, является «ручная» оценка веб-страниц экспертами. Однако стоит заметить, что зачастую даже экспертное заключение о принадлежности веб-страницы к той или иной категории может быть ошибочно. Кроме того, скорость работы любого эксперта намного ниже, чем рост количества новых веб-сайтов и изменение информации, представленной на них. Другим направлением решения данной проблемы является использование для анализа веб-страниц автоматизированных систем. В данном случае качество анализа веб-страниц по сравнению с их экспертной оценкой может быть ниже, однако очевидно, что

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru/document/cons_doc_LAW_61798.

[2] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию». URL: http://www.consultant.ru/document/cons_doc_LAW_108808.

автоматизированные системы позволяют значительно повысить оперативность и снизить трудоемкость анализа веб-сайтов [3].

Потребность в использовании автоматизированных систем для защиты от нежелательной и вредоносной информации в настоящее время четко осознается разработчиками программного обеспечения, что выражается в появлении программных средств с этим предназначением. Так, во многих социальных сетях (например, в сети «Вконтакте»), а также в глобальных информационных поисковых системах (Яндекс, Google) реализованы средства безопасного поиска информации. Схожим функционалом обладает отечественный браузер «Спутник», обеспечивающий детектирование нежелательной и опасной информации, а также фильтрацию контента. Кроме того, существуют модули родительского контроля, входящие в состав антивирусного программного обеспечения (ПО), и полноценные самостоятельные решения, обеспечивающие ограждение несовершеннолетних от неприемлемой информации. Более частной задачей, которая, тем не менее, также связана с нежелательной информацией, является определение рекламного контента, рассылаемого пользователям на электронную почту (борьба со спамом).

Специфика программных систем защиты от информации, ориентированных на обеспечение высокого уровня информационной безопасности пользователей, заключается в том, что типовой пользователь не способен самостоятельно дать адекватную оценку степени опасности поступающей к нему информации [4]. Тем самым роль пользователей в таких системах существенно снижается. По этой причине на первое место выходят автоматизированные системы оценки контента, управляемые небольшим количеством экспертов в области информационной безопасности и основанные на использовании релевантных источников первичной информации об анализируемых объектах.

Рассматривая аспекты функционирования автоматизированных систем оценки контента, можно обосновать предъявляемые к ним функциональные требования. Прежде всего, следует отметить, что вычисление показателей, характеризующих информацию, хранящуюся на веб-сайтах, должно проводиться не только в контексте данных, полученных

---

[3] *Котенко И. В., Чечулин А. А., Комашинский Д. В.* Автоматизированное категорирование веб-сайтов для блокировки веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 69–79.

[4] *Комашинский Д. В. и др.* Автоматизированная система категорирования веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2013. № 3(9). С. 119–127.

от пользователя (от пользовательской рабочей станции), но и с учетом остальной доступной информации (опыт других пользователей; белые/черные/серые списки; текстовое и графическое содержимое; структурные признаки; связи между объектами; внешние данные, предоставляемые сообществами пользователей, экспертов и других компаний, специализирующихся в области информационной безопасности) [1].

Далее, анализ информации, содержащейся на веб-сайте, должен осуществляться централизованными средствами технологической инфраструктуры, размещенной «в облаке».

Процесс анализа веб-сайта должен начинаться по факту регистрации событий, инициированных пользователем, последствия которых могут повлечь риски его информационной безопасности.

Наконец, скорость принятия решения об информации, предоставляемой веб-сайтом, должна быть сопоставима, по крайней мере, со скоростью типового антивирусного приложения, находящегося на рабочей станции пользователя.

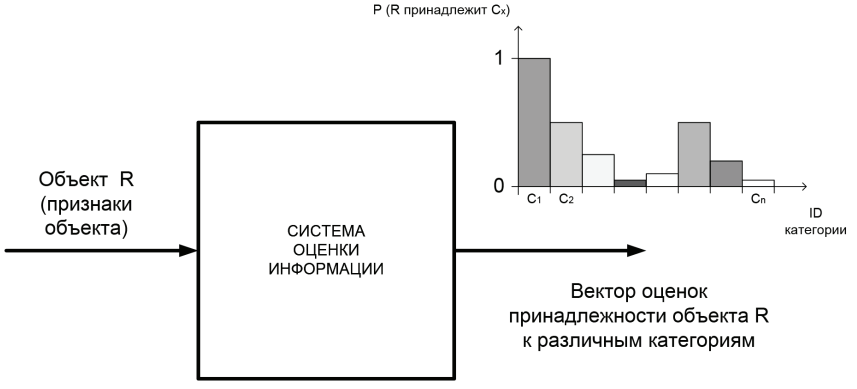


Рис. 17. Вход и выход системы оценки информации

Показатели, характеризующие информацию, хранящуюся на веб-сайтах, рассматриваются в виде набора величин (оценок), определяющих

[1] *Комашинский Д. В., Котенко И. В., Чечулин А. А.* Категорирование веб-сайтов для блокирования веб страниц с неприемлемым содержимым // Системы высокой доступности. 2011. № 2. С. 102–106.

в числовом виде степень принадлежности P веб-сайта (объекта R) к набору контролируемых категорий $\{C_1, C_2, \ldots, C_n\}$ (рис. 17). Степень принадлежности P изменяется в диапазоне от 0 до 1. Таким образом, на вход системы оценки информации поступает объект R, а на выход выдается вектор значений $\{P_1, P_2, \ldots, P_n\}$, где P_i — степень принадлежности R к категории C_i, $i = 1, \ldots, n$.

Для оценки эффективности функционирования системы оценки информации (классификатора) необходимо ввести в рассмотрение соответствующие количественные показатели. В наибольшей степени для этой цели подходят показатели, используемые для оценки эффективности информационно-поисковых систем. Разобьем все множество элементов выборки (множество анализируемых веб-сайтов) на четыре возможные группы в зависимости от релевантности веб-сайта и правильности его выбора. Дадим условные обозначения количеству элементов в каждой группе, как показано в табл. 7.

Таблица 7

Количество элементов в возможных группах выборки

Обозначение	Определение
TP	Количество верно распознанных элементов выборки
TN	Количество правильно отвергнутых элементов выборки
FP	Количество элементов, не принадлежащих к категории, но неверно отнесенных к ней («ложное срабатывание» или ошибка I рода)
FN	Количество элементов, принадлежавших категории, но ошибочно отвергнутых («пропуск события» или ошибка II рода)

На основе представленных в табл. 7 обозначений можно ввести в рассмотрение систему показателей эффективности для систем оценки информации, представленную в таблице 8.

Показатель «точность» (p) определяет долю документов, действительно принадлежащих данному классу, относительно всех документов, которые система отнесла к нему.

Показатель «полнота» (r) показывает долю найденных классификатором документов, принадлежащих к заданному классу, относительно всех документов этого класса в выборке.

F-мера является показателем, объединяющим в себе информацию о точности и полноте. Она представляет собой сбалансированное взвешенное гармоническое среднее между этими двумя показателями.

Аккуратность (a) есть отношение количества документов, по которым классификатор принял правильное решение, к размеру всей выборки.

Таблица 8

Показатели эффективности систем оценки информации

Наименование	Обозначение	Выражение для расчета
Точность (precision)	p	$p = \frac{TP}{TP + FP}$
Полнота (recall)	r	$p = \frac{TP}{TP + FN}$
F-мера	F	$F = \frac{2 \cdot p \cdot r}{p + r}$
Аккуратность (accuracy)	a	$a = \frac{TP + TN}{TP + TN + FP + FN}$

Необходимо отметить, что в зависимости от конкретной решаемой задачи введенные показатели обладают разной важностью для решения различных задач. Например, для модуля анализа веб-страниц, входящего в состав антивирусного ПО, первостепенное значение будет иметь высокая точность, так как большое количество ложных срабатываний не допускается.

В случае систем родительского контроля более важным будет показатель «полнота», так как необходимо оградить детей от неприемлемого содержимого, к которому будут относиться, в том числе, и сайты, вызывающие сомнения, но не отнесенные к определенной категории.

Подходы к построению автоматизированной системы защиты от информации. Для разработки подхода к построению автоматизированной системы защиты от информации рассмотрим вначале существующие решения, применяемые к анализу веб-сайтов и реализованные в известных автоматизированных системах. Существуют решения, которые основываются на проверке вхождения заранее определенных ключевых слов и их

сочетаний, а также других правилах, задаваемых, например, с помощью регулярных выражений. На их основании принимается решение: разрешать или блокировать веб-сайт. Недостатком такого метода является его низкая точность, так как слова могут быть заменены на синонимы, что приведет к пропуску нежелательной информации, а наличие запрещенных слов, используемых в «легальном» контексте, может привести к запрету доступа к веб-сайтам, не содержащим нежелательной информации.

Другой подход связан с использованием режима безопасного поиска на поисковых сайтах Яндекс или Google. Их основной недостаток заключается в ограниченной применимости. Пользователь может зайти на менее популярную поисковую систему, в которой данный режим не предусмотрен, или попасть на нежелательную веб-страницу по внешней ссылке. Многие системы используют ведение и анализ «белого» или «черного» списков. В первом случае запрещается подключение ко всем сайтам, кроме заранее определенного «белого» списка. Во втором случае блокировка сайта осуществляется только тогда, когда он присутствует в «черном» списке. Однако оба эти подхода имеют существенный недостаток, обусловленный высокой изменчивостью веб-сайтов. После формирования списков тематика сайтов может измениться, что приведет к получению нежелательной или блокировке необходимой информации. Трудность выявления нежелательной информации среди значительных объемов разнородных, зачастую противоречивых и изменчивых данных обусловлена, в т. ч., особенностями построения веб-сайтов. Обычно они имеют сложную иерархическую структуру и состоят из множества элементов: форматированного текстового и графического содержимого, программного кода, ссылок на другие документы и т. д. Поэтому нежелательная информация не всегда определяется на основе одних только текстовых признаков. Зачастую в определении направленности сайта помогает информация об указателе (адресе) размещения сайта в Интернете (URL) или структурных особенностях.

Общий недостаток систем, использующих заранее определенные слова, правила или списки, состоит в отсутствии возможности самообучения. Поэтому в некоторых системах предлагается использовать подходы, основанные на методах машинного обучения. Основная задача этих методов формулируется следующим образом: требуется отнести исследуемый объект к одному из множества заранее известных классов. Применительно к защите от нежелательной информации примером применения методов машинного обучения может послужить функционирование системы родительского контроля, распределяющей

веб-страницы по категориям и блокирующую те из них, которые оказались нежелательными («сайты для взрослых», «алкоголь», «оружие», «наркотики» и т. д.). При рассмотрении предлагаемого подхода к построению автоматизированной системы защиты от информации остановимся на двух его аспектах: общей архитектуре предлагаемого классификатора и механизме извлечения данных для анализа веб-страниц. Как было указано выше, веб-страницы отличаются от обычных текстовых документов более высокой сложностью и, прежде всего, тем, что они частично структурированы (semi-structured) с помощью HTML-тэгов разметки, связаны между собой ссылками, содержат фрагменты кода, исполняемого как на стороне сервера, так и у клиента. Поэтому в процессе классификации предлагается учитывать указанные аспекты веб-страниц. Классификатор является важнейшей частью автоматизированной системы защиты от информации. На его основе функционирует аналитический модуль системы. Особенность предлагаемой архитектуры классификатора заключается в том, что она, по сути, представляет собой иерархию классификаторов (рис. 18).

В рамках каждого из аспектов веб-страницы (текстового содержимого, структурных особенностей, URL сайта и других) существуют классификаторы 1-го уровня. Их количество совпадает с числом категорий классификации. Каждый из них принимает решение о принадлежности поступающих на вход данных к своей категории. Результаты классификаторов 1-го уровня служат входными данными для классификатора 2-го уровня — мета-алгоритма (например, Stacking), который принимает решение на основе информации от классификаторов 1-го уровня. Результаты классификаторов 2-го уровня по каждому из аспектов анализируются классификатором 3-го уровня, выдающим окончательное решение о принадлежности веб-страницы к тому или иному классу. Данный подход является модульным и, как следствие, позволяет легко добавлять новые аспекты и категории. Более того, каждый из алгоритмов классификации является «черным ящиком» с входами и выходами, что позволяет легко заменять одни алгоритмы другими на каждом из уровней.

Еще одним из преимуществ данной архитектуры является локализация изменений, так как переобучение может происходить только для отдельных классификаторов. Кроме того, достоинством данного подхода является возможность «дообучения» классификаторов. С течением времени информация устаревает: например, с появлением новых видов веществ в категории «наркотики» классификатор, обученный на старых данных, будет работать хуже. Однако, используя предложенную

архитектуру, можно актуализировать отдельные классификаторы, обучив их на обновленной информации. При этом остальные компоненты системы не будут затронуты.

Предлагаемый механизм извлечения данных для анализа веб-страниц основывается на анализе следующих признаков:

1) текстового содержимого [1];
2) адреса размещения сайта в Интернете (URL);
3) структурных признаков (HTML-тэгов) [2];
4) истории сайта (возраст сайта, страна, в которой зарегистрирован сайт, организация, предоставляющая хостинг сайту, история серверов, на которых размещался сайт);
5) внешних источников информации («черные» или «белые» списки, ответы от поисковых систем).

Все перечисленные выше признаки в той или иной мере использовались в ряде известных методов классификации.

Классификация по текстовому содержимому является наиболее широко применяемым методом, состоящим из двух этапов. На первом этапе производится подготовка данных с переводом их в форму, воспринимаемую классификатором. На этом этапе осуществляется удаление тегов разметки, извлечение текстового содержимого веб-страниц, выполнение операции стемминга (т. е. сохранение основы слов и отбрасывание их окончаний), исключение знаков препинания, а также стоп-слов в виде предлогов, союзов, местоимений и т. д. Второй этап состоит в подаче предварительно обработанных данных на тот или иной стандартный текстовый классификатор (Naïve Bayess, SVM и т. д.).

Большинство известных методов текстовой классификации основываются на разделении выборки на две части: тестовую и обучающую

---

[1] *Kotenko I., Chechulin A., Komashinsky D.* Evaluation of Text Classification Techniques for Inappropriate Web Content Blocking // Proc. of the IEEE8th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2015), Warsaw, Poland, Sept. 24–26, 2015. 2015. P. 412–417.

[2] *Novozhilov D., Kotenko I., Chechulin A.* Improving the Categorization of Web Sites by Analysis of Html-Tags Statistics to Block Inappropriate Content // Proc. of the 9th Intern. Symp. on Intelligent Distributed Computing (IDC-2015), Guimaraes, Portugal, October 7–9, 2015. 2016. P. 257–263; *Новожилов Д. А., Чечулин А. А., Котенко И. В.* Улучшение категорирования веб-сайтов для блокировки неприемлемого содержимого на основе анализа статистики html-тэгов // Информационно-управляющие системы. № 6. 2016. С. 65–73.

Рис. 18. Иерархическая архитектура классификатора

(supervised method). Примером является метод SVM [1]. Более перспективным является метод без предварительного обучения (unsupervised method) [2], предназначенный для классификации по тексту с небольшими затратами ресурсов, а также для создания обучающих выборок. В нем документ делится на предложения, а затем каждому предложению сопоставляется категория на основе предварительно подготовленных списков ключевых слов и метрики подобия предложений.

Для определения спама успешно применяется метод категоризации, основанный на анализе общего числа слов на странице, средней длины слова, принадлежности слов веб-страницы к набору из наиболее часто встречаемых слов, а также статистики *n*-грамм (комбинаций из *n* символов) [3].

Альтернативным в текстовой классификации является метод, в котором переходят от рассмотрения документов в виде наборов слов к анализу их значений, которые берутся из лексических баз данных. Однако проведенные эксперименты показали, что хотя рассмотрение смысла слов несколько повышает величину аккуратности, оно не ведет к значительному улучшению точности и полноты классификации [4].

Текстовая классификация не может считаться достаточной. Она не учитывает структурных особенности веб-страниц. HTML-документ, как правило, связан ссылками с другими документами и может содержать изображения, а также другие нетекстовые элементы. Кроме того, известные трудности вызывают категории, обладающие сходным текстовым наполнением, но различающиеся по своей структуре (например, «блоги», «форумы», «чаты»).

Поэтому получил развитие метод, основанный на анализе URL. При этом исходят из предположения, что страницу в Интернете будут редко посещать, если ее адрес не отражает каким-то образом его тематику [5]. Один

---

[1] *Joachims T.* Text Categorization with Support Vector Machines: Learning with Many Relevant Features // Proc. of 10th European Conf. on Machine Learning (ECML-98), Chemnitz, Germany, April 21–23, 1998. P. 137–142.

[2] *Ko Y., Seo J.* Automatic Text Categorization by Unsupervised Learning // Proc.of the 18th Conf. on Computational linguistics (Coling-2000). 2000. P. 453–459.

[3] *Ntoulas A., et al.* Detecting Spam Web Pages through Content Analysis/ A. Ntoulas, M. Najork, M. Manasse, D. Fetterly // Proc. of the 15th Intern. World Wide Web Conf. (WWW-2006). 2006. P. 83–92.

[4] *Kehagias A., et al.* A Comparison of Word- and Sense-based Text Categorization Using Several Classification Algorithms/ A. Kehagias, V. Petridis, V. G. Kaburlasos, P. Fragkou // Journal of Intelligent Information Systems. 2000. Vol. 21(3). P. 227–247.

[5] *Attardi G., Gulli A., Sebastiani F.* Automatic Web Page Categorization by Link and

из способов такого анализа заключается в разбиении URL на составные части, подлежащие затем анализу. Такой подход успешно применяется для защиты от фишинговых сайтов [1]. При этом каждый фрагмент URL представляется в виде двумерного вектора, содержащего сам фрагмент и его позицию, которые затем подаются на вход обученному классификатору.

Другой способ состоит в использовании длины имени хоста и всего URL, подсчете количества в нем различных символов (например, точек) и анализе заключенных между этими символами фрагментов URL. При этом используются признаки на основе информации о хосте (географические особенности, дата регистрации, величина предельного периода времени, за который пакет может существовать до своего исчезновения (TTL) и т. д.). Все эти атрибуты подаются на вход стандартному классификатору (Naïve Bayess, SVM, Logistic Regression) [2].

Одним из вариантов дальнейшего разделения URL на фрагменты может быть использование энтропии. Такой подход позволяет разбивать на составные части названия доменов, в которых несколько слов слиты воедино. То из пробных разбиений, которое имеет наименьшую энтропию среди остальных, станет наиболее вероятным новым фрагментом [3]. Дополнительно можно использовать анализ последовательности *n*-грамм, для которых считается частота встречаемости [4]. Данный метод способен показывать хорошие результаты категоризации при решении частных задач («спам»/«обычное письмо», «phishing»/«benign»), однако в общем случае, при произвольном количестве и составе категорий, качество классификации снижается. Главная причина заключается в том, что в действительности не всегда адрес страницы в Интернете совпадает с ее содержанием.

Таким образом, для выявления категорий, основанных на структурных признаках, необходимо искать другие методы, одним из которых

Context Analysis // Proc. of 1st European Symp. on Telematics, Hypermedia and Artificial Intelligence (THAI-1999). 1999. P. 105–119.

[1] *Khonji M., Iraqi Y., Jones A*. Enhancing Phishing E-Mail Classifiers: A Lexical URL Analysis Approach // Intern. Journal for Information Security Research. 2012. Iss. 6. P. 236–245.

[2] *Ma J., et al.* Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs/ J. Ma, L. K. Saul, S. Savage, G. M. Voelker // Proc. of Conf. on Knowledge Discovery and Data Mining. 2009. P. 1245–1254.

[3] *Kan M.-Y., Thi H. O.N.* Fast Webpage Classification Using URL Features // Proc. of Conf. on Information and Knowledge Management. 2005. P. 325–326.

[4] *Geide M.* N-gram Character Sequence Analysis of Benign vs. Malicious Domains/ URLs. http://analysis-manifold.com/ngram_whitepaper.pdf.

может быть использование информации об HTML-тэгах сайта. Здесь также существуют различные подходы к анализу. Важным источником может служить информация, заключенная в таких тэгах, как <title> или <meta>, которая, наряду с текстовым содержимым веб-страниц, извлекалась специальным парсером [5]. С другой стороны, существуют методы, основанные на подсчете количества тэгов на странице [6]. Таким образом, построение автоматизированной системы защиты от информации необходимо осуществлять на основе следующих принципов:

1) выделение из всех доступных данных такой информации, которая является наиболее значимой для анализа информационного содержимого веб-сайта;
2) поиск наиболее значимых внешних источников информации, позволяющих производить анализ;
3) объединение разнородной информации от множества источников в общее представление о веб-сайте;
4) минимизация нагрузки на хосты конечных пользователей при сборе информации;
5) противодействие намеренным и случайным искажениям (шумам) в информации, получаемой от внешних источников;
6) поиск эффективных методик определения категории веб-страниц с требуемыми значениями производительности, вычислительной сложности и точности принятия решения.

Возможная реализация автоматизированной системы защиты от информации на back-end сервере (серверах) может базироваться на комбинации следующих двух подходов:

1) использование роботов-пауков, оценивающих сайты по мере возможности,
2) применение модуля, оценивающего каждую запрашиваемую страницу по запросам от пользователя.

---

[5] *Patil A. S., Pawar B. V*. Automated Classification of Web Sites using Naive Bayesian Algorithm // Proc. of the Intern. Multiconf. of Engineers and Computer Scientists. 2012. P. 466; *Riboni D.* Feature Selection for Web Page Classification // Proc. of the Workshop on Web Content Mapping: A Challenge to ICT (EURASIA-ICT). 2002. P. 121–128.

[6] *Kotenko I., et al.* Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking / I. Kotenko, A. Chechulin, A. Shorov, D. Komashinsky // Proc. of 14th Industrial Conf. on Data Mining (ICDM 2014). 2014. P. 39–54; *Meshkizadeh S., Masoud-Rahmani A*. Webpage Classification Based on Compound of Using HTML Features & URL Features and Features of Sibling Pages // Intern. Journal of Advanced Computer Technology. 2010. Iss. 2(4). P. 36–46.

На клиентской части (front-end) системы предполагается использовать запасной модуль анализа. Этот модуль необходим в случае разрыва связи с сервером, в обычное время он отключен. Кроме того, для большей надежности и гибкости системы возможно ведение простого поиска по ключевым словам. Достоинства данного подхода заключаются в его высокой производительности (не требуется дополнительных расходов, кроме возможных расходов на оборудование), в защите от сайтов, не скрывающих свою принадлежность к какой-либо категории, а также в возможности оценки всех запрашиваемых сайтов. К недостаткам можно отнести: возможность обмана системы (создание сайта таким образом, чтобы автоматическая система давала некорректную оценку); ложные срабатывания; потребность использования мощного вычислительного оборудования при большом количестве запросов к сайтам; устаревание оценки (в случае использования только робота-паука).

Реализация и экспериментальная оценка системы защиты от информации. На основе анализа возможных способов построения автоматизированной системы защиты от информации было решено представить ее программную инфраструктуру в виде набора программных модулей с четко определенными входами и выходами, последовательная работа которых будет обеспечивать весь процесс классификации веб-сайтов.

Отличительными чертами этой инфраструктуры являются [1]:

1) встроенный аналитический модуль, сочетающий различные алгоритмы и методы машинного обучения, который будет не только следовать предустановленным правилам, но и самообучаться;
2) использование различных аспектов веб-страниц (текстовое содержимое, структурные признаки, URL-адрес);
3) модульность структуры.

В реализованном программном прототипе этой инфраструктуры на первоначальном этапе производится загрузка из Интернета категорированных списков веб-сайтов. Использовались следующие источники данных: URLBlacklist [2], Shalla's Blacklist [3] и DMOZ [4]. Каждый из источни-

---

[1] *Новожилов Д. А., Чечулин А. А.* Разработка стенда для проведения экспериментов с методами классификации веб-сайтов // Часть 9-й Российской мультиконференции по проблемам управления (РМКПУ-2016) — конференция «Информационные технологии в управлении» (ИТУ-2016). 4–6 октября 2016 г. Материалы конференции. — СПб., 2016. С. 740–749.

[2] URLBlacklist URL: http://urlblacklist.com/.

[3] Shalla. URL: http://www.shallalist.de/.

[4] DMOZ. URL: https://www.dmoz.org/.

ков имеет свой формат представления данных. Например, URLBlacklist состоит из набора папок, имена которых соответствуют категориям классификации, а внутри каждой из них присутствует файл domains, содержащий URL конкретных веб-сайтов, относящихся к данной категории. Shalla's Blacklist обладает похожей структурой, однако допускает наличие вложенных подпапок. DMOZ же имеет иерархическую структуру и поставляется в виде двух XML-файлов, в одном из которых содержится перечень всех доступных категорий и подкатегорий, а во втором — URL принадлежащих к ним веб-сайтов. По окончании загрузки содержимое списков извлекается и помещается в базу данных. Затем по имеющимся URL веб-сайтов происходит загрузка их HTML-представления. После загрузки из сохраненного HTML-представления извлекаются различные признаки, используемые в процессе анализа. Источниками признаков являются следующие аспекты веб-страниц [5]:

1) текстовые (полный текст веб-страницы и текст, извлеченный из HTML-тэгов, например, содержимое тега <meta>);
2) структурные (статистика HTML-тэгов);
3) URL-страницы (для последующего анализа *n*-грамм).

Другими аспектами, которые возможно анализировать (их анализ является одним из направлений будущей деятельности), являются:

1) изображения;
2) информация от WHOIS-серверов, которые позволяют получить регистрационные данные о владельцах доменных имен и IP-адресов, а также другую информацию;
3) динамическое содержимое, генерируемое на странице с помощью языка JavaScript.

После того, как все данные собраны, выполняется их очистка. В частности, из полученного текста веб-страниц удаляются все символы, кроме пробелов и букв алфавита, которые затем преобразуются к нижнему регистру. За очисткой следует этап построения словаря и преобразования признаков в форматы, воспринимаемые специальным ПО для анализа данных. Из специального ПО используется средство RapidMiner [6]. В процессе своей работы оно осуществляет построение моделей и обучение классификаторов от первого до третьего уровней. Отчеты, полученные

[5] *Kotenko I., Chechulin A., Komashinsky D.* Categorization of web pages for protection against inappropriate content in the Internet // International Journal of Internet Protocol Technology (JIPT), 2016. http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijipt.

[6] Rapid Miner. URL: https://rapidminer.com/.

по результатам классификации веб-страниц, отображаются затем в формате Microsoft Excel [1]. На исходные данные, которые используются для обучения системы и проверки ее работы, накладывались следующие ограничения:

1) длина основного текста веб-страниц после процедуры очистки должна находиться в пределах от 500 до 5000 байт. Данное значение, установленное экспериментально, позволяет исключить из выборки сайты со слишком коротким содержимым (которое обычно не относится к категории, например, сообщение о необходимости включить JavaScript или обновить Flash Player), а также слишком большие по объему сайты (на которых будут встречаться слова из всех категорий, что снизит качество обучения);
2) в выборку включались только те веб-страницы, основной язык которых — английский. Подобное ограничение объясняется особенностями лексического анализатора (стеммера) Портера [2], который лучше всего работает со словами английского языка.

В соответствии с введенными ограничениями были выделены два набора данных. Первый из них включал следующие категории: «Сайты для взрослых» (adult), «Алкоголь» (alcohol), «Сайты о медицине» (medical) и «Сайты о религии» (religion). Во второй набор были добавлены «Онлайн-игры» (gamesonline), «Охота» (hunting) и «Музыка» (music). Все они могут использоваться в процессе защиты несовершеннолетних от нежелательной информации и борьбы с распространением нелицензионного контента.

Помимо перечисленных сайтов, в каждом из наборов также присутствовала дополнительно введенная категория, указывающая на неизвестный результат, получившая наименование «Unknown». Количество веб-страниц во всех наборах данных было взято одинаковым и равным 1200.

Результаты экспериментальной оценки предложенного подхода к проведению классификации веб-сайтов применительно к двум наборам данных представлены на рис. 19–23. На рис. 19 приведена оценка по показателю «аккуратность». Из рисунка видно, что для обоих наборов данных предложенный подход показывает достаточно высокую «аккуратность». При экспериментах по первому набору она составляет 92,7%, по второму — 86,1%. Для второго набора эта величина оказалась меньше,

[1] *Kotenko I., et al.* Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking / I. Kotenko, A. Chechulin, A. Shorov, D. Komashinsky // Proc. of 14th Industrial Conf. on Data Mining (ICDM 2014). 2014. P. 39–54.

[2] *Porter M. F.* An algorithm for suffix stripping // Program. Vol. 14. No. 3. 1980. P. 130–137.

поскольку в нем присутствует большее количество категорий (7 против 4), что затрудняет классификацию.

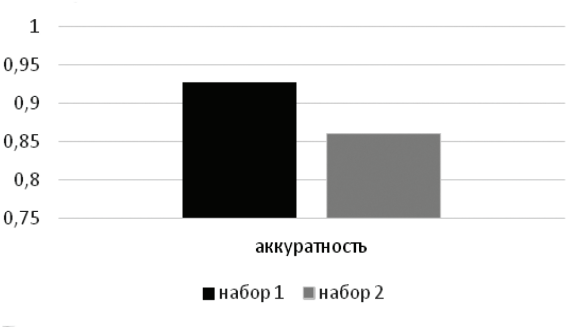


Рис. 19. Результаты экспериментальной оценки «аккуратности»

На рис. 20 и рис. 21 представлены экспериментальные оценки «аккуратности» по каждому набору данных в разрезе различных анализируемых классификационных признаков. Из рисунков видно, что наибольшего значения «аккуратность» классификаторов достигает при анализе основного текста (81,7% и 73,0% для первого и второго набора соответственно). На втором месте оказался классификатор, ориентированный на анализ содержимого ссылок (70,7% и 58,6%).

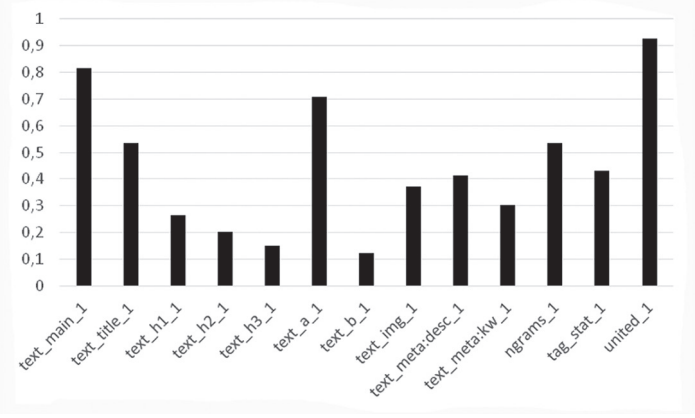


Рис. 20. Оценка «аккуратности» на наборе 1

Данные результаты показывают, что анализ специфики веб-документов обладает достаточно высокой эффективностью. Интернет-ресурсы обычно связаны с другими сайтами похожей тематики, поэтому учет подобной специфики является именно тем фактором, который отличает классификацию веб-страниц от классификации обычных текстовых документов. Другие признаки, обладающие высокими значениями аккуратности, — это текст из тэга <title> и *n*-граммы. Для первого набора: 53,6% и 53,6% соответственно, для второго: 53,6% и 47,2% соответственно.

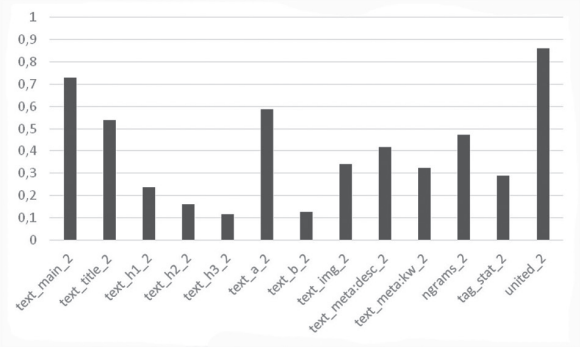


Рис. 21. Оценка «аккуратности» на наборе 2

На рис. 22 и рис. 23 представлены результаты экспериментальной оценки других показателей — точности, полноты и *F*-меры.

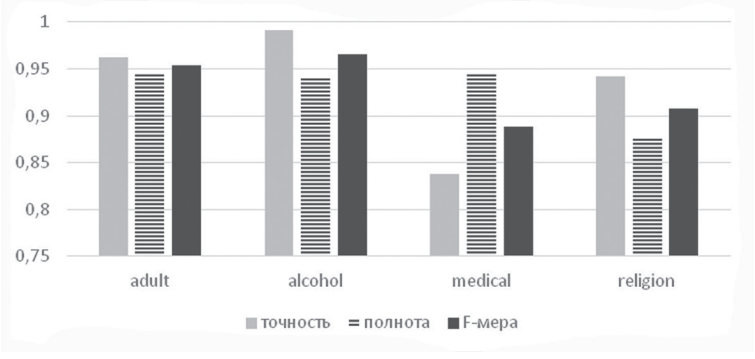


Рис. 22. Оценка точности, полноты и F-меры на наборе 1

Из рисунков видно, что предложенный подход в целом отличает высокая точность. Исключениями являются сайты категории «Медицина» для первого набора и категории «Онлайн-игры» — для второго. Значения полноты в большинстве своем достигают 85–95%. Исключения составляют категория «Религия» для набора 1 и категории «Медицина» и «Религия» для набора 2. Для категорий-исключений, показавших в предложенном подходе более плохое качество классификации, в будущем планируется добавить классификаторы на основе новых аспектов, что в целом повысит эффективность функционирования системы защиты от информации.

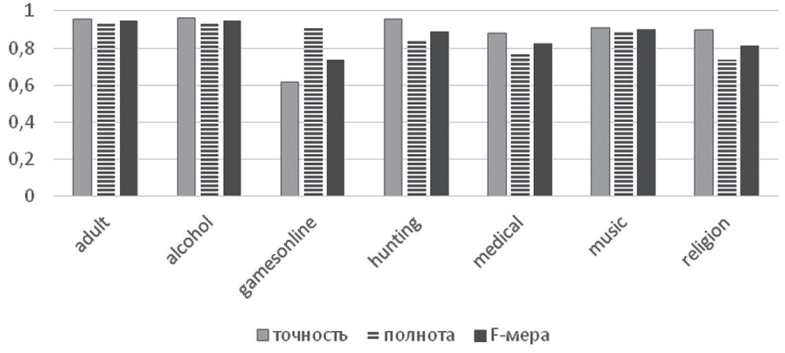


Рис. 23. Оценка точности, полноты и F-меры на наборе 2

Из анализа полученных результатов также можно сделать вывод, что большинство классификаторов характеризуется высокими (87–98%) значениями показателя «точность». Это объясняется использованием деревьев решений в качестве базовых классификаторов и свидетельствует о том, что большинство предсказаний соответствует действительности. В то же время значение показателя «полнота» в большинстве классификаторов не превышает 50%. Это означает, что в «сомнительных» случаях классификатор не стремится отнести информацию к той или иной из своих категорий. Эта особенность важна, например, для производителей антивирусного ПО, для которых недопустимо большое число ложных срабатываний.

При совместном анализе различных признаков точность и полнота классификации приобретают достаточно высокие значения, что объясняется объединением и комбинированием классификаторов, анализирующих

отдельные признаки. В результате система защиты от информации достаточно редко относит веб-сайты к неизвестным (высокая полнота), а количество ложных срабатываний будет достаточно низким (высокая точность). Соответственно, *F*-мера у системы защиты, определяемая через эти два показателя, также будет высокой. В настоящем разделе показано, что защита от нежелательной и вредоносной информации в глобальных информационных сетях является достаточно большой проблемой, основным направлением решения которой является создание и использование автоматизированных систем, способных осуществлять классификацию веб-сайтов по различным признакам с использованием методов интеллектуального анализа данных. Предложенный подход к построению классификатора веб-сайтов реализует трехуровневую иерархическую архитектуру. Экспериментальная оценка программного прототипа автоматизированной системы защиты, реализующего эту архитектуру, показала достаточно высокие значения показателей эффективности классификации для различных категорий веб-сайтов и позволила выявить направления дальнейших исследований, среди которых следует выделить повышение полноты принимаемых решений на основе использования других типов признаков, в том числе текстовых. Работа выполнена при финансовой поддержке гранта РНФ 15–11–30029 в СПИИРАН.

Раздел III.
Социально-психологические и когнитивные аспекты обеспечения национальной безопасности России

Глава 1. Информационно-психологическая и когнитивная безопасность: в поисках мировоззренческих и теоретико-методологических оснований

От мироощущения к идеологии

Рассматривая весь комплекс вопросов об информационно-психологической и когнитивной безопасности, информационно-психологических войнах и операциях, мы должны четко представлять, что их объектом выступает не просто человек, коллектив, общество как таковые, а их духовная деятельность, которая воплощается в мировоззрении, идеологии, общественном сознании и опредмечивается в деятельности, конкретных поступках. Если же мы будет переводить рассуждения о соотношении информационно-психологической и когнитивной безопасности в сферу существования угроз по отношению к человеку, его интеллекту, воле, психосоматической деятельности, то должны четко себе представлять, что информационно-психологические операции существенно отличаются от когнитивных, направленных на деструкцию мироощущения, миропонимания и целостного мировоззрения. Если проще — под воздействием когнитивных операций подавляется сознание противника. Если результатом информационно-психологической войны является нежелание противника продолжать борьбу, то когнитивной — внушение ему мысли, что самой борьбы нет, а враг становится другом. Если результатом

информационно-психологических операций оказывается поражение воли противника, то когнитивных — поражение его сознания.

Попытаемся разобраться в этих «тонких субстанциях», которые порой остаются за пределами анализа существа происходящих во всем многообразии духовной деятельности процессов и зачастую сводятся лишь к сугубо психологическим процессам и явлениям, подвластные манипулированию и управлению. Однако не менее актуальными оказываются проблемы манипулирования и управления собственно духовным миром человека, который самопрезентируется в мировоззрении, идеологических установках и массовом сознании.

В данном контексте мировоззрение будем рассматривать как синтез различных черт духовной деятельности человека, **эмоционально-психологической** стороной которой (на уровне настроений, переживаний, чувств) являются мироощущение и мировосприятие, а миропонимание — это **когнитивно-интеллектуальная** сторона мировоззрения, определяющая способ и характер мыслительной деятельности человека. Миропонимание представляет собой наиболее развитую форму мировоззрения, некий его каркас и его существенную часть. В свою очередь, в мировоззрение входят мироощущение (оно исключительно индивидуально, поскольку человек ощущает с помощью органов чувств то, что на них непосредственно воздействует) и мировосприятие, которое имеет целый «веер» характеристик. Уровень интеллектуальности, да и степень эмоциональной насыщенности мировоззрений неодинаковы. Но, так или иначе, им присущи оба эти «полюса». Даже самые зрелые по мысли формы мировоззрения не сводятся без остатка лишь к интеллектуальным составляющим. Мировоззрение — не просто набор нейтральных знаний, бесстрастных оценок, рассудительных действий. В его формировании участвует не одна лишь хладнокровная работа ума, но и человеческие эмоции в сочетании мироощущения и миропонимания. Какова же структура миропонимания как такового? Это:

— лингвистическое, языковое понимание (при включенном сознании во время бодрствования) на основе владения иностранными языками;
— смысловое понимание, имеющее несколько уровней проникновения в смысл происходящего, в суть процессов и явлений сущего.

Миропонимание — это, во-первых, контекстуальное понимание предложений и повествования. Далее — понимание существа происходящего, установление причинно-следственных связей, части и целого, случайного и необходимого и т. д., следуя канонам диалектического

метода познания. Выделяется также структурное понимание, основанное на изучении структуры изучаемых предметов, процессов и явлений и их элементов, а также системное и эволюционное (историко-генетическое). При этом необходимо учитывать, что понимание — процесс мыслительной деятельности, который заключается в усвоении новой информации и включении его в систему уже устоявшихся идей и представлений. В таком случае смысл предстает как некий продукт, результат понимания в процессе познания (о каком-либо конкретном предмете, процессе, явлении), получивший определенную ценностную характеристику, оценку (достоверности, справедливости, эстетичности, уникальности). Результирующая функция понимания заключается в наделении смыслом объектов социально-культурной и природной реальности и включении его в духовный мир человека и в его деятельность.

В ткани мировоззрения разум и чувства органично переплетены и к тому же соединены с волей, что придает всему составу мировоззрения особый характер. Мировоззрение, по крайней мере, его узловые моменты, его основа, тяготеет к тому, чтобы стать более или менее целостным комплексом убеждений. Таким образом, включаясь в мировоззрение, различные его составляющие приобретают новый статус: они вбирают в себя содержательную сторону взаимоотношений людей, окрашиваются эмоциями, воплощаются в волевые поступки. Даже знания в контексте мировоззрения обретают особую тональность. Срастаясь со всей совокупностью взглядов, позиций, чувств, они становятся больше чем просто знанием, превращаясь в убеждения как целостный способ видения, понимания мира и ориентации в нем. Силу убеждения приобретают также нравственные, правовые, политические и другие взгляды — ценности, нормы, идеалы. В сочетании с волевыми факторами они составляют основу жизни, поведения, действия личностей, общественных групп, наций, народов, а в пределе — всего мирового сообщества. Непременными элементами миропонимания являются вера и сомнение как своеобразные его регулятивы и корректировщики. Диапазон человеческой веры, *у-веренности* широк. Он простирается от практической, жизненной познавательной несомненности (или очевидности), то есть вполне рациональной веры, до религиозных верований или даже легковерного принятия нелепых вымыслов, что тоже свойственно человеческому сознанию определенного типа и уровня. Некогда человек с присущими ему атеистическими убеждениями нежданно-негаданно становится (или представляется) истинно верующим в Бога. Что это — самостоятельный поступок или же результат смены жизненной позиции, влияние смены

социально-политической ситуации в обществе или же манипулятивное внешнее воздействие? Это, правда, вопрос вне поля нашего рассмотрения, однако следует помнить, что великий русский ученый И. П. Павлов, будучи человеком верующим, до конца своей жизни оставался последовательным естественнонаучным материалистом.

В системе мировоззрения в качестве осмысленной позиции как непременного звена всегда присутствует **сомнение**. И вот здесь-то как раз следует обратить внимание на состояние, которое я бы назвал «бифуркацией миропонимания». Любому из нас присуще сомневаться в достоверности той или иной информации, искренности чувств или дружбы окружающих, справедливости поступков или решений. Но в то же время достаточно легко бывает внести сомнения в правильность толкования тех или иных исторических событий или решений, что в корне может перевернуть саму суть миропонимания прошлого и настоящего. Сомнение, в таком случае, предстает как «бифуркационный след миропонимания», ведущий к коренной перестройке мировоззрения, ценностно-смысловых установок личности. Человек теряется в поисках смысла происходящего, а общество взывает к тем, кто способен рассуждать о смысле жизни и истории. При этом необходимо учитывать то, что сомнение есть психическое состояние процесса умственной деятельности, приводящее к невозможности принятия конкретного суждения или же раздвоение его становления вследствие невозможности человека осознанно прийти к какому-либо однозначному выводу. Сомнение является отрицательным в том случае, когда человек не обнаруживает причин, которые позволили бы ему прийти к однозначному решению относительно правильности или ошибочности своего мнения. В этом случае происходит блокирование дальнейшего анализа происходящего. Если же человек выявил причины, дающие основание считать какое-либо одно решающее мнение невозможным, в таком случае сомнение считается позитивным, т. е. допускающим инвариантность в принятии решения. В обоих случаях результатом является: невозможность формирования окончательного суждения, т. е. воздержание от него. На этом же «бифуркационном следе миропонимания» легко включаются механизмы манипуляции сознанием, что должно предполагать выработку превентивных механизмов и методов информационно-психологической безопасности. Дело в том, что сомнение, присущее человеку, недоступно искусственному интеллекту. Какая-либо возникающая перед ним проблема имеет определенный набор решаемых вариантов, предполагающий «взвешивание» с определенной

степенью погрешности, что и вызывает сомнения в достоверности решения проблемы. Системе искусственного интеллекта не присуще сомнение, поскольку состояние неопределенности парализует действие этой системы. Из этого следуют два варианта «разрешения сомнения»:

a) Homo sapiens находится в состоянии «искусственного интеллекта», предполагающего однозначность решения проблемы. В таком случае целевая функция обеспечения информационно-психологической безопасности сводится к блокировке одного из двух вариантов решения проблемы (выход из состояния 2^0, т. е. два в нулевой степени).

b) Homo sapiens собственным разумением доходит до состояния «искусственного интеллекта» ($2^n \rightarrow 2^{n-1} \rightarrow \ldots 2^0$). Далее реализуется вариант **a**).

Решение проблемы (разрешение сомнения) может считаться окончательным, или абсолютно определенным, лишь в случае его привязки к определенной точке зрения, одной системе координат, в качестве которой следует рассматривать идеологию. Мировосприятие регулируется этическими нормами и ценностными установками, присущему данному обществу, что дает основание рассматривать его как наиболее дифференцированную форму мировоззрения, которая более всего подвержена какому-либо внешнему воздействию, будь то воспитание, обучение или же программируемое психологическое воздействие. Более того, мировоззрение — это единство знаний и ценностей, разума и чувств, миропонимания и мироощущения, разумного обоснования и веры, убеждений и сомнений, закрепляющихся в идеологии. Сочетание таких «полярностей» в одном целом, будь то конкретный индивид, «коллективный разум» или общественное сознание тех или иных социальных общностей, неизбежно предполагает определенные деформации этого целого в случае какого-либо целенаправленного внешнего воздействия на один или несколько компонентов мировоззрения [1].

Смысл сам по себе относится к тем загадочным для многих явлениям, которые считаются вроде бы общеизвестными, поскольку постоянно фигурируют как в научном, так и обыденном общении. Помимо семантических определений смысла, существуют и прагматические, которые оценивают это явление с позиции человека как субъекта деятельности. В этом случае смысл обретает статус ценности, значимости, становится

---

[1] *Козлова М. С.* Мироощущение и миропонимание // Введение в философию / Авт. колл.: Фролов И. Т. и др. 3-е изд., перераб. и доп. М.: Республика, 2003. 623 с.

характеристикой какой-либо полезности предмета. Смысл обретается в контексте жизненной ситуации, потребностей, самосохранения и проективной деятельности. Смысл содержит компонент как знания о предмете, так и отношения к нему. В выражении «какой в этом смысл?» смысл отождествляется с пользой. Понимание смысла происходящего, будь то природные и социально-политические процессы или же повествовательный текст, следует рассматривать как результат познания, получивший определенную ценностную характеристику, оценку достоверности, справедливости на основе определенной нормы, стандарта, принципа. Понять можно то, что сравнимо с чем-либо уже существующим. Функция понимания заключается в наделении определенным смыслом объектов социально-культурной реальности и включении их в духовный мир человека и его повседневную деятельность. Понять поступок, действия кого-либо предполагает необходимость объяснения тех целей и ценностей, которые мотивировали их свершение («В ситуации ***A*** следовало совершить поступок ***x***; человек ***D*** находился в ситуации ***A***; значит, он должен совершить поступок ***x***»). Причиной многообразия характеристик смысла является его многогранность, многозначность его проявления в разных ситуациях. Если в одних случаях имеется в виду субстанциональная сущность смысла, то в других — способы его программирования в тексте, в третьих — закономерности декодирования и др. Это означает необходимость наличия большого спектра процедур по обеспечению информационно-психологической безопасности. Смысл характеризуется тем, что его необходимо «искать», «понимать», что свидетельствует не о рутинном, а о творческом характере этого процесса. Смысл является результатом понимания, его конечной целью, но и само по себе понимание происходит на основе поиска смысла.

В таком случае возникает вопрос о том, как соотносятся между собой «смысл-инструмент» и «смысл-результат» применительно к вопросу об обеспечении собственно психологической безопасности, информационно-психологической и когнитивной безопасности в рассматриваемом нами контексте. Ответы на поставленные вопросы в одних случаях могут оказаться достаточно простыми, в других же случаях это может потребовать проведения специальных исследований, тем более что в своей деятельности человек ищет смысл, который служит ему и целью, и стимулом, и средством: «Человек стремится обрести смысл и ощущает фрустрацию или вакуум, если это стремление остается нереализованным» [2].

---

[2] *Франкл В.* Человек в поисках смысла. М.: Прогресс, 1990. С. 11.

В таком случае мы должны обратиться к выяснению вопроса о том, как эта проблема решается, с одной стороны, собственно психологами, а с другой — в контексте социологии жизни как теоретико-методологической основы исследований жизненного мира.

Первой системой научной психологии, обратившейся к понятию смысла для объяснения поведенческих проявлений человека (преимущественно непроизвольных), закономерно стал психоанализ [1]. Как утверждал в свое время Дж. Клейн, «Ориентация на поиск смысла и используемые концептуальные орудия позволяют аналитику видеть закономерности, отличные от тех, которые обычно видят другие психологи, наблюдающие то же самое поведение» [2]. Это дает основание, как следует из данного утверждения, относить психоанализ к «классу теорий… пытающихся утверждать, что поведение имеет определенный смысл, который можно вывести из истории этого смысла в жизни личности» [3]. Другой представитель научной психологии А. Адлер, предшественник современного экзистенциально-гуманистического направления в психологии, связывал смысл жизни с представлениями о трех фундаментальных жизненных проблемах, вытекающих из соответствующих трех объективных аспектов человеческого бытия (трех «связей»):

— факт жизни человека на Земле в конкретных условиях существования порождает проблему труда и профессионального самоопределения;
— факт жизни человека в обществе порождает проблему межличностных отношений, кооперации и дружбы;
— факт существования двух полов порождает проблему отношений между ними, любви и брака.

Смысл жизни, по Адлеру, определяется этими тремя связями, заключен в них, и правильное решение трех жизненных проблем помогает нам найти его. «Если бы мы поняли смысл жизни, — пишет он, — то целенаправленный взлет человеческого рода нельзя было бы остановить. У нас была бы общая цель, и все направили бы все свои силы на служение задаче осуществить этот смысл <…>Смысл нашей жизни был бы компасом для нашего стремления <…>Пока же мы не обладаем таким смыслом, наши повседневные смыслы во всем своем многообразии кажутся

[1] *Леонтьев Д. А.* Психология смысла: природа, строение и динамика смысловой реальности. 2-е, испр. изд. М., 2003. С. 27.

[2] *Klein G. S.* Psychoanalytic theory: an explorations of essentials. New York: International Universities press, 1982. X, 330 p. P. 52.

[3] Ibid. P. 56.

нам — не столько рассудку, сколько чувствам — неустойчивыми и легко взаимозаменяемыми. Мы меняем свою одежду, свой образ мыслей, свою профессию, своих мужей и жен, своих друзей, и ищем в них ценности, которые сами же потом отвергнем» [4].

В целях более глубокого прояснения проблемы манипулятивного воздействия на смысловую реальность, в пределах которой осуществляется и волевая саморегуляция личности, и управление его поведением, обратимся к вопросу о смысле как интегрирующем факторе человеческой жизни, как его решал В. Франкл, определяя человека как существо, которое постоянно решает, кем он будет в следующий момент («Человек решает за себя; любое решение есть решение за себя, а решение за себя — всегда формирование себя») [5]. Принятие такого решения — акт не только свободы, но и ответственности, а свобода, лишенная ответственности, вырождается в произвол. Эта ответственность сопряжена с бременем выбора человеком, какие таящиеся в мире и в нем самом возможности заслуживают реализации, а какие нет. У Франкла, в отличие от Адлера, для которого смысл жизни выступал как нечто непроизвольно и неизбежно складывающееся в первые годы жизни человека, обретение и реализация смысла выступает как стоящая перед ним задача, на решение которой он направляет все свои усилия. Иначе говоря, Франкл предложил психологическую интерпретацию смысла как определенной смысловой реальности, в которой для человека первично самостоятельное обретение и реализация смысла. Внешнее манипулятивное воздействие, препятствующее этому, устранимо с помощью такого же внешнего психологического приема, который вступает в резонанс с ответственным «решением за себя». В этом, на наш взгляд, заключается тот идейно-теоретический потенциал представлений о смысле, смысловой реальности субъекта, которые дают основание рассматривать в конструктивном плане вопросы информационно-психологической безопасности. Практически все те приемы, которые входят в арсенал средств волевой саморегуляции, — как подтверждают психологические исследования, приведенные и обобщенные Д. А. Леонтьевым, —в применении к другому человеку оказываются средствами управления его поведением в контексте межличностной манипуляции, к которым относятся:

— переоценка значимости мотива или предмета потребности;

---

[4] *Adler A.* Psychotherapie und Erziehung: Ausgewahlte Aufsatze. Bd I: 1919–1929 / Hg. von H. L. Ansbacher, R. F. Antoch. — FrankfurtamMain.ю 1982. 267 s. S. 79.

[5] *Франкл В.* Человек в поисках смысла. М.: Прогресс, 1990. С. 114.

— изменение роли, позиции человека;
— предвидение и переживание последствий действия или отказа от его осуществления;
— обращение к внешним символам, напоминающим о последствиях действий, к ритуалам, укрепляющим значимость совершаемых действий, к другим людям или божеству за поддержкой;
— соединение заданного и принятого действия с новыми мотивами или с новыми целями и за счет этого переосмысление действия;
— включение заданного действия в другое, более широкое и значимое для человека действие;
— связывание заданного действия с возможностью затем осуществить другое желаемое человеком действие;
— связывание действия с обещаниями и клятвами другим людям и себе, с самооценкой и самоодобрением, со сравнением себя с другими людьми или литературными героями при выполнении необходимого действия.Чтобы сделать правильный выбор, субъекту предстоит построить общее пространство смысловых критериев сравнения всех альтернатив и затем сделать свой выбор. Если же такое пространство не будет построено, то выбор будет делаться по одним основаниям без учета других. Ответ на вопрос «что такое хорошо и что такое плохо» зависит от ответа на вопрос: «по каким критериям» [1].

Мировоззрение представляет собой систему взглядов, оценок представлений о мире и месте в нем человека, общее отношение человека к окружающей действительности и самому себе. Мировоззрение придает деятельности человека организованный, осмысленный и целенаправленный характер, будучи оформленное в идеологию как определенную систему моральных, эстетических, научных, религиозных (или же атеистических), политических и правовых взглядов, идей, теорий. Любая идеология обусловлена конкретно-исторически и носит социально-классовый характер. Идеология как система теоретических взглядов отражает масштабы познания обществом мира в целом и отдельных его сторон и потому представляет более высокий, по сравнению с общественной психологией, уровень общественного сознания. Нет идеологии индивидуальной: она всегда носит общественный характер, но индивидуализируется в мировоззрении конкретного человека и различных социальных

[1] *Леонтьев Д. А.* Психология смысла: природа, строение и динамика смысловой реальности. 2-е, испр. изд. М.: Смысл, 2003. С. 354–355; *Иванников В. А.* Психологические механизмы волевой регуляции. М.: Изд-во МГУ, 1991. 142 с.

групп. Необходимо иметь в виду, что понятие «идеология» употребляется в социальной философии в еще одном, более узком смысле — как система теоретических взглядов одной большой социальной группы, прямо или опосредованно отражающая ее коренные интересы. Таким образом, если в первом случае доминирует познавательный аспект, выясняется уровень общественного сознания, то при втором варианте применения акцент смещается в сторону аксиологического (ценностного) аспекта, причем оценка тех или иных социальных явлений и процессов дается с узкогрупповых позиций.

Правда, при обращении к вопросу о социальной основе современной идеологии невольно обращаешь внимание на то, что современные российские социологи как-то невразумительно высказывают свое отношение к классическому ленинскому определению классов и сводят свои расчеты и рассуждения о «среднем классе» как об аморфном, но весьма многочисленном, социальном слое, который помещают между «высшим классом» (собственники экономических ресурсов общества) и «низшим классом» (промышленные наемные рабочие, низкоквалифицированные работники). Однако данный термин для социологии до сих пор остается не столько понятием, сколько метафорой. В общепринятом понимании «средний класс» классифицируется по признаку дохода — то есть был не классом в строгом значении, а всего лишь стратой. Свое же сугубо классовое существование эта страта получает на наднациональном уровне — как часть формировавшегося на протяжении всего прошлого столетия глобального эксплуататорского класса. К концу XX века все более отчетливо стало выявляться несоответствие между внутринациональной и наднациональной социальной структурой: прежние эксплуатируемые в государственных пределах (в странах «первого мира») начали превращаться в эксплуататоров в мировом масштабе. В этом несоответствии — ключ к классовым отношениям в рамках сегодняшнего глобального порядка. Сегодня, как справедливо отмечает Ю. И. Семенов, формируется глобальное классовое общество с «центром» и «периферией» в качестве глобальных классов, не отменяющих традиционной классовой структуры отдельных обществ, но служащих к ней дополнением [2].

В таком глобальном классовом обществе формируется и соответствующая глобальная идеология сильного, власть имущего. В новом глобальном обществе, которое американский литературовед М. Хардт и итальянский

---

[2] *Семенов Ю. И.* Философия истории. М.: Современные тетради, 2003. С. 510–513, 613–617.

политический философ А. Негри назвали «Империей», материальный и нематериальный труд оказывают принципиально различное воздействие на общество. Если промышленная или сельскохозяйственная продукция при капитализме имеет чисто товарное значение, то идеи, информация, аффекты и все остальное, произведенное нематериальным трудом, — это уже не столько товар, сколько *средство манипулирования населением* (курсив наш. — *И.К.*). Нематериальный труд создает «не просто товары в вещественном смысле, а социальные взаимоотношения и жизненные формы как таковые» [1]. В новом глобальном обществе — «Империи», в котором идеология — это указанное выше *средство манипулирования населением*, ее смысл, по меткому выражению А. С. Панарина, выражается в таких феноменах, как последовательное отстранение от всех местных интересов, норм и традиций, отказ от завоеваний великой эпохи модерна, переориентация с демократии на властные системы, зависящие от глобальных экономических и политических центров силы и влияния, а в международных отношениях — подмена плюралистической системы международного равновесия, базирующегося на принципе национального суверенитета, апологией диктата ревнителей «однополярности».

При рассмотрении идеологии как базового социального механизма формирования мировоззрения, социальных установок и ориентаций личности в качестве системы указанных выше взглядов, идей, теорий необходимо учитывать, для сравнения, особенности идеологии американской, роль которой выполняет эквивалентный понятийный конструкт «американская мечта», выступающая аккумулятором высших ценностей американского государства. «Американская мечта», изначально утверждающая идею национального превосходства, вбирает в себя мессианизм, эсхатологию, идею и образ «плавильного котла», гражданскую религию, традиционализм и патриотизм, которые выступают основой системы государственного управления и, соответственно, политики. Это, что говорится, идеология для внутреннего пользования американцами. Когда же речь заходит о внешней политике, то американская идеология однозначно следует в русле неоконсерватизма, который, несмотря на свой неофициальный статус, с 80-х гг. XX в. является политической идеологией американской властной элиты. У. Кристол, один из лидеров неоконсерватизма и соруководитель проекта «Новый американский век» (PNAC)» откровенно заявлял: «“национальные интересы” для великой державы

[1] *Хардт М., Негри А.* Множество: война и демократия в эпоху империи. М.: Культурная революция, 2006. С. 125.

не являются геополитическим понятием — за исключением довольно прозаических вещей вроде торговли или проблем охраны окружающей среды. Лишь маленькие нации справедливо полагают, что их интересы замыкаются в их границах, так что их международная политика почти всегда является охранительной. Интересы больших наций гораздо шире. Большие нации, чья идентичность построена на идеологии, как в случае с почившим в бозе Советским Союзом и как с ныне здравствующими Соединенными Штатами, неизбежно имеют идеологические интересы в дополнении к более материалистическим заботам» [2]. В подтверждение этого В. Э. Багдасарян приводит выдвинутую недавно Д. Трампом новую идеологическую формулу: «Американизация, а не глобализация! Это наш новый девиз. Мы должны расстаться с якорем, который нас тянет вниз» и задает риторический вопрос: сумеет ли Россия выдвинуть такую идеологию? «США смогли, — рассуждает по этому поводу Багдасарян, — стать сверхдержавой и достигнуть политического доминирования в мире, артикулировав идентичную американскую идеологию. Эта идеология имела двоякое преломление — внутреннее, мотивировавшее американцев на свершения, и внешнее, побуждающее другие народы идти под американские знамена. Победить такого противника возможно только имея не уступающую ему по мотивационным потенциалам и мировой конвертируемости идеологию» [3].

Действительно, российское общество ныне находится в поисках «объединяющей идеологии», потребность в которой давно назрела, тем более что, с одной стороны, признание пагубности неолиберального курса, которому продолжает следовать российское правительство, становится очевидным, а с другой — заявления В. В. Путина о необходимости возглавить курс на создание «Большой Евразии» взывают к ее созданию. Однако на сегодня мы имеем российскую Конституцию, в которой государственная, которой должна быть «объединяющая идеология», никак не закреплена. Согласно 13-й статьи Конституции: «1. В Российской Федерации признается идеологическое многообразие. 2. Никакая идеология не может устанавливаться в качестве государственной или обязательной». В качестве одной из основ конституционного строя России устанавливается принцип многообразия (плюрализма) в сфере идеологии.

---

[2] *Irving Kristol*. The Neoconservative Persuasion // The Weekly Standard, August 25, 2003.

[3] *Багдасарян В. Э.* Идеократия США: опыт американского идеологического строительства для России // www.1601228-ideokratiya-ssha-opyt-amerikanskogo-ideologicheskogo-stroitelstva-dlya-nbsp-rossii.

Обратимся к российской истории. «В длительном процессе своего исторического развития, — отмечал Г. В. Вернадский, — русский народ освоил и объединил территорию Евразии в смысле политическом, экономическом и культурном, сперва в виде Российской Империи, затем в виде Советского Союза» [1]. Исходя из того тезиса, что история Евразии есть история совокупности народов Евразии, Вернадский делает вывод, что «русская история есть отдел истории отдельных евразийских народов — или народов СССР — причем русская история поневоле должна была включать в поле своего зрения геополитически все более и более широкую область по мере того, как русский народ в своем историческом развитии охватывал все большую и большую часть евразийского месторазвития» [2]. Но, что более важно отметить в контексте рассматриваемой проблемы, Вернадский особое внимание обращал на необходимость сохранения «евразийского самосознания» как той идеологемы «евразийской миссии России» [3]. На протяжении XX–XXI вв. евразийство выступает «идеей-силой», которая объединила духовные интенции православного мессианизма «Москва — Третий Рим», славянофильские идеи о самобытности русской культуры, принцип культурно-цивилизационного разнообразия Н. Я. Данилевского, идею пассионарности Л. Н. Гумилева, советский проект и выражающую его созидательную роль социалистическую идеологию.

Представляется, что евразийство как государственная «объединяющая идеология» современного российского общества имеет полное право на свое существование, выступать смысловым ориентиром, социально-политическим ядром мировоззрения и общественного сознания, а также методологическим основанием обеспечения информационно-психологической безопасности. Необходимость разработки этих методологических оснований вполне соответствует положениям недавно принятой Доктрины информационной безопасности Российской Федерации (5.12.2016). В ней, в частности, отмечается, что национальными интересами в информационной сфере является «применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации» (ст. 8а), а одним из основных направлений обеспечения информационной

[1] *Вернадский Г. В.* Опыт истории Евразии с половины VI века до настоящего времени // Вернадский Г. В. Опыт истории Евразии. Звенья русской культуры. М.: КМК, 2005. С. 4.

[2] Там же. С. 5.

[3] *Вернадский Г. В.* Начертание русской истории. СПб.: Лань, 2000. С. 35–36.

безопасности в области обороны страны выступает «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества» (ст. 21д).

Когнитивные науки, НБИКС-технологии и когнитивная безопасность. В системе мер обеспечения глобальной безопасности, наряду с информационно-психологической безопасностью, необходимо особо выделять когнитивную безопасность. Выше речь уже шла о взаимосвязи последней с информационно-психологической безопасностью. В данном случае мы будем рассматривать феномен когнитивной безопасности в связке «когнитивные науки — когнитивные технологии — когнитивные операции –когнитивная безопасность». Это вполне объяснимо: чтобы решать проблемы обеспечения когнитивной безопасности, связанные с выработкой превентивных мер противодействия когнитивным операциям в ходе гибридных войн, мы должны иметь четкие представления о когнитивных технологиях, о которых ученые стали говорить и писать с первых лет XXI в., рассматривая их как систему, объединяющую нано-, био-, инфо- и когнитивные технологии (НБИК-технологии). Сами по себе когнитивные технологии разрабатываются, как уже отмечалось во второй главе второго раздела книги, на основе когнитивной науки. Остановимся на этом вопросе несколько подробнее.

Когнитивная наука. Когнитивная наука (когнитивистика) представляет собой междисциплинарное научное направление, которое нацелено на изучение мыслительной деятельности человека, в первую очередь, методами когнитивной нейробиологии, объединившей усилия психологии, нейробиологии и теории искусственного интеллекта. Когнитивная нейробиология, сформировавшаяся на базе психологии и нейробиологии в 80-х гг. XX в., нацелена на изучение связи активности головного мозга человека с различными психическими процессами, мыслительной деятельностью (ее нейронной основой) и поведением человека. Изначально когнитивная нейробиология заявила о себе как экспериментальная наука, занимающаяся изучением нарушений психической деятельности людей вследствие каких-либо повреждений головного мозга. В процессе своего становления предметом когнитивной нейробиологии определились процессы, происходящие в человеческом мозгу, направленные на создание так называемого «сильного искусственного интеллекта», способного к самообучению, творчеству, свободному общению с человеком. У истоков теории когнитивизма, наряду с представителями психологии и нейрофизиологии, стоял Н. Винер,

который, вспоминая о своих работах в Массачусетском технологическом институте в годы Второй мировой войны, отмечал, что «практический интерес к вычислительным машинам побудил меня заняться общей философией проблемы… мы начали понимать, что существует определенная аналогия между цифровыми вычислительными машинами и человеческим мозгом, особенно если принять во внимание то обстоятельство, что импульсы в нервной системе, по всей видимости, подчиняются закону "все или ничего" и, следовательно, изображают две цифровые возможности… Мне стало ясно, что человеческий мозг служит своего рода показателем того, на что способна автоматическая машинерия, и подчиняется тем же принципам» [1].

С тех пор минула целая эпоха революционных открытий в науке и технике, приведших на современном этапе к практическому применению НБИК-технологий. По справедливому замечанию акад. А. П. Кулешова, из общего объема данных, находящихся в мировом совокупном storage (совокупное компьютерное пространство для хранения документов), более 90% появились за последние несколько лет. Современные информационные технологии позволяют получать принципиально новые знания в различных областях человеческой деятельности — от машиностроения до социологии. По сути это означает извлечение новых знаний из больших объемов информации [2]. В таком случае объектом познавательной деятельности начинает выступать уже не сам по себе человек и окружающая его природная и социальная реальность, а информация о них, созданная и полученная ранее. Оборотная сторона этого процесса — уникальная возможность манипулировать этой информацией: управление формированием нового знания может привести к созданию некоего «параллельного мира», не адекватного реальной действительности и чуждого смыслу человеческого существования.

Когнитивные технологии в связке НБИКС-технологий. В этой «связке технологий» нанотехнологии — это технологии и соответствующее оборудование для атомно-молекулярного конструирования любых материалов. Если двигаться по этому пути, то это означает, как отмечает М. В. Ковальчук, переход к нанотехнологиям, к атомарному конструированию, который дает «важнейший результат — дематериализацию

---

[1] *Винер Н.* Мое отношение к кибернетике. Ее прошлое и будущее. М., 1969. С. 15, 18.

[2] URL: http:// www.ras.ru/news/shownews.aspx?id=4581d2db-f466–4ae5–8704-db40f015a7a8

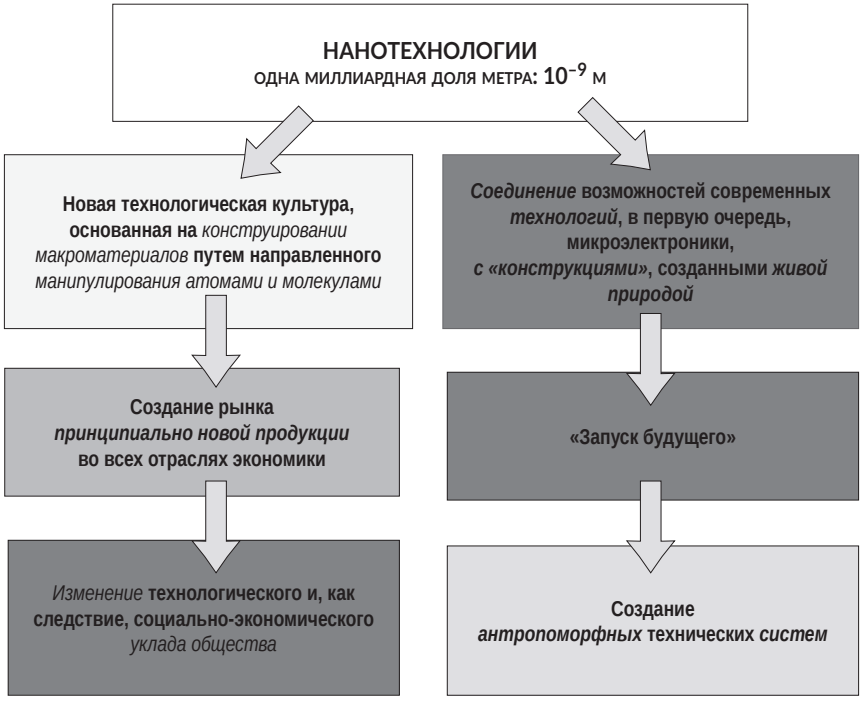


Рис. 24. Направления развития нанотехнологий

производства и резкое качественное уменьшение энерго- и ресурсоемкости. При этом развитие нанотехнологий подразумевает развитие двух самостоятельных направлений»[3] (рис. 24).

Обратим внимание на то, что одно из направлений развития нанотехнологий (на рис. 24 справа) органично связано с решением задач развития био- и когнитивных технологий. Это направление развития нанотехнологий называется «запуск будущего» и состоит в соединении возможностей современных технологий, в первую очередь твердотельной микроэлектроники как наивысшего технологического достижения современности, с «конструкциями», созданными живой природой (рис. 25).

Сегодня, продолжает далее Ковальчук, мы подошли к технологическим

[3] *Ковальчук М. В.* Конвергенция наук и технологий — прорыв в будущее // Российские нанотехнологии. 2011. № 1–2.

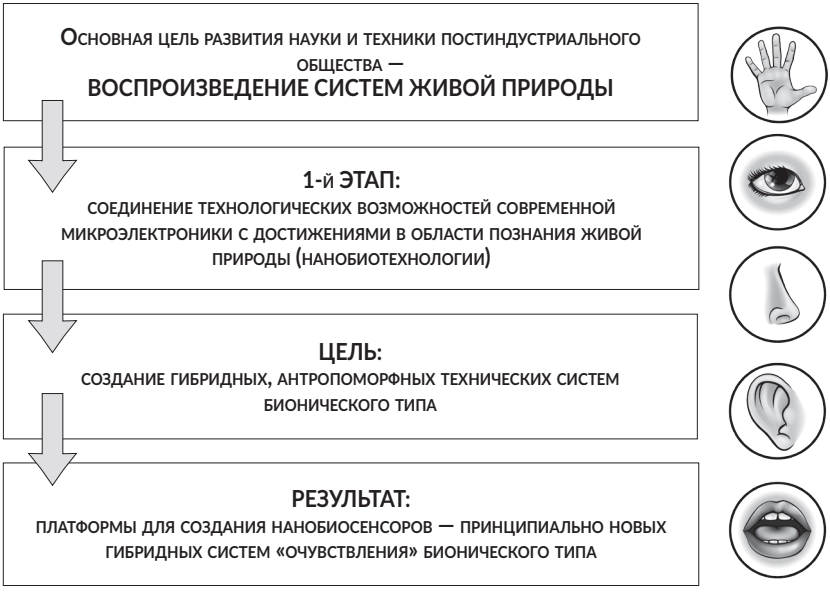


Рис. 25. «Запуск будущего»

решениям, в основе которых лежат базовые принципы живой природы, — начинается новый этап развития, когда от технического, модельного копирования «устройства человека» на основе относительно простых неорганических материалов мы готовы перейти к воспроизведению систем живой природы на основе нанобиотехнологий (рис. 26).

Что касается собственно когнитивных технологий, то они, по мнению Ковальчука, могут предоставить возможность, «основываясь на изучении функций мозга, механизмах сознания, поведения живых существ, разрабатывать алгоритмы, которые фактически и будут “одушевлять” создаваемые нами системы, наделяя их неким подобием мыслительных функций» [1]. Когнитивные (познавательные) технологии — это те же информационные технологии, описывающие основные мыслительные процессы человека, которым уготовано фантастическое будущее, где временна́я смена событий происходит ускоренными темпами. В настоящее время объем информации, который накопило о себе человечество, удваивается каждые 4 года, а в 2020 г. он будет удваиваться уже каждые 72

[1] Там же.

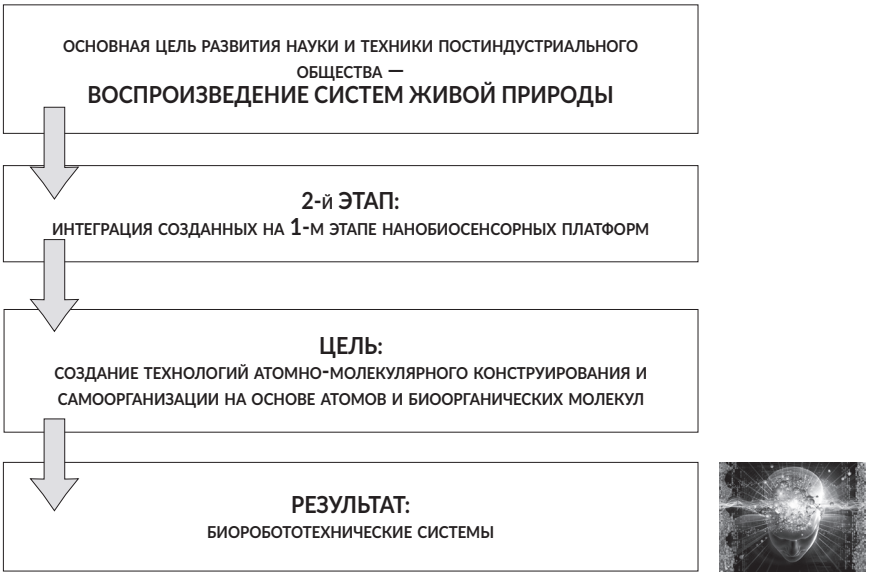


Рис. 26. Применение нанобиотехнологий

дня. По мнению специалистов компании Cognitive Technologies, сегодня, в условиях колоссального роста объема необходимой для обработки информации, ее нечеткости, сокращения времени для принятия решения и т. п., традиционные подходы к решению многих управленческих задач оказываются бессильными. И здесь на первый план выходят когнитивные технологии. В конце XX века произошел научный прорыв, связанный с исследованиями мозга, с компьютерным моделированием элементов сознания. Появились математические модели таких процессов и явлений, изучение которых еще недавно считалось предметом и привилегией гуманитарных дисциплин. Когнитивные технологии получили широкое применение при описании слабоструктурированных систем, которым характерно отсутствие достаточной количественной информации о динамике их функционирования, изменчивость характера процессов во времени и т. д. Предметом когнитивных технологий стали возможность и условия автоматизации таких мыслительных процессов, как интуиция, ассоциативность мышления, догадка, предвидение. Специалисты в области информационных операций и геополитики руководствуются теперь не только ставшим уже традиционным правилом

«***Кто владеет информацией, тот правит миром***», но и новым — «***Кто умеет систематизировать информацию и из нее получать знания, тот правит миром!***» [1]

Когнитивные технологии используют данные о процессах познания, обучения, коммуникации, обработки информации человеком и животными на представление нейронауки, на теорию самоорганизации, информационные технологии, математическое моделирование элементов сознания. Основой для внедрения когнитивных технологий во все сферы общественной жизни должно быть наличие гигантской информационно-телекоммуникационной инфраструктуры от глобального до локального уровня. Ряд авторов отмечают, что когнитивные технологии ориентированы на следующий шаг — на помощь человеку в постановке задач, на решение плохо формализованных творческих задач, на выявление и эффективное использование своего когнитивного потенциала, своей способности познавать, мечтать, творить. Компьютерные технологии в считанные десятилетия из больших, дорогих, сложных инструментов ученых и военных превратились в товары массового потребления, изменили работу, досуг и образ жизни сотен миллионов людей. В настоящее время возникла реальная возможность создания когнитивной отрасли промышленности, сравнимой по масштабу с компьютерной индустрией. Когнитивный вызов, с которым столкнулись мир и Россия, открывает новые горизонты. К быстрому прогрессу когнитивных технологий, к превращению этой области в мощную индустрию человечество понуждает объективная потребность быстрого достижения нового качества управления во всё более сложном и нестабильном мире [2] (рис. 27).

Кстати, в своем выступлении в Совете Федерации 30 сентября 2015 г. М. В. Ковальчук обратил особое внимание сенаторов на угрозы, глобальные вызовы, которые таит в себе природоподобная технология. Вот некоторые выдержки из этого выступления: «Мы, с одной стороны, переходим к технологическому воспроизведению живой природы<…>Но возникает возможность целенаправленного вмешательства в жизнедеятельность человека, даже в процесс эволюции<…> Развиваются когнитивные исследования по изучению мозга, сознания, значит, фактически, открывается возможность для воздействия на психофизиологическую сферу человека, причем очень легкую и простую<…> Существует обратная связь

---

[1] URL: https://mipt.ru/education/chairs/KognTech/about/future.php.

[2] *Малинецкий Г. Г., Маненков С. К., Митин Н. А., Шишов В. В.* Когнитивный вызов и информационные технологии // Препринт ИПМ им. М. В. Келдыша. 2010. № 46.

УКРУПНЁННАЯ БЛОК-СХЕМА КОГНИТИВНОЙ ОТРАСЛИ

Рис. 27. Одна из возможностей организации когнитивной отрасли

мозго-машинных интерфейсов или мозго-мозговых, когда вы можете создавать ложную картину действительности внутри человека<…> В природоподобии двойственный характер технологий изначально: размыты границы между гражданским и военным применением, а как следствие — полная неэффективность существующих методов контроля<…> Сегодня возникла реальная технологическая возможность в процессе эволюции человека. И цель — создать принципиально новый подвид *Homo sapiens* — "служебного" человека <…> сегодня биологически это становится возможным сделать. Свойство популяции "служебных" людей очень простое: ограниченное самосознание, и когнитивно это регулируется элементарно, мы с вами видим, это уже происходит. Вторая вещь — управление размножением, и третья вещь — дешевый корм, это генно-модифицированные продукты. И это тоже уже все готово. Значит, фактически, сегодня уже возникла реальная технологическая возможность выведения "служебного" подвида людей» [1].

Честно говоря, к подобным заявлениям следует отнестись весьма осторожно и не торопиться с выводами. Эти рассуждения напоминают то, чему была посвящена научно-фантастическая пьеса К. Чапека R. U. R. («Россумские универсальные роботы» — от *чеш.* Rossumovi univerzální roboti,), написанная в 1920 году. Пожалуй, будет уместно кратко напомнить содержание пьесы. В прологе речь идет об ученом Россуме-старшем, который поставил своей целью опровергнуть существование Бога путем создания искусственных людей. Россум-младший отбросил такую философию и начал производить на заводе упрощенных человекоподобных существ для выполнения различных работ, что и положило начало технологии создания роботов — существ, обладающих знаниями и умениями, но лишенных чувств, желаний, потребностей. В первом акте мечты директора фабрики R.U. R. освободить человека от унизительного труда, создать ему обстановку безграничного благополучия осуществились — на Земле царит мир изобилия — товары и пищевые продукты в избытке производят роботы. Однако остановилось воспроизводство рода человеческого как такового, и в то же время начались спонтанные «мутации» среди роботов. Вскоре люди узнали о том, что роботы во всем мире восстали. Во втором акте восставшие роботы уничтожают фабрику R.U. R. и уничтожают всех людей на Земле, оплакивавших крах цивилизации, за исключением одного. В третьем акте — на Земле остался только старый архитектор

[1] Стенограмма выступления М. В. Ковальчука в Совете Федерации 30 сентября 2015 г. URL: http://trv-science.ru/2015/10/08/vystuplenie-mikhaila-kovalchuka-v-sf/ 08.10.2015.

Алквист, которого правительство роботов заставляет восстановить формулу, чтобы продолжить создание роботов. Для этого архитектор пытается вскрыть живых роботов, чтобы понять, как оживить вновь созданных. Выбор пал на пару роботов, которые отказались, защищая друг друга от смерти и предлагая каждый себя в обмен на другого. И, о чудо! Последний из оставшихся людей на Земле, обратившись к Библии, вдруг прозревает: «Жизнь не погибнет! Она возродится вновь от любви, возродится — нагая и крохотная, и примется в пустыне, и не нужно будет ей все, что мы делали и строили, не нужны города и фабрики, не нужно наше искусство, не нужны наши мысли… Но она не погибнет! Только мы погибли! Рухнут дома и машины, развалятся мировые системы, имена великих опадут, как осенние листья… Только ты, любовь, расцветешь на руинах и ветру вверишь крошечное семя жизни…»

Не правда ли, сюжет пьесы почти столетней давности очень напоминает события сегодняшнего дня? Наступил 2017 год, и в информационном пространстве начали появляться тревожные сообщения о налогах на роботов. Об этом одним из первых заявил Б. Гейтс: необходимо введение подоходного налога на роботов, которые заменяют людей на производстве. Он указывает на быстрое развитие робототехники и особенно технологий искусственного интеллекта, что резко ускорит тренд роботизации. Гейтс уверен, что без регулирования рынок не сможет самостоятельно справиться с эффектами очень быстрого перехода к производственным технологиям нового поколения. Тренд информатизации и роботизации развивается очень быстро, доля дистанционных работников в США близка к 40%. Ведущие производители рассматривают возможность создания в США заводов-роботов, в результате чего под угрозой окажутся 80 млн рабочих мест.

Какие последствия может иметь осуществление этой идеи? Концепция проста: рабочий на заводе платит подоходный налог, а робот, который приходит на смену рабочему, налог не платит. В результате роботы занимают рабочие места людей, но при этом налоговые поступления в бюджет страны снижаются. Это приводит к негативным макроэкономическим последствиям в виде дефицита бюджета, роста налоговых ставок, инициатив, ограничивающих финансовые возможности бизнеса, и т. д. Таким образом, по мнению сторонников «налога с роботов», необходимо взимать дополнительный налог с автоматизации, то есть, фактически, с повышения эффективности производства. Политики, обеспокоенные таким ходом событий, уже рассматривают вопрос введения ограничительных мер, которые могли бы дать время на подготовку к переходу

на автоматизированные технологии производства. В частности, в ЕС уже рассматривался вопрос введения «налога на роботов» для оплаты учебы потерявших работу людей, но пока парламентарии отвергли эту идею. В конечном счете, тренд роботизации не изменить, и деревянный ботинок в ткацком станке не управляет прогрессом. Единственным выходом является повышение квалификации рабочей силы, и этот тренд будет актуален всегда [1].

Когнитивные риски, операции и безопасность. Прежде всего, следует отметить, что весь круг вопросов, относящихся к рискам, которые порождаются конвергентными технологиями, необходимо анализировать так же конвергентно, совместно, поскольку сама по себе элементная база, обеспечивающая возможные риски, имеет однопорядковые наноразмеры:

— одна живая клетка, имеющая генетический код, может служить оружием массового поражения;
— исследования по изучению мозга, сознания открывают возможности для воздействия на психофизиологическую сферу деятельности человека;
— существующая обратная связь мозго-машинных или мозго-мозговых интерфейсов позволяет создавать ложную картину действительности в сознании человека, управлять индивидуальным и массовым сознанием. Рассуждения подобного рода приводят к тому выводу, что конвергентные НБИК-технологии — это не просто очередной этап технологического развития; они открывают реальные перспективы разрушения жизненного мира человека, тех устоев, которые делают человека человеком.

Следует иметь в виду, что создание принципиально новой технологической базы природоподобных технологий, т. е. включение их в цепочку замкнутого ресурсооборота, существующего в природе, порождает большую «зону риска»: в природоподобии размыты границы между гражданским и военным применением, а как следствие — полная неэффективность существующих методов контроля. В связи с этим большая роль должна отводиться разработке и привлечению гуманитарных технологий, что дает право говорить о создании новой конвергентной НБИКС-технологии, где «С» означает социогуманитарные технологии. Недаром еще в 2003 г. в материалах одной научной конференции были четко определены на ближайшие 10–20 лет семь направлений использования разработок НБИК-технологий с целью

[1] URL: https://www.ffin.ru/market/review/82/57919/#ixzz4Zvgi2E2M.

обеспечения национальной безопасности США, в т. ч. создание боевых машин-роботов, приложение интерфейса мозг-машина, немедикаментозное лечение для повышения работоспособности человека и др. Реализация этих целей потребует тесной интеграции нанотехнологии, биотехнологий, информационных технологий и когнитивных областей деятельности, а «чистый результат выполнения поставленных целей позволит сократить вероятность войны, предоставляя подавляющее технологическое преимущество США, значительно сократит стоимость подготовки военных кадров и, с другой стороны, количество жертв конфликта» [2]. Иначе говоря, когнитивные и социогуманитарные технологии уже на стадии разработок закладываются в стратегию национальной безопасности и решение широкого круга гуманитарных проблем. На одно из направлений решения подобных проблем в правовом поле обратил внимание И. Ю. Сундиев. Предмет юридического осмысления и законотворческой деятельности, по его мнению, — когнитивные и информационные технологии в деятельности экстремистских и террористических организаций. Результаты НБИКС-конвергенции заставили иначе взглянуть на военную стратегию — если возможно изменить смысл ценностных ориентаций и поведение больших социальных групп потенциального противника, то роль вооруженного насилия принципиально меняется. Доминирующими стали «стратегия непрямых действий» и «стратегия безлидерного сопротивления», опирающиеся на сетевые структуры, создаваемые среди населения потенциального противника. Следствием развития этих стратегий стало рождение концепции сетецентрических войн, где террористическая и экстремистская деятельность является разновидностью военных действий, в которых участвуют государства и их правительства, политические партии, силовые министерства и ведомства, транснациональные коммерческие организации через создаваемые сетевые структуры.

К настоящему времени узловой точкой, в которой пересекаются замыслы инициаторов и исполнителей террористических и экстремистских действий, стали «операции базовых эффектов» (Effects-based operations — EBO), определяемые как «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил

---

[2] Converging technologies: for improving human performance nanotechnology, biotechnology, information technology and cognitive science / Edited by Mihail C. Roco and William Sims Bainbridge. Kluwer Academic Publishers, 2003. P. 328.

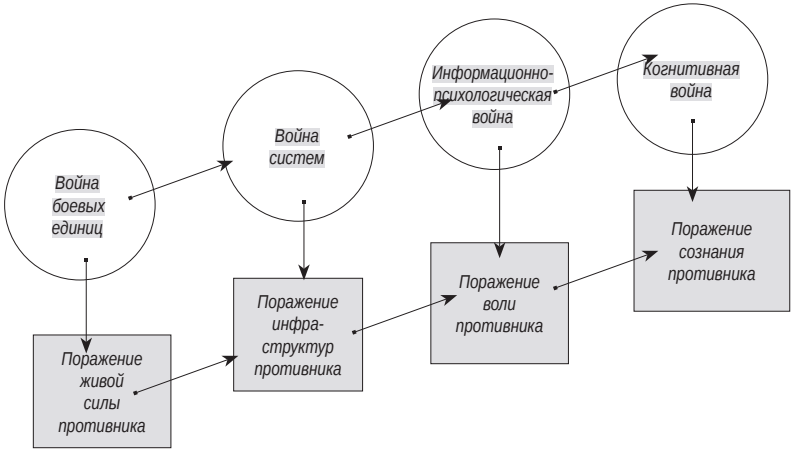


Рис. 28. Когнитивная война в эволюции военных стратегий (В.Э. Багдасарян)

и врагов в ситуации мира, кризиса и войны» [1]. На приведенном ниже рис. 28 представлена эволюция военных стратегий, современный этап которой представлена когнитивными операциями и когнитивной войной.

Вопросы, рассмотренные в данном разделе, носят постановочный характер и требуют дальнейшей разработки.

[1] *Сундиев И. Ю.* Когнитивные технологии: темная сторона прогресса // http://crimpravo.ru/blog/deviantnoe_povedenie/1458.html.

Глава 2. Когнитивно-аксиологическая концепция общественной безопасности

Информационные и гибридные войны, «цветные революции» в различных странах ставят вопрос о противодействии информационно-когнитивным технологиям. Факты говорят о том, что большинство подобных «революций», имевших негативные, а иногда катастрофические последствия, имеют иностранных спонсоров и целенаправленное информационное и организационное воздействие. Анализ таких ситуаций — предмет самостоятельных исследований [2]. Приведем только признанные факты: официальное лицо в американской дипломатии — М. Макфол (бывший посол США в России) подтвердил вмешательство правительства США в целый ряд «цветных революций». Оправдывая администрацию Обамы, он уверял, что, в отличие от предыдущих правительств, Обама уже «не спонсирует цветные революции», что это предшественники Обамы финансировали свержение Моссадыка в Иране в 1953 г., оказали финансовую поддержку «контрас» в Никарагуа, что в сербских событиях «прямые деньги были переданы оппозиции, чтобы дестабилизировать ситуацию, и это сработало» [3]. А Виктория Нуланд обнародовала, что правительство США потратило «на развитие демократии» на Украине 5

---

[2] См. например: *Шульц Э. Э.* Технологии бунта (Технологии управления радикальными формами социального протеста в политическом контексте). — М.: Подольск. ф-ка офсет. печати, 2014. С. 288, 297, 298, 315, 316, 318, 319.

[3] *Дэвид Ремник.* Наблюдая за затмением: Майкл Макфол находился в России, когда там появились перспективы демократии… и когда эти перспективы начали тускнеть The New Yorker. URL: http://www.inopressa.ru/article/05aug2014/newyorker/mcfaul.

млрд долларов [1], и, конечно, эти деньги были потрачены не на печенье, которое раздавала Нуланд на Майдане. Учитывая столь значительные финансовые затраты правительства США на достижение своих целей в суверенных государствах и направленные не на производственные объекты или гуманитарные нужды (что очевидно, т. к. никто нигде и никогда не указал, на какие гуманитарные грузы, на какие жизненно ванные объекты потрачены эти деньги), закономерно, что термин «информационная война» вошел во все языки из английского и является прямым переводом американских документов.

Как понятно из контекста современных геополитических отношений, самая большая угроза не только целостности общественной системе, но и, как показывают события арабской весны, оранжевой революции, рекрутирования в формирования ИГ, угроза человеческим жизням исходит не от военно-технической вооруженности противника. В ходе этих событий противнику не приходится рисковать жизнями своих граждан — граждане стран, подвергшихся информационно-психологическому воздействию, сами сокращают собственное население. В ходе этих событий противнику не приходится нарушать формальные международные обязательства и вторгаться на суверенную территорию — граждане сами разрушают собственные политико-правовые институты и социальный порядок. А после этого противнику нет нужды (как когда-то древним колонизаторам) выкачивать ресурсы из попавших в зависимость стран — пришедшие к власти на волне чужих денег сами вывозят из страны все то, что вообще возможно вывезти и чем можно заинтересовать своего кредитора. Современный вид войн — преэмптивные войны, основной характеристикой которых является невозможность применения международных санкций к государству-агрессору, так как формально оно в этих действиях не участвует. Первым и необходимым этапом таких войн, который и делает их возможным, является создание внутри государства-объекта оппозиционного слоя посредством информационного и психологического воздействия [2].

Надо ли убеждать кого-либо, что в защите от информационного воздействия неэффективны ни ПВО, ни «космический зонтик», ни другие традиционные военно-технические средства? В этом смысле так называемый «железный занавес» выполнял функцию информационной защиты

[1] Нуланд признала, что США вложили в Украину с 1991 года 5 млрд долл. Взгляд. Деловая газета. 2014. 22 апреля / URL: http://vz.ru/news/2014/4/22/683263.html.

[2] *Комлева Н. А.* Преэмптивная война как технология ресурсного передела мира // Пространство и время. 2012. № 2(8). С. 28–33.

общества. Но он же и показал, что создание барьеров на пути циркулирования информации не только не эффективно, но и приводит к пагубным последствиям для экономики, науки и, в целом, для развития страны. К тому же, в современных условиях достижение информационной закрытости общества не представляется возможным, поэтому единственным надежным средством противодействия программирующему воздействию возможного противника является создание психологических барьеров, противостоящих деструктивному воздействию недружественных сторон.

Как кажется, термин «психологическая война» достаточно нов. Но автор книги «Психологическая война» — подробного исследования методов, особенностей и задач психологической войны, П. Лайнбарджер [3] считал, что исход исторических войн, ведущихся традиционным способом, всегда в значительной степени зависел от предварительных или ведущихся в ходе войны психологических воздействий. Другой автор, гораздо более известный в контексте современных событий, — Д. Шарп, детально разработавший технологию смены режимов в суверенных государствах, указывает из 96 методов «ненасильственной смены власти» примерно одну треть символического характера [4]. Надо ли еще убеждать, что безопасность государства, по меньшей мере, в значительной степени зависит от информационно-психологической безопасности, а в современную эпоху информационных технологий и свободной циркуляции информации в сетях от психологической устойчивости контрагента — населения, на которое направлено информационно-психологическое воздействие? Это означает, что наряду с категориями «техническая оснащенность», «технологическая вооруженность», «развитость инфраструктуры» в обсуждении проблем национальной безопасности следует ввести понятия «символическая вооруженность», «символическое оснащение», «развитость символических систем», так же как и проблемное поле, покрываемое этими понятиями. Чтобы общество могло противостоять информационно психологической войне, необходимо, «чтобы собственные символические комплексы были структурированы, институциализированы и, в известном смысле, агрессивны. Только тогда данный социум сможет и сохранить себя, и увеличить собственные “жизненные шансы”» [5].

---

[3] *Лайнбарджер П.* Психологическая война. М.: Воениздат-Язык: Русский Формат, 1962. 352 с.

[4] *Шарп Д.* От диктатуры к демократии. Концептуальные основы освобождения. Институт им. Альберта Эйнштейна. США // URL: www.aeinstein.org.

[5] *Кармадонов О. А.* Социологическая рациональность отсутствия в исследовании современного мира // Социс. 2008. № 3(287). С. 3.

В силу того, что мероприятия, проводимые в ходе информационно-психологической войны, направлены не только на индивида, а на социум и общественные группы, его составляющие, строить концепцию информационно-психологической защиты населения (государства) нужно, исходя из теории социокультурной системы, включая теорию социальной и культурной психологии. Прежде всего, стоит остановиться на специфике переживаемого в познавательной сфере момента. Если говорить о культурологии как о дисциплине, исследующей специфически человеческую форму бытия, то в настоящее время определяющим методологию исследования культурных феноменов подходом является культуроцентристский подход. Смысл его заключается в том, что координирующим и целеполагающим началом человеческой деятельности (как праксеологической, конструктивной, так и когнитивной) является система символов. Это означает, что именно символическая деятельность определяет специфику экономической, политической и др. сфер человеческого бытия. И именно система символов содержит в себе основные цели, ориентиры и мотивацию деятельности, из чего вытекает системоформирующий характер символической сферы. В соответствии с такой концепцией человеческой деятельности не столько наличие материальных и технологических средств взаимодействия с действительностью определяет нашу безопасность в самом широком смысле этого слова (а также и в самом конкретном), сколько идеи, которыми руководствуются те, кто эти материальные средства контролирует и использует.

Современный период научного познания характеризуется еще и тем, что имеет смысл обозначить как культуроцентристский поворот. Смысл его заключается в том, что, во-первых, в научном сообществе произошло осознание того факта, что само по себе естествознание, каких бы впечатляющих результатов в облегчении человеческого существования оно ни достигло, не может обеспечить безопасность и гарантированную жизнеспособность человеческого рода. Как прозорливо писал А. Печчеи, основатель Римского клуба, «проблема пределов человеческому росту и человеческому развитию является, по сути своей, проблемой, главным образом, культурной» [1]. Во-вторых, в научном сообществе в процессе конституирования социального знания надежды на решение острых (иногда имевших финальный характер) социальных проблем возлагались на разные социальные дисциплины. Сначала казалось, что становление экономики как рационального знания разрешит все социальные

[1] *Печчеи А.* Человеческие качества. М.: Прогресс, 1980. С. 129.

конфликты. Потом наступил черед социологии — ее основателям казалось, что построение рационально обоснованных социальных институтов доставит человечеству такое долгожданное спокойствие. Затем решили, что теория политики — ключ к человеческому счастью (кстати, О. Конт — один из основателей социологии назвал свой основополагающий труд «Система позитивной политики»). Но оказалось, что ни экономическая наука, ни социология, ни политология не могут (во всяком случае, в современном виде — как знание, ограниченное дисциплинарными рамками) вскрыть закономерности человеческого бытия, т. к. предметом своего исследования имеют лишь частный его аспект. И этот (тот или иной) аспект не может быть ни познан вне взаимосвязи с другими сторонами человеческого бытия, ни, тем более, управляем без адекватного воздействия на систему.

К концу XX в. пришло понимание, что наиболее общей наукой, обнимающей все сферы человеческого бытия, является культурология, т. к. именно культура в ее целостности детерминирует отдельные виды человеческой деятельности (материальное производство, социальные институты, властные отношения, художественную деятельность), но культура не сводится ни к духовности, ни к традициям и обычаям. Первыми заговорили о том, что «культура имеет значение» (как с некоторым изумлением названа книга известного исследователя современных глобальных процессов [2]), американские социологи. Т. Парсонс, один из создателей современной теоретической социологии, в своей книге «Социальная система» (1951) [3] показал, что не существует абстрактных, универсальных социальных систем и социальных законов, что культура — это та переменная, которая определяет функционирование целого. В то же время П. А. Сорокин пошел еще дальше и в своем труде «Социальная и культурная динамика» [4] показал, что все как раз наоборот: не социальная система выступает в качестве целостности при культурной переменной, а культура включает в себя зависимые структуры — политику, право,

---

[2] Культура имеет значение. Каким образом ценности способствуют общественному прогрессу / Под ред. Л. Харрисона и С. Хантингтона (Lawrence Harrison, Samuel Huntington (eds.) Culture Matters: How Values Shape Human Progress. New York, 2000). М.: МШПИ, 2002. 320 с.

[3] *Парсонс Т.* О социальных системах / Под ред. В. Ф. Чесноковой и С. А. Беленького. М.: Академический проект, 2002. 832 с.

[4] *Сорокин П. А.* Социальная и культурная динамика: исследования изменений в больших системах искусства, истины, этики, права и общественных отношений / Пер. с англ., комментарии и статьи В. В. Сапова. СПб.: РХГИ, 2000. 1056 с.

социальные институты, религию и т. д. Таким образом, строить любую концепцию социального проектирования, ограничиваясь инструментальным подходом, по меньшей мере неэффективно. По большому счету вообще безграмотно.

Итак, выделим важные для нашего рассуждения свойства социетальных систем. Т. Парсонс предложил этот термин — социетальные системы, для того, чтобы избежать терминологической путаницы и отделить понятие, обозначающее реально существующий социокультурный объект, вместе с носителями культурных ценностей, от социальной структуры (также представляющей собой систему, являющейся предметом специальных исследований), которая является элементом социетальной системы. Прежде всего, современная научная позиция заключается в том, что интегрирующим стержнем социетальной системы является система ценностей, от нее зависят вариативные элементы системы (экономика, политика, право и т. д.), и они инвариантны по отношению к системе ценностей. Система ценностей является не только стержнем социетальной системы, но ее скрепами, от которых зависят ее целостность, бытие во времени, а также способность преодолевать кризисные ситуации.

Хорошо известно, что именно ценностно-символическая мотивация обеспечила советскому обществу способность противостоять военной и технологической мощи Германии во время Великой Отечественной войны. Поэтому первым элементом концепции системы безопасности в целом и информационно-психологической безопасности в частности является наличие *ценностных императивов*, не подвергаемых сомнению и признаваемых всеми членами общества. Не случайно поэтому упоминаемый выше Д. Шарп советовал начинать свержение правительств с замещения символов. Эти советы не только хорошо себя зарекомендовали в ходе «цветных революций», но и получили эмпирическое подтверждение в глобальных исследованиях. В знаменитом исследовании глобализационных процессов под руководством С. Хантингтона «Многоликая глобализация» многими исследователями фиксируется факт: признаком распада идентичности является проникновение чуждой идеологии и чуждых культов [1]. А. О. Кармадонов, предложивший понятия «символической оснащенности», по этому поводу пишет: «Социум, как и человек, потерявший память, больше не уверенный в том, кто он есть, понятия не имеющий — для чего и для кого он существует, по определению не является субъектом

[1] Многоликая глобализация / Под ред. П. Бергера и С. Хантингтона; пер. с англ. В. В. Сапова. М.: Аспект-пресс, 2004. 379 с.

самостоятельных и ответственных решений… Символическая система общества во всех институциональных горизонтах — альфа и омега социального организма, первый и последний бастион текущих и грядущих культурных сражений в глобализирующемся мире» [2].

Система ценностей, выраженная в символической форме, в том случае эффективно противостоит альтернативной системе ценностей, если не имеет ценностных лакун — отсутствие ценностных императивов, дающих ответы на запросы социальной системы. Запросы различных частей социума могут не иметь витального значения для системы в целом. Наибольшую опасность представляют те ценностные лакуны, которые не дают ответа на социальный запрос, возникший в связи с цивилизационным вызовом. Понятие цивилизационного вызова, предложенное А. Тойнби, уже давно успешно применяется не только в различных отраслях социогуманитарного знания, но и в политическом дискурсе. В концепции «Вызов-Ответ» содержится важный вывод о том, что вызов — проблема, стоящая перед социальной системой и не получившая адекватного ответа (в виде новой руководящей идеи, технологии, социального института), разрушает и приводит к гибели социальную систему. Тойнби указывал на то, что формулирует вызов (разрабатывает пути выхода из кризиса, вырабатывает адекватные новым условиям ценности) именно творческая элита. В его концепции социальной массе отводится пассивное место. Мы добавим, что в случае, когда элита не в состоянии дать адекватный ответ вызову (по причине неспособности) или элита блокирует возможные ответы (по причине несоответствия этих ответов качествам и императивам действующей элиты), социальные группы рекрутируют извне ценности и символы, выражающие эти ценности. Видимая адекватность альтернативных ценностей может оказаться иллюзией, т. к. они должны быть комплиментарны доминирующей системе ценностей и существующим социальным институтам. Поэтому инфицирование чужеродными ценностями чаще приводит к разрушению системы.

В целом концепция «Вызов-Ответ» представляется достаточно гармоничной, но то, что Тойнби отводит культуротворческую роль только элите, вызывает возражение: в современном социогуманитарном знании уже стала общим местом идея, пришедшая из естествознания, — концепция самоорганизации. Не будем здесь излагать основы теории хаоса — они достаточно освещены в науке и применительно к социогуманитарному

---

[2] *Кармадонов О. А.* Социологическая рациональность отсутствия в исследовании современного мира // Социс. 2008. № 3(287). С. 11.

знанию в частности [1]. Укажем только на то, что фундаментальным положением современной теории систем является принцип самоорганизации. Применительно к рассматриваемой проблеме это означает, что в случае отсутствия адекватного ответа, исходящего от элиты, социум в процессе самоорганизации (поиска выхода из кризиса) рекрутирует недостающие в данной символической системе ценности из альтернативных ценностных систем.

В контексте теории социальной самоорганизации обозначим два важных момента. Во-первых, альтернативные ценности диффундируют в области, где существуют ценностные лакуны — социальные проблемы, которые не получают ценностного ответа (или даже ценностный вакуум, в случае кардинального несоответствия ценностей изменившимся задачам). Во-вторых, на функционирование социальной системы имеет место влияние не только актуальных сущностей — реально существующих институтов, структур и механизмов, но и отсутствие таковых. Отсутствие необходимой сущности (организационной, инструментальной, целеполагающей и т. д.) затормаживает развитие социальной системы или даже разрушает ее. Но дело не только в этом. Это означает, что отсутствующие феномены, как материальные, так и институциональные и идеациональные, оказывают влияние на функционирование социального организма. Именно этим объясняется, например, разрушающее влияние «железного занавеса». Ценности, которые играли созидательную роль в становлении индустриального общества, в нашу общественную систему допущены не были. Предполагалось (не без оснований), что они будут играть разрушающую роль в данной социетальной системе. Но эффект отсутствия сыграл свою деструктивную роль: во-первых, они диффундировали в ценностные лакуны; а во-вторых, в силу того, что не было выработано собственных ценностных императивов, востребованных технологическим вызовом эпохи, не только темпы, но и траектория развития нашей системы изменились. Точно так же, в социологической и политологической литературе уже давно пришли к заключению о том, что само существование советской альтернативы — как несуществующее в западной социальной системе, повлияло на либеральное общество, заставив эволюционировать в сторону увеличения доли социально ориентированных программ.

---

[1] *Василькова В. В.* Порядок и хаос в развитии социальных систем (синергетика и теория социальной самоорганизации). СПб.: Лань, 1999. 478 с.; *Плебанек О.* В. Парадигмальные основания анализа социальной реальности. СПб.: Петрополис, 2012. 352 с.; Человек перед лицом неопределенности / Ред. И. Р. Пригожин. Москва–Ижевск: Институт компьютерных исследований, 2003. 304 с.

Несуществующее — это не несуществующее вообще, а недостающее здесь и сейчас. И оно (недостающее здесь и сейчас) подчас важнее, чем актуально существующее. Так оказалось, что актуально существующее социальное равенство (относительное, как отсутствие большой социальной дистанции между социальными группами) не заменило собой отсутствующей интеллектуальной и информационной свободы в советской общественной системе. Признание факта, что своим отсутствием несуществующее влияет на социум, А. О. Кармадонов назвал *абсентеистской рациональностью* [2]. Полагаем, что в конструировании символического комплекса следует учитывать как наличие социально значимой сущности, так и ее отсутствие. На практике это означает, что, например, в рассуждениях о корнях, о традициях, о национальной идее стоит иметь в виду не только укорененные ценностные императивы, но и отсутствующие, но необходимые в силу стоящих перед общественной системой вызовов.

Принципы самоорганизации сложных систем, во-первых, отрицают жизнеспособность гомогенных образований больших масштабов и предполагают наличие локальных организационных структур, а во-вторых, предполагают производство структур, институтов и ценностей, гетерогенного по отношению к доминирующей культуре характера. Гетерогенность обеспечивает жизнеспособность системы, гарантируя наличие структур и элементов, взаимодействующих со средой, всегда имеющей полиструктурный, динамичный, комплексный характер. Поэтому любая культура в своем составе имеет субкультуры, и любая большая социокультурная система предполагает известную степень вариативности, тем большую, чем масштабнее социум она объединяет. В силу названных особенностей сложных, самоорганизованных систем, социетальная система не может иметь жестко организованный и гомогенный символический комплекс. Условием нормального развития социокультурной системы и эффективного функционирования является биполярность или даже культурная полицентричность при интегративном ценностно-символическом стержне. При этом резистентность социетальной системы и по отношению к вызовам среды, и по отношению к деструктивным инъекциям чуждых ценностей достигается гетерогенностью культуры, которая обеспечивает наличие в запасе варианты ответов, а также отсутствие ценностных лакун.

Роль метанарратива в исторических общественных системах играла религия, консолидируя социум вокруг дальнесрочных,

---

[2] *Кармадонов О. А.* Социологическая рациональность отсутствия в исследовании современного мира // Социс. 2008. № 3(287).

не обнаруживаемых рациональным способом, целей. Причем чем большего масштаба социум объединял метанарратив, тем более он отрывался от традиционных ценностей. И если для родовых общественных систем достаточной была консолидирующая идея в форме веры в первопредка, для локальных социумов, выходящих за пределы кровного родства, требовались уже институциализированные религиозные системы, то социумы, имеющие надэтнический характер, для своей интеграции и консолидации потребовали и сформировали надэтнические мировые религии. В современную эпоху, а главное, для России, не только полиэтнической, но и поликонфессиональной, религия не может выполнять роль метанарратива. Такую функцию в «расколотой» (С. Хантингтон) цивилизации может выполнить идеология.

Идеология, как бы ее ни понимать: хоть в значении, предложенном авторами этого понятия — А. де Трасси и Э. де Кондильяком, как учение об идеях, первоосновах морали, политики и права; хоть в значении современных авторов — например, Р. Барта, как метаязыковую коннотативную систему, социализирующую действительность, способна перекинуть мост и через религиозные границы. Что, в общем-то, демонстрировала советская идеология, объединившая целый ряд разнородных обществ. Слабым местом советской идеологии было несоблюдение предыдущего условия — необходимость учитывать абсентеистский фактор. Идеология, хоть в значении теории (Кондильяк), хоть в значении мифа (Барт), включает в себя теоретически осмысленные верования (представления) о целях и идеалах социального бытия. Как пишет Решетников: «Иногда ее <идеологию> определяют как гражданскую религию, или религию гражданственности. Отбор и презентация национальных мифологем, скрепляющих цивилизационное единство, …является необходимой частью работы по осмыслению идеологии консолидации. По крайней мере, ни один народ не смог обойтись без воодушевляющих мифов» [1].

Тем не менее, идеология представляет собой рациональный уровень восприятия действительности (хотя и включает в себя верования), и поэтому является необходимым, но недостаточным элементом системы противодействия информационному противнику. Национальная идея представляет собой эмоционально мотивационный механизм программирования социальной деятельности на иррациональном уровне.

[1] *Решетников В. А.* Основания становления идеологии консолидации России // Идеология консолидация России: возможность и действительность. Иркутск, Иркутск. гос. ун-т, 2006. С. 53.

Национальная идея на символическом уровне имеет идеологемную экспликацию. Идеологема как когнитивная единица идеологии в силу своей лаконичности и упрощенности быстрее достигает сознания адресата и ориентирована на самый широкий адресный круг, независимо от возраста, уровня образования, этнической и религиозной принадлежности индивидуума. Поэтому система символического оснащения социальной системы должна строиться на уровневом принципе — на теоретическом уровне как рационально обоснованная идеология и на эмоционально-подсознательном уровне как система идеологем. Система символического оснащения общества для выполнения функции информационно-психологической защиты и функции социального конструирования должна включать следующие типы идеологем [2]: идеологемы-понятия, идеологемы-фреймы, идеологемы-гештальты, отражающие идеологию государства, как положительного (Родина, гуманизм), так и отрицательного аксиологического модуса (терроризм, геноцид). Конструктивно-регулятивная деятельность по обеспечению национальной безопасности должна быть направлена:

— на вытеснение из СМИ (и из системы образования) идеологем со смешанным аксиологическим модусом (воля, личность, конкуренция);
— на нейтрализацию идеологем ограниченного употребления, конституирующих деструктивную идеологию (чеченский борец за независимость, советский оккупант);
— на формирование цепочек идеологем-историзмов, конституирующих осознание цивилизационной преемственности (русская идея, светлое будущее, геополитическое равновесие).

Итак, концепция информационно-психологической безопасности, которую мы называем когнитивно-аксиологической, т. к. сущностью ее является формирование не только информационного поля социума, формирующего отношение к действительности, но особенностей мышления и восприятия действительности, блокирующих попытки инфицирования деструктивными ценностями. Представленная концепция в основе имеет изложенные выше закономерности, которые формулируются в следующих принципах:

— принцип символической вооруженности, который заключается в том, что безопасность общественной системы и способность

[2] О типологии идеологем см.: *Малышева Е. Г.* Идеологема как лингвокогнитивный феномен: определение и классификация // Политическая лингвистика. 2009. Вып. 30. С. 32–40.

противостоять деструктивным влияниям обеспечивается наличием системой символического оснащения — ценностных императивов, идеалов, целей;

— принцип абсентеистской рациональности, который заключается в том, что символическая вооруженность общества обеспечивается не только ценностями, релевантными актуальным структурам, но и влияющим на социальное бытие своим отсутствием;

— принцип метанарратива, который заключается в том, что символическая система, обслуживающая суперсложный социум, каким является российский (и не только), должна носить надэтнический, надрелигиозный, но при этом консолидирующий и интегрирующий характер.

В связи с таким видением социальной реальности нам не хочется употреблять узкое понятие информационно-психологической безопасности, так как принципиальная позиция культуроцентристского подхода заключается в том, что никакая безопасность — экономическая, экологическая и т. д. невозможна вне символического капитала, и поэтому предлагается употреблять категорию, вынесенную в заголовок статьи, — общественная безопасность.

Глава 3. Массмедиа в системе информационно-психологической безопасности

Во второй половине XX и в первые два десятилетия XXI в. изменились подходы к национальной и международной безопасности. На сайте Совета безопасности Российской Федерации указано, что в России разработаны шесть доктрин в области национальной безопасности (в том числе морская и военная), четыре концепции и восемь стратегий. Сложность и противоречивость самого феномена безопасности, особенно ярко проявившиеся в современных условиях, вызвали к жизни многочисленные дискуссии о подходах к определению безопасности, ее уровней и видов.

Информационная безопасность в условиях глобализации. Сегодня принято выделять международную глобальную безопасность, международную региональную безопасность и национальную (государственную и страновую). Последняя, в свою очередь, подразделяется на национальную, национально-государственную, федеральную (в условиях федерального устройства), общественную и индивидуальную [1]. Понятие «национальная безопасность» в емкой формуле предложено петербургским ученым И. Ф. Кефели: «это состояние государства, при котором сохраняется его целостность и возможность быть самостоятельным субъектом системы международных отношений» [2]. По определению

[1] *Сергунин А. А.* Национальная и международная безопасность: новые подходы и концепты // Проблемы безопасности и военно-силовой политики в международных отношениях. СПб.: Изд-во СПбГУ, 2007. С. 300.

[2] *Кефели И.* Ф. Судьба России в глобальной геополитике. СПб.: Северная звезда, 2004. С. 131.

исследователя А. А. Сергунина, «Национальная безопасность — это состояние, при котором в государстве защищены национальные интересы страны в широком их понимании, включающем политические, социальные, экономические, военные, экологические аспекты, риски, связанные с внешнеэкономической деятельностью, распространением оружия массового поражения, а также предотвращением угрозы духовным и интеллектуальным ценностям народа» [1]. Этому широкому взгляду на безопасность соответствует и многосторонний подход к установлению различных видов безопасности: политической, экономической, технологической, военной, экологической, социальной, правовой, культурной, интеллектуальной, демографической, генетической, психологической.

Как отмечалось в предыдущих разделах книги, на глобальном, региональном и национальном уровнях сегодня большое место занимают проблемы обеспечения информационной безопасности. Не менее значимым представляется и определение информационной сферы, под которой в данной Доктрине понимается «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений» [2].

Современное развитие глобальных сетей создает возможности для слияния вещания, телекоммуникаций и информационно-компьютерной технологии. Неминуемо актуализируются проблемы правового регулирования этого процесса в условиях конвергенции, когда информационный обмен приобретает «трансграничный» характер. Аудитория превращается в активного преобразователя, создателя и распространителя информации [3].

Усиление внимания к информационной безопасности объясняется многими причинами. Так, информация является неотъемлемой частью процессов управления, в том числе социального и политического управления. Эффективное функционирование любой системы зависит от характера

[1] *Сергунин А. А.* Указ. соч. С. 301.

[2] Доктрина информационной безопасности Российской Федерации. URL: https://www.rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

[3] *Быкова А. С.* Массмедиа стран — членов Европейского Союза: политико-правовые вопросы регулирования содержания информации. СПб.: Роза мира, 2004. С. 43.

процессов информационных потоков. В частности, это относится к системе международных отношений. «В эпоху глобализации мы можем говорить о глобальной конфигурации сил, которые должны соответствовать глобальным культурным кодам и специальной модели управления» [4]. В современных военно-политических конфликтах ведущие мировые державы активно используют Интернет [5], «трансформируя и модифицируя с его помощью функциональные возможности органов военного управления, делая их более гибкими» [6]. Кроме того, концепция «войн шестого поколения» предполагает «использование всех преимуществ информационных и компьютерных технологий для проведения боевых операций совершенно нового — сетецентрического типа» [7]. Перспективы изменений в конфигурации мирового пространства — однополярного или многополярного — вызывают острые дискуссии. Некоторые ученые и политики связывают будущее нашей планеты с деятельностью «мирового правительства», другие — с созданием «глобальной империи», третьи — с формированием «глобального управления». От реализации этих моделей зависит, каким будет наш мир в будущем. В частности, в контексте глобальных процессов второй половины прошлого столетия было аксиомой, что в основе системного противостояния лежат, прежде всего, идеологические императивы, наиболее мощные и конфликтогенные, и их устранение приведет одновременно к устранению первопричины ожесточенного соперничества, существующего на грани глобального военного конфликта. Эта идеологема была положена в основу многих доктрин, в том числе и военных, и активно поддерживалась не только советскими, но и западными акторами мировой политики. В общественное сознание

---

[4] *Немчук А. А.* Глобальное управление в современном мире: политологический анализ: автореф. канд. дисс. М., 2004 // Научная библиотека диссертаций и авторефератов disserCat. URL: http://www.dissercat.com/content/globalnoe-upravlenie-v-sovremennom-mire-politologicheskii-analiz#ixzz4AJdterbz.

[5] *Остапенко В. С.* Государственная политика в области обеспечения информационной безопасности органов исполнительной власти. М., 2009; *Соловьева Е. А.* Информационное противоборство в сети Интернет: автореф. дисс. …канд. полит. наук. М., 2011; *Зиновьева Е. С.* Глобальное управление Интернетом: Российский подход и международная практика // Вестник Моск. гос. ин-та международных отношений — Университета. 2015. № 4(43). С. 111–117.

[6] *Мельник Г. С., Никонов С. Б.* Медийный компонент в доктрине информационной безопасности // Управленческое консультирование. 2014. № 1. С. 20.

[7] *Райский Д. А.* Национальная безопасность России в контексте сетецентрических войн в условиях меняющейся мировой архитектуры: автореф. канд. дисс. …канд. полит. наук. СПб., 2016. С. 23.

была внедрена идея того, что корреляция ценностей социалистических и западно-либеральных носит контрарный характер и является чуть ли не единственной причиной враждебности. С устранением этого яблока раздора наступит, мол, всеобщее благоденствие. В связи с этим стоит рассмотреть некоторые аспекты противостояния советской и западной политической машинерии.

В СССР был разработан и в целом небезуспешно функционировал механизм пропаганды социалистических ценностей, а также контрпропаганды, охватывающий практически все сферы жизни общества. Несмотря на громоздкость аппарата, порой доходящие до абсурда организационные решения, неадекватность кадровой политики, советской системе удавалось противостоять натиску западной идеологии. После Второй мировой войны институт пропаганды, прежде всего США, стал менять вектор воздействия: поскольку сопротивление нацистской Германии и ее сателлитов было сломлено, основным глобальным противником стал СССР, позже представленный как «империя зла». Американская внешняя пропаганда стала обретать более системный характер и четкую структурную организацию. Важнейшим ее компонентом и орудием практического воздействия стала психологическая война, способы ведения которой отрабатывались еще на заре XX столетия. Примечательно, что она практически сразу же была соотнесена с областью сугубо милитаристской, рассматривалась как орудие духовного разложения, уничтожения и захвата противника.

Подытожив опыт применения психологического оружия в первые десятилетия минувшего века, крупный американский теоретик и практик Н. Коупленд не просто разрабатывал технологии эффективного использования методик психологической войны, но, что особенно важно, касался духовной стороны этого явления. Он утверждал: «Нелегко найти удовлетворительное определение такому не поддающемуся исчислению качеству, как моральное состояние, однако нас поймут, если мы определим его как духовное состояние. Моральное состояние — более широкое понятие, чем физическое или умственное. Его нельзя заключить в узкие рамки нравственности. Действительно, это что-то выходящее за пределы всех этих понятий вместе взятых, и в то же время исходящее на них. Называя моральное состояние духовным, мы не собираемся относить его к прерогативам людей набожных или спиритуалистов. Это определение мы используем в философском, а не в теологическом смысле, и тот, кому оно не нравится, может называть его психологическим состоянием,

хотя это определение будет менее удовлетворительным» [1]. Здесь нельзя не обратить внимание на то, что предметом психологической войны становится «моральное состояние», которое «нельзя заключить в узкие рамки нравственности». Законы войны, даже психологической, как известно, всегда игнорируют нравственные максимы, будь то советский период первых послевоенных десятилетий или конец правления президента Обамы, ознаменованный лихорадочным введением новых санкций, разрушающих отношения между Россией и США. Это был период, когда стал реальностью факт публикации французским еженедельником Charlie Hebdo кощунственной «сатиры» на крушение российского самолета с многочисленными жертвами в декабре 2016 г. Эта идеологическая акция, преступная в отношении общегуманитарных принципов, оказалась результативной в плане ведения психологической войны, независимо от того, отдавали себе отчет в содеянном «сатирики» из редакции еженедельника или глумились над безвинно убиенными просто ради удовлетворения собственной прихоти. Как бы то ни было, авторы публикации не просто шокировали нормальных людей, но и дали понять, что самое святое, а именно память о человеческих жертвах, может стать объектом издевательства и пошлых насмешек, если это отвечает достижению поставленных целей. Они показали всему миру: можно поступать и так, как они поступили, заходить за черту, за которой начинается пространство сатаны.

Случай с Charlie Hebdo, конечно, не просто предельно циничен, но даже иррационален в своей вызывающей непостижимости. Однако и солидные массмедиа, становясь элементом психологической войны, грешат против истины и лукавят. Политолог и профессор права Монро Э. Прайс уличает даже «Голос Америки» в предвзятости: «В момент обострения угрозы национальной безопасности страны те качества, которые "Голос Америки" считал основными для своей репутации, оказались эфемерными, которыми легко пожертвовали в это волнительное время» [2].

Но теория ведения психологической войны выглядит вполне корректно. Ее основы представил в книге «Психологическая война» упомянутый выше Пол Лайнбарджер, который имел значительный опыт проведения специальных операций. Он настоятельно подчеркивал, что эффект можно

---

[1] *Коупленд Н.* Психология и солдат / Пер. с англ. А. Т. Сапронова, В. М. Катеринича. 2-е изд. М.: Воениздат, 1991. С. 22.

[2] *Прайс Монро Э.* Масс-медиа и государственный суверенитет: Глобальная информационная революция и ее вызов власти государства / Пер. с англ. Я. Скляровой. М.: Ин-т проблем информ. права, 2004. С. 250.

достичь исключительно на научной основе: «Пропаганда может стать действительным оружием психологической войны, научной по духу и превращенной в искусство, если будут четко сформулированы ее посылки, определены задачи, приведены в постоянную готовность ее средства, а проведение пропагандистских операций будет хотя бы частично контролироваться на основе научных методов. Из наук психология стоит всех ближе к пропаганде, хотя антропология, социология, политическая наука, экономика, география и другие науки также в какой-то мере имеют к ней отношение. Но именно психология определяет необходимость обращения к другим наукам» [1]. Любая война, даже если она психологическая, — дело чрезвычайно затратное. США и их союзниками была создана впечатляющая по масштабам воздействия и техническому оснащению служба, которая была призвана вести подрывную работу прежде всего против СССР и стран, входящих в организацию Варшавского договора. С целью разрушения советской системы был введен в действие комплекс ведения психологической войны по многим направлениям, в том числе и связанным с вооруженными силами. Совершенствовались технологии специальной пропаганды, которая включается в действие как инструмент психологической войны в боевых условиях: «В уставном документе американской армии, наставлении М 33–5, говорится, что психологическая война "есть планомерное ведение пропаганды, главная цель которой заключается в том, чтобы влиять на взгляды, настроения, ориентацию войск и населения противника, населения нейтральных и союзных стран, с тем чтобы содействовать осуществлению государственных целей и задач"» [2].Если технологии специальной пропаганды среди войск и населения противника полномасштабно применяются в условиях крупного вооруженного конфликта — даже в условиях локальных боестолкновений их применение затруднено, — то совершенно особое место в системе психологической войны заняли «мирные» средства, а именно массмедиа. Они самым активным образом включились в процесс идеологической обработки собственного населения и населения потенциального противника. Следует подчеркнуть, это была не бессистемная и спорадическая деятельность разрозненных печатных изданий и аудиовизуальных каналов, а деятельность хорошо спланированных и организованных медийных структур, фактически встроенных в общий комплекс психологической войны. Недружественное,

---

[1] *Лайнбарджер П.* Функции психологической войны. URL.: http://psyfactor.org/psywar2.htm.

[2] *Белов А. В., Шилкин А. Д.* Диверсия без динамита. М.: Политиздат, 1972. С. 7–8.

по сути своей экспансионистское и реально угрожающее социалистическому сообществу поведение США и их союзников отнюдь не маскировалось, а демонстрировалось со всё возрастающим напором. Оно обрело статус национального политико-социального учения и было официально оформлено: «При разработке доктрины психологической войны в США значительное внимание уделялось также и чисто практическим мероприятиям. На протяжении всех послевоенных лет непрерывно совершенствовался аппарат психологической войны — правительственные, полуправительственные, военные и так называемые "частные" органы, занимавшиеся не только внешней пропагандой, но и диверсионно-разведывательной деятельностью, — непрестанно усовершенствовалось и расширялось использование современных средств массовой информации и пропаганды, и в первую очередь радио» [3]. Конечно, нет оснований утверждать, что Советский Союз перестал существовать именно вследствие воздействия на него комплекса психологической войны со стороны США. Но вклад субъектов её ведения в развал советской системы был огромен. В то же время надо учитывать, что данный мощный пропагандистский комплекс действовал не только против Советского Союза и стран, входящих в организацию Варшавского договора, но навязывал выгодную США идеологию странам практически всего мира, и «особое значение приобретает вопрос об информационной экспансии и информационном неоколониализме, становящихся новыми формами империалистической эксплуатации развивающихся стран» [4].

К началу перестройки в СССР был уже запущен механизм ревизии марксистско-ленинского учения, отказа от незыблемых, казалось бы, догм партийно-советского строительства. Плюрализм мнений стал реальностью. Звучали голоса в пользу разрядки напряженности, сотрудничества и проявления доброй воли. Советские идеологи порой обращались к западным партнерам с предложениями о сотрудничестве, стремились призвать их к ответственности. Вот одно из подобных обращений: «Западные политики должны, наконец, внять голосу разума и изъять из сферы идеологической борьбы такие приемы пропаганды, как извращенная информация, замалчивание фактов, клевета, разжигание ненависти и недоверия, подрывные методы психологической войны» [5].

---

[3] *Панфилов А.* Ф. За кулисами «Радио Свобода». М.: Междунар. отношения, 1974. С. 16–17.

[4] *Федякин И. А.* Общественное сознание и массовая коммуникация в буржуазном обществе. — М.: Наука, 1988. С. 189.

[5] *Кондратенко В. М.* Под маской объективности («Нью-Йорк таймс»: американская информационно-пропагандистская машина). М., 1986. С. 233.

Приходится констатировать, что взаимной интеграции, основанной на доверии и доброжелательном отношении, между Россией и западными государствами так и не произошло. Пользуясь временной слабостью России, страны Запада максимально близко придвинули к ее границам базы НАТО, спровоцировали государственный переворот на Украине, ввели санкции. Отсутствие серьезных идеологических противоречий не устранило цивилизационных причин глобального противостояния России и Запада, прежде всего США. Это вызвало разочарование и сожаление даже у М. С. Горбачева, главного «архитектора» перестройки. По его мнению, «Россия была миром миров, своеобразным сплавом культур и народов, а не какой-то империей, наподобие Великобритании» [1]. Что касается Великобритании, то с ней отношения фатально не складывались, и их суть отражает краткая реплика одного из героев, приведенная в книге воспоминаний советского журналиста о Великой Отечественной войне: «– Что же англичане? — Как всегда, ведут двойную игру. В лондонских газетах открыто выступают с защитой Гесса. Он якобы военнопленный и суду не подлежит. Подумайте, палач в роли невинного агнца» [2].

В настоящее время уже очевидно, что Запад сохраняет не просто негативное, но во многом и враждебное отношение к России как к стране. Достаточно вспомнить упоение, с каким Обама говорил о том, что «санкции разорвали российскую экономику в клочья», Меркель, снова и снова призывающую к введению санкций против России и поддерживающую режим на Украине, где, по выражению Б. Ф. Славина, правят теперь олигархи с «профашистскими лицами». Политолог с полным на то основанием заявляет: «После заживо сожженных одесситов в Доме профсоюзов, я уверен, уже нельзя говорить в ироническом ключе о наличии фашизма на Украине. К сожалению, до сих пор это не хотят понять ни на Западе, ни в наших российских либеральных и оппозиционных СМИ» [3]. Вопрос об ответственности политиков за многие трагедии на Украине остается без ответа.

Истинная подоплека противостояния России и Запада оказалась намного сложнее, чем представлялось раньше: идеологическая составляющая оказалась, пожалуй, не самой главной. В какой-то мере

---

[1] Неоконченная история. Беседы Михаила Горбачева с политологом Борисом Славиным / Автор-сост. Б. Славин. М.: ОЛМА-пресс, 2001. С. 49.

[2] *Кованов П. В.* И слово — оружие. Изд. 2-е, доп. М.: Советская Россия, 1978. С. 44.

[3] *Славин Б. Ф.* «Если в России произошел крах двух прежних идеологий (советской, а затем либеральной), то где гарантии, что это же не случится с нынешней консервативной идеологией?» URL: http://www.gorby.ru/userfiles/06_slavin__red.pdf.

прояснить ситуацию, может быть, позволит высказывание А. А. Зиновьева: «Финансовый тоталитаризм подчинил себе политическую власть. Холодному финансовому тоталитаризму чужды эмоции и чувство жалости. По сравнению с финансовой диктатурой, диктатуру политическую можно считать вполне человечной. Внутри самых жестоких диктатур было возможно хоть какое-то сопротивление. Против банков восставать невозможно» [4]. Финансовая диктатура охватывает все слои общества, порождает глобализационные процессы, подчиняет «свободную» прессу и провоцирует противоречия в сфере коммуницирования, обусловливает жесточайшую конкуренцию с претензией на лидерство.

Во второй половине XX в. отчетливо проявилась обеспокоенность международного сообщества в связи с дисбалансом в области информации и коммуникации. Сохраняет свою важность проблема международно-правового регулирования информационных потоков, которые рассматриваются в качестве инструментов социального контроля и используются теми, у кого есть власть и кто использует силу информации, чтобы сохранить или завоевать лидирующие позиции на мировой арене [5]. Противостояние между сторонниками нового международного информационного и коммуникационного порядка и приверженцев свободного потока информации показало наличие серьезных противоречий в сфере информации и коммуникации как между различными регионами мира, так и между различными субъектами международных отношений. Позже не оправдали надежды прогнозы о том, что вступление в электронную эру способно привести к забвению идей порядка и контроля в сфере информации и коммуникации.

На сегодняшний день не утратил своей актуальности вопрос о том, кто будет доминировать в области информации и коммуникации. Существует серьезная озабоченность тем, что контроль над глобальной телекоммуникационной инфраструктурой (как технически, так и содержательно) будет по-прежнему являться прерогативой частных транснациональных коммерческих структур, принадлежащих к финансовой элите мира,

---

[4] *Лупан В.* Александр Зиновьев: Запад против России. Взгляд философа (Берлинское интервью, опубликованное французской газетой Le Figaro 24 июля 1999 г.). URL: http://www.ng.ru/ideas/2014–08–14/4_zinoviev.html.

[5] *Никонов С. Б.* Глобальное информационное пространство и международно-правовые аспекты управления информационными потоками: автореф. канд. дисс… полит.н. СПб., 2007 //Научная библиотека диссертаций и авторефератов disserCat. URL: http://www.dissercat.com/content/globalnoe-informatsionnoe-prostranstvo-i-mezhdunarodno-pravovye-aspekty-upravleniya-informat#ixzz4AK1VnBO9.

которая стремится осуществлять свою власть, используя возможности современных информационных технологий [1].

В 2014 г. лидирующие позиции среди крупнейших медиа-компаний сохранял Google. Второе место занял DirecTV, на третьем месте был Walt Disney, на четвертом — 21st Century Fox [2]. В 2015 г. акции Google были преобразованы в акции AlphbetInc. В мае 2016 г. AlphabetInc. стала самой дорогой в мире. Несомненно, одним из современных проявлений информационного дисбаланса продолжает оставаться цифровой разрыв. ИКТ — Индекс развития в странах мира в 2015 г. продемонстрировал, что первые 30 мест в рейтинге традиционно занимают страны с высоким уровнем дохода, что говорит о сильной взаимосвязи между финансами и прогрессом в области информационно-коммуникационных технологий. Авторы исследования также подчеркивают, что почти две трети из 30 стран, приведенных в рейтинге, находятся в Европе, где есть разработанная нормативно-правовая база, устоявшийся набор приоритетных целей и задач, а также сфер деятельности ИКТ, что помогло этим странам превратиться в передовые информационные экономики. Но следует заметить, что в число ведущих стран рейтинга входят также страны Азиатско-Тихоокеанского региона и Северной Америки [3]. По данным индекса развития ИКТ в 2015 г., первое место в рейтинге принадлежало Южной Корее [4].

В 2016 г. лидером рейтинга ИКТ «снова стала Республика Корея: (значение Индекса — 8,84). Россия, несмотря на рост значения индикатора с 6,79 до 6,95, потеряла одну позицию в рейтинге, переместившись с 42-го на 43-е место. В отличие от Республики Корея, характеризующейся сбалансированным развитием системы ИКТ, в России наблюдается значительный разрыв между значениями трех субиндексов. Несмотря

---

[1] Глобальное управление посредством контроля над массовой информацией. URL: http: //www.razumei.ru/lib/article/2827=Международный союз электросвязи: Индекс развития информационно-коммуникационных технологий в странах мира в 2015 году // Центр гуманитарных технологий. 03.12.2015. URL: http://www.gtmarket.ru/news/2015/12/03/726.

[2] Zenith Optimedia: Топ-30 крупнейших медиакомпаний мира // Медиа. 07 Мая 2014. № 3. URL: http://www. adindex.ru/news/media/2014/05/7/109946.phtml (дата обращения: 24.12.2016).

[3] Международный союз электросвязи: Индекс развития информационно-коммуникационных технологий в странах мира в 2015 году // Центр гуманитарных технологий. 03.12.2015. URL: http://www.gtmarket.ru/news/2015/12/03/7267.

[4] Там же.

на то, что в 2016 г. значение субиндекса "Использование ИКТ" выросло на 0,35 пункта — до 5,87, в рейтинге по его значению Россия потеряла три позиции, переместившись с 42-го места на 45. По субиндексу "Доступ к ИКТ" наша страна оказалась на 49 месте (7,23 пункта, рост на 0,04 пункта), потеряв две позиции по сравнению с 2015 г. По субиндексу "Навыки использования ИКТ" России удалось сохранить высокий результат 2015 г. — 8,55 пункта (при максимальном возможном в 10 пунктов) и 14-ю строчку в рейтинге» [5].

В 2014 г., согласно рейтингу «Топ-30 крупнейших медиакомпаний мира», китайская государственная телекомпания CCTV впервые вошла в этот рейтинг и заняла там 23 место. Еще одна китайская компания Baidu — крупнейшая поисковая система, местный эквивалент Google, который отсутствует на китайском рынке, оказалась на 28 месте. В развивающихся странах наиболее видное место занимает бразильская медиакомпания Globo, которая также представлена в указанной «тридцатке» [6]. Индекс развития ИКТ (2015) показывает, что две трети людей, у которых есть возможность доступа к онлайновой среде, живут в развивающихся странах. Активно растет рейтинг Коста-Рики, Бахрейна, Ливана, Ганы, Таиланда, Объединенных Арабских Эмиратов, Саудовской Аравии, Суринама, Кыргызстана, Беларуси и Омана [7]. Таким образом, информационная картина мира становится все более разнообразной.

Состоявшийся 2015 г. в Бразилии Форум, посвященный вопросам управления Интернетом, был сосредоточен на таких аспектах, как Интернет и права человека, кибербезопасность, интернет-экономика, открытость и разнообразие информации, многостороннее сотрудничество в информационно-коммуникационной сфере и т. д [8]. Формирование концепции управления Интернетом связано с идеей устойчивого развития, оказавшейся в центре внимания мировой общественности после Саммита Земли в 1992 г., когда в качестве жизненно важных для нашей планеты были определены три задачи человечества — экономический

---

[5] Связь. 43-е место заняла Россия в рейтинге стран по Индексу развития ИКТ в 2016 году. URL: http:// www.news.ivest.kz/117000438-svyaz-43-e-mesto-zanyala-rossiya-v-reytinge-stran-po-indeksu-razvitiya-ikt-v-2016-godu.

[6] Zenith Optimedia: Топ-30 крупнейших медиакомпаний мира // Медиа. 07 Мая 2014. № 3. URL: http://www. adindex.ru/news/media/2014/05/7/109946.phtml.

[7] Международный союз электросвязи: Индекс развития информационно-коммуникационных технологий в странах мира в 2015 году // Центр гуманитарных технологий. 03.12.2015. URL: http://www.gtmarket.ru/news/2015/12/03/7267.

[8] About IGF2015 // internet governance forum. URL: http://www.igf2015.br/.

рост, социальная интеграция и экологическая устойчивость. В сентябре 2015 г. вопросы устойчивого развития стали кардинальным пунктом повестки дня ООН в области развития до 2030 г.[1] По словам Генерального секретаря ООН Пан Ги Муна, в 2015 г. Организация вступила на путь дальнейшей борьбы с изменением климата, а также достижения целей устойчивого развития и процветания всех, живущих на одной планете. ИКТ и Интернет должны помочь пройти эту тернистую дорогу[2].

Преодоление информационного дисбаланса как на внешнем, так и на внутреннем уровне, — одна из составляющих информационной безопасности нашей страны. Согласно оптимистической версии прогноза о развитии Интернет в России, 84,8% населения станут пользователями Интернета[3]. Пока мы все еще продолжаем сталкиваться с информационным дисбалансом. По уровню проникновения Интернета в различные населенные пункты России лидируют Москва и Санкт-Петербург, затем в порядке убывания следуют города, население которых составляет один миллион человек и выше, от 500 тысяч до миллиона, от 100 до 500 тысяч, менее 100 тысяч, на последнем месте находятся села (хотя здесь наблюдаются позитивные сдвиги: половина сельских жителей страны — пользователи интернета). Что же касается развития информационного общества, то и здесь мы видим заметные расхождения. Например, в рейтинге Минкомсвязи РФ по уровню развития информационного общества за 2015 г. два последних места занимают Севастополь и Республика Крым. В последнюю десятку входят Карачаево-Черкесская Республика (76 место), Республика Северная Осетия — Алания (77), Республика Тыва (78), Кабардино-Балкарская Республика (79), Ненецкий автономный округ (80), Республика Ингушетия (81), Республика Дагестан (82), Чеченская Республика (83). Если Москва в указанном рейтинге стоит на первом месте, Санкт-Петербург — на втором месте, то Московская область — на 30, а Ленинградская на 54[4].

---

[1] The Internet and Sustainable Development. URL.: http://www.internetsociety.org/fr/node/426653.

[2] Countries adopt plan to use Internet in implementation of Sustainable Development Goals. URL: http: // http://www.un.org/sustainabledevelopment/blog/2015/12/countries-adopt-plan-to-use-internet-in-implementation-of-sustainable-development-goals.

[3] Интернет в России в 2015 году. Состояние, тенденции и перспективы развития в 2015 году. Отраслевой доклад. — М., 2016. URL: http://www.fapmc.ru/rospechat/activities/reports/2016/inet/main/custom/00/0/file.pdf.

[4] Интернет в России в 2015 году. Отраслевой доклад. М., 2016. URL: http://www.fapmc.ru/rospechat/activities/reports/2016/inet/main/custom/00/0/file.pdf.

Информационная безопасность обретает особую злободневность и в связи с тем, что медиарынок страны сталкивается с серьезными проблемами. Как считают отраслевые эксперты, существует неблагополучие в области периодической печати страны, которое «вызвано общим экономическим и валютно-финансовым кризисом в стране. Двукратное обесценивание рубля за неполных полтора года, вызвавшее резкое удорожание производства печатной продукции из-за роста цен на бумагу, типографские пластины, краски и другие полиграфические материалы, заметное сокращение реальных доходов и покупательной способности населения негативно влияют на развитие газетно-журнального бизнеса в России и его экономические показатели. Сказывается и недостаточность мер государственной поддержки этого бизнеса, включая обременительность налогов, практически повсеместное сокращение в субъектах Российской Федерации количества специализированных точек розничных продаж периодической печатной и книжной продукции, рост почтовых подписных тарифов, падение у населения интереса к чтению. Вносит свою лепту и бурное развитие цифровых средств массовых коммуникаций» [5]. Во многом этими же причинами обусловлено сокращение доли времени, которое среднестатистический российский гражданин отводит на медиапотребление. По сравнению с 2012 г. уменьшилось время, уделяемое нашими соотечественниками не только на чтение печатной продукции — книг, газет, журналов, но и на обращение к радио и телевидению [6].

Что касается отечественного радио, то оно, как и другие медиа, столкнулось с определенными трудностями, хотя это средство информации в условиях нынешнего витка научно-технической революции обладает огромным потенциалом. В силу экономических проблем сократился объем рекламных поступлений при одновременном снижении государственных субсидий: «Поскольку снижение рекламной выручки было сильнее, это привело, по оценкам экспертов, к повышению веса дотационных источников среди государственных радиостанций с 65% в 2014 г. до 74% в 2015 г.» [7]. В ходе изучения аудитории радио выясни-

---

[5] Федеральное агентство по печати и массовым коммуникациям. Управление периодической печати, книгоиздания и полиграфии. Российская периодическая печать. Состояние, тенденции и перспективы развития. Отраслевой доклад. 2016. URL: http://www.fapmc.ru/rospechat/activities/reports/2016/pechat/main/custom/0/0/file.pdf.

[6] Федеральное агентство по печати и массовым коммуникациям. Книжный рынок России. Состояние, тенденции и перспективы развития. 2016. URL: http://www.fapmc.ru/rospechat/activities/reports/2016/bookmarket/main/custom/0/0/file.pdf.

[7] Федеральное агентство по печати и массовым коммуникациям. Радиовещание

лось, что в ряде городов уменьшилось число измеряемых радиостанций. Если в 2014 году в Москве насчитывалось 50 таких радиостанций, то в 2015 г. — 48. В то время как число станций, вещающих в Москве, составило более 60: «Таким образом, почти половина станций, реально вещавших в Москве, оказалась либо вообще вне системы измерения, либо в группе с ограниченной поставкой информации об аудитории. Причины такого положения дел следует искать в отсутствии специального регулирования измерения аудитории. В итоге измерители произвольно устанавливают цены на аудиторную информацию, которая определяет количество показателей, и полный набор оказывается "не по карману" многим радиовещателям» [1]. В Санкт-Петербурге также стало меньше измеряемых станций, хотя их общее количество не изменилось [2].

Если рассматривать мирополитический контекст, то следует отметить обострение отношений России и Запада, России и США на фоне украинского кризиса и вооруженного конфликта с ИГИЛ в Сирии, антироссийских операций, нацеленных на создание виртуальной картины, неадекватной реальной обстановке. Одна из этих операций, по мнению академика РАН А. Кокошина, — информационно-психологическое и физическое воздействие на персонал правительственных, экономических и военных органов управления государств [3]. Яснее должна быть выражена мысль об активном участии России на международной арене как сильного и самостоятельного государства.

В интервью журналисту российской газеты «Аргументы недели» ветеран российской разведки, полковник в отставке С. В. Новиков рассказал о самой засекреченной глобальной системе электронного шпионажа «Эшелон» [4]. Она засекает всё, от болтовни по телефону домохозяек до электронных подписей президента или начальника Генштаба на запуск стратегических ракет. Фактически каждый человек в мире, использующий телефон, факс или электронную почту, ежедневно контролируется

в России в 2015 году. Состояние, тенденции и перспективы развития. Отраслевой доклад. Москва, 2016. URL: http://www.fapmc.ru/rospechat/activities/reports/2016/radio/main/custom/00/0/file.pdf.

[1] Там же.

[2] Там же.

[3] *Подзоров Е.* Осторожно: кибервойны // Красная звезда. 29.01.2011. № 14(25744). С. 24.

[4] *Кондрашов А.* «Фейсбук» — находка для агента: Как спецслужбы используют социальные сети // Аргументы недели. № 36 (527). 2016. 15 сентября. URL: http://www.argumenti.ru/espionage/n556/467414.

«Эшелоном», даже не догадываясь об этом. По сути дела, все мы находимся в мировом электронном концлагере.

Электронная разведывательная система «Эшелон» — это более ста спутников-шпионов, наземные станции слежения и подслушивания, большое количество суперсовременных и мощных компьютеров (по некоторым данным, в американском Агентстве национальной безопасности, АНБ, работает до 10 только сверхмощных компьютеров «Крей» стоимостью в десятки миллионов долларов каждый). Впрочем, не отстают от них и контрразведка, полицейское ведомство, другие спецслужбы. Так, недавно Федеральное бюро расследований США (ФБР) тоже обзавелось спецподразделением для мониторинга Интернета. Центр стратегической информации ФБР разместил на сайте ведомства запрос на создание «Приложения по социальным сетям». В документе сказано: «Социальные сети стали основным источником разведывательной информации, так как в них можно найти первую реакцию на ключевые события». Программа должна собирать информацию из «открытых источников» и иметь возможность обеспечить автоматизированный поиск и фильтрацию информации из социальных сетей, включая «Фейсбук» и «Твиттер» [5]. Исследователи и раньше обращали внимание на Интернет как огромный ресурс для воздействия на большие массы людей.

Доктрина информационной безопасности — основной официальный документ, определяющий главные информационные угрозы и направления борьбы с ними, разработана в соответствии со стратегией национальной безопасности, которая была принята в декабре 2015 г. Согласно новому документу, подписанному Президентом Российской Федерации В. Путиным от 5 декабря 2016 г., стратегическая цель обеспечения информационной безопасности в области обороны России — предотвращение военных конфликтов, которые могут возникнуть при применении информационных технологий.

В обеспечении информационной безопасности существенную роль играет вся система средств массовой информации. Как отмечается в Доктрине 2016 г., «Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской

[5] *Кондрашов А.* «Фейсбук» — находка для агента. Как спецслужбы используют социальные сети. № 36(527). 15.09.2016 // Аргументы недели. URL: http://www.argumenti.ru/espionage/n556/467414.

и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности» [1]. Нам бы хотелось особо подчеркнуть роль средств массовой информации и массовых коммуникаций как участников системы обеспечения информационной безопасности нашей страны.

Как видим, в новом документе вводится ряд основных понятий. Одно из них — «информационная инфраструктура Российской Федерации» (далее — информационная инфраструктура), которая определяется как совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации [2]. Таким образом, продукты журналистской деятельности в массмедиа становятся объектами информационной инфраструктуры. Неслучайно Доктрина вызвала интерес самих СМИ, которые по-разному оценивали значение документа [3]. Журналисты обращали внимание, с одной стороны, на необходимость превращения СМИ в пространство открытости, широкого обмена информацией, на сохранение их суверенитета и самобытности, выступали против признания Интернета враждебной средой, но, с другой стороны, соглашались с возможностью поиска эффективных защитных механизмов массмедиа от мощных негативных воздействий.

---

[1] Доктрина информационной безопасности Российской Федерации, сайт Совета безопасности. URL: http://www.scrf.gov.ru/documents/6/5.html.

[2] Там же.

[3] *Коростиков М., Черненко Е.* Интернет в России признан враждебной средой // «Ъ» ознакомился с проектом новой доктрины информационной безопасности России. http://www.kommersant.ru/doc/3023100 24.06.2016; *Замахина Т.* Самое сильное оружие в России — новая доктрина. URL: https://www.rg.ru/2016/12/07/deputaty-prokommentirovali-novuiu-doktrinu-informacionnoj-bezopasnosti.html.

«Созданная глобальная информационная сеть, декларируемая как сеть для мирного сосуществования в глобальном информационном пространстве, перешла практически в неконтролируемый поток информации. Выпуск необходимой информации в свет, информационный шум, забивающий информацию конкурента, формирование постановочной информации, информационный поток — все стало на сторону обладателя возможностей выпускать такую информацию. Провозглашенная свободной зона глобальной сети ставится под контроль» [4].

Оценивая значение Доктрины, известный тележурналист, заместитель председателя Госдумы П. Толстой *заявил:* «Если мы хотим сохранить наши ценности, нашу правду, нашу историю, нашу страну — мы должны уметь защитить их. Но без участия в этом каждого отдельного человека, пользующегося Интернетом, каждого родителя ребенка, сидящего в соцсетях, любые меры будут малоэффективны. Никакие доктрины не помогут, пока мы сами не начнем отдавать себе отчет в грозящих опасностях, пока не начнем соблюдать информационную гигиену и не приучим к этому своих детей» [5].

Таким образом, остается открытым вопрос о сохранении баланса между доступом к информации, открытостью и свободой ее распространения и ответственностью работников коммуникационно-информационной сферы за содержание информации. Новые медиа в силу специфики требуют новых способов установления такого баланса, равно как и соответствующего закрепления их в юридических нормах, учитывающих «исчезновение физических границ» для доступа к информации в киберпространство и свободу пользования благами ее получения и отправления.

Медийный компонент в доктрине информационной безопасности: сущность, концепты, принципы реализации. Информационная безопасность — это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств» (Закон РФ «Об участии в международном информационном обмене»). Информационная безопасность общества в целом и личности в частности характеризуется степенью защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности (экономики, науки, техники, сферы управления, военного дела, общественного сознания и т. д.) по отношению к опасным,

[4] *Мельник Г. С., Никонов С. Б.* Медийный компонент в доктрине информационной безопасности // Управленческое консультирование. 2014. № 1. С. 20.

[5] На войне как на войне. Вице-спикер Госдумы Петр Толстой — о том, зачем нужна доктрина информационной безопасности // News. Закон и право. news2.ru/509453.

дестабилизирующим, деструктированным, ущемляющим интересы общества и личности информационным воздействиям на уровне как внедрения, так и получения информации. Информационная безопасность определяется способностью либо нейтрализовать, либо ликвидировать такие последствия. Информационная безопасность — одно из направлений внешнеполитической деятельности России в современных международных отношениях. Вопросы информационной безопасности занимают большое место в юридических разработках и документах международных организаций ООН, ЮНЕСКО, Совета Европы, ОБСЕ, Европейского союза. В документах о свободе коммуникаций в Интернете есть положения: государственные органы не должны использовать блокировки и фильтры, которые препятствуют доступу к информации, кроме как в целях защиты несовершеннолетних; государства должны поощрять и поддерживать доступ для всех к коммуникационным и информационным услугам на недискриминационной основе и по доступной цене [1]. Однако вопреки этим принципам в конце ноября 2016 г. была принята европейская резолюция по противодействию российским СМИ. ЕС стремится наполнить информационное пространство исключительно идеями и новостями европейской медиапродукции, укрепляя свои позиции в киберпространстве и цифровой среде. Новая доктрина стала симметричным ответом на эту резолюцию. По мнению Европарламента, средства массовой информации России ведут «враждебную пропаганду» против государств Евросоюза.

В тексте документа особо отмечается «тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности», например, на Украине. Одним из рисков признано «наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру РФ в военных целях». Этот вопрос неоднократно поднимался на разных уровнях. Так, 20 апреля 2011 г., выступая в Госдуме с отчетом о работе правительства, премьер-министр В. Путин сказал: «Интернет — это<…> возможность общения,

[1] *Гайдарева И. Н.* Информационная составляющая национальной безопасности // Вестник Адыг. гос. ун-та. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. Вып. 2007. № 1. URL: http://cyberleninka.ru/article/n/informatsionnaya-sostavlyayuschaya-natsionalnoy-bezopasnosti.

самовыражения, это инструмент повышения качества жизни. Правда, основные ресурсы находятся не в наших руках — за бугром, вернее, за океаном. Именно это вызывает озабоченность некоторых спецслужб, имею в виду возможность использования этих ресурсов в интересах, противоречащих интересам общества» [2].

В ряде информационных угроз России указано, что «расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий» [3].

Аналитики указывают на «многочисленные религиозные группы различной направленности, которые, лицемерно используя лозунги мультикультурности, толерантности и политкорректности, наращивают свое влияние, стремятся войти в правительства различных государств и получить доступ к власти» [4]. В информационной доктрине: «Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников» [5].

В частности, отмечается тенденция к увеличению в зарубежных СМИ объема материалов, содержащих предвзятую оценку о действиях Российской Федерации. Смысл антироссийских публикаций можно свести к ряду тезисов, которые повторяются как мантра. Во внешней

---

[2] Путин против ограничений в Интернете // Регнум. Информационное агентство. URL: https://www.regnum.ru/news/1396929.html.

[3] Доктрина информационной безопасности Российской Федерации, сайт Совета безопасности. URL: http://www.scrf.gov.ru/documents/6/5.html.

[4] *Черкасов А.* Информационно-психологическая безопасность в условиях глобализации. URL: http://www.ruskline.ru/analitika/2011/04/27/informacionnopsihologicheskaya_bezopasnost_v_usloviyah_globalizacii/?commsort=votes.

[5] Доктрина информационной безопасности. Национальная безопасность. Информационная безопасность России. 13 декабря 2016 // Совет Безопасности России. URL: http://www.scrf.gov.ru/documents/6/135.html.

политике: Россия аннексировала Крым; российские войска вторглись на Украину; Россия опасно приблизилась к НАТО; Россия угрожает безопасности США (Украины, Польши, Прибалтики и далее по всему европейскому списку вплоть до Турции). Относительно внутренней политики тематический набор тоже не отличается разнообразием: в России режим авторитарный, путинский; народ нищает, экономика падает; Россия должна развалиться; надо поднимать экономику, а не укреплять Вооруженные силы. Также в связи с участившимися террористическими актами в России и мире, Доктрина обращает внимание на информационное воздействие через социальные сети со стороны запрещенных в России организаций на жителей страны, в частности на молодежь, которая больше подвержена влиянию. Информационное давление именно на молодежь оказывается «в целях размывания традиционных российских духовно-нравственных ценностей» [1]. Здесь имеется в виду преемственность российской культуры и традиций, связь между поколениями, которая из-за развития новых информационных технологий становится все слабее. Действительно, в сети находятся и активно публикуются до сих пор различные отчеты экстремистских акций. Они передаются всеми возможными способами как форумы, закрытые чаты, сообщества, цитаты, картинки и музыка, видеоконтент и т. д. Как показывают социологические исследования, пространство в самой меньшей мере подвержено цензуре и наиболее популярно у молодого поколения. Таким образом, в настоящее время киберпространство расценивается экстремистскими организациями как наиболее привлекательная площадка для ведения своей деятельности [2].

Сильнейшим информационным сетевым атакам подвергаются дети. На правозащитном сайте размещена «кричащая» информация: на пространстве российского Интернета в открытую функционируют ресурсы, заявляемые как пародия на российскую гомофобию, а в реальности нарушающие законодательство РФ. Под предлогом сатиры популяризируются

---

[1] *Панов В.* Аватары для «избранных». Сетевые технологии и оппозиционное движение в России. Столетие.Ru. 26.03.2016 // Русская народная линия. URL: http://www.ruskline.ru/monitoring_smi/2016/03/2016–03–26/avatary_dlya_izbrannyh.

[2] *Васина Е. И.* Экстремизм в молодежной среде, СМИ и интернет // Молодой ученый. 2016. № 10. С. 1322–1325; *Тхакохов А. А.* К проблеме молодежного экстремизма: факторы распространения, особенности, способы борьбы // Молодой ученый. 2015. № 4. С. 481–482; *Старкова Н. А., Старков А. Н., Чернова Е. В.* Киберэкстремизм в молодежной среде как социальная проблема // Фундаментальные исследования. 2014. № 12–7. С. 1550–1557.

сайты, обучающие наших детей и гомофилии, и педофилии. После того, как порнография заявляется как пародия, если ты начинаешь критиковать, то оказываешься в положении человека, который не понимает юмора, неотесанным грубым быдлом, не понимающим тонкого креативного юмора [3].

Администратору «группы смерти» «ВКонтакте» Ф. Будейкину, известному в Интернете под псевдонимом Филипп Лис, предъявлено официальное обвинение в доведении подростков до самоубийства, сообщили в пресс-службе ГСУ СК по Санкт-Петербургу. В списке его жертв — 15 подростков со всей России. Еще пять человек, состоявших в закрытом сообществе, отказались совершать самоубийство. Только по официальным данным за последний год в России покончили с собой более 700 подростков. Но реальные цифры гораздо выше. Это были дети из благополучных семей и разных уголков России. Всех их, на первый взгляд, объединяло лишь одно — подростки активно пользовались соцсетями, в которых, как им казалось, они спасались от унылой жизни в реальности. Савёловский суд Москвы закрыл доступ к 13-ти страницам в социальной сети «ВКонтакте», пропагандирующим зацеперство — популярное среди детей и подростков смертельно опасное развлечение, заключающееся в проезде на поездах с внешней стороны.

Виртуальное общение — неотъемлемая часть времяпрепровождения практически всех, кто знает, что такое Интернет. Только использовать такую возможность общаться можно по-разному. За пять минут онлайн-переписки можно узнать домашний адрес ребенка и назначить встречу. А на месте виртуального знакомого может оказаться кто угодно [4]. Вместе с тем 1 октября 2014 г. в ходе заседания Совета безопасности РФ президент заявил: «Хотел бы подчеркнуть — мы не намерены ограничивать доступ в сеть, ставить ее под тотальный контроль, огосударствлять Интернет, ограничивать законные интересы и возможности людей, общественных организаций, бизнеса в информационной сфере» [5].

Доктрина характеризует состояние информационной безопасности

---

[3] 18+. Почему Роскомнадзор разблокировал сайты гомопедофилов? Детская порнография как пародия // Наш дом — наша крепость. Информационно-независимый портал родителей. URL: http:// www.nezavisroditeli.ucoz.ru/load/sajty_gde_zombirujut_nashikh_detej /sajty_dlja_promyvanija_mozgov/inet_zombirovanie/7–1–0–22 25.07.2012.

[4] Группы и сообщества в социальных сетях. URL: http:// nezavisroditeli.ucoz.ru/load/sajty_gde_zombirujut_nashikh_detej/gruppy_i_soobshhestva_v_socialnykh_setjakh_opasnye_dlja_detej/30.

[5] Доктрина информационной безопасности РФ. Досье, информационное агентство ТАСС. URL: http:// www.tass.ru/info/3845810.

в области науки, технологий и образования в том числе «низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности». Именно в этом и состоит одна из задач СМИ — получать, обрабатывать и распространять информацию, с целью осведомления граждан об информационной политике государства. В Доктрине предлагается нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества [1]. Изучение практики современной российской журналистики показывает болезненность проблемы. Так, РИА Новости опубликовало социологические исследования, проведенные центром социально-политического мониторинга Института общественных наук опроса, Российской академии народного хозяйства и государственной службы (ИОН РАНХиГС), согласно которым более 80% россиян признают, что зарубежные СМИ искажают историю войны 1941–1945 гг. Факты искажения истории войны в зарубежных СМИ отметили 83,5% опрошенных. При этом 61% респондентов уверены, что зарубежные средства массовой информации очень часто распространяют неверную информацию о Великой Отечественной войне, а 22,5% россиян признают, что это случается время от времени. Впрочем, 60% россиян отмечают, что и отечественные СМИ искажают историю Великой Отечественной войны: 12% уверены, что это происходит часто, а 48,1% опрошенных считают, что «иногда» [2].

В новой доктрине информационной безопасности России практически ничего не сказано о возможностях массмедиа в скрытом воздействии на граждан и той опасности, которую таят в себе психологические ресурсы воздействия. Тогда как сегодня, благодаря применению новейших разрушительных информационных технологий, «человек постепенно утрачивает способность к проблематизации и личностному целеполаганию. Это объясняется, по словам военного специалиста ведущего сотрудника Российского института стратегических исследований В. В. Карякина, “информационным перегревом” сознания человека, на фоне которого формируется потребность в быстром получении информации по интересующим вопросам, что обеспечивается демонстрацией поверхностных

[1] Доктрина информационной безопасности. Национальная безопасность. Информационная безопасность России. 13 декабря 2016 // Совет Безопасности России. URL: http://www.scrf.gov.ru/documents/6/135.html.

[2] Опрос: 83% россиян обвиняют зарубежные СМИ в искажении истории ВОВ. 06.04.2011. URL: https://ria.ru/society/20150406/1056932011.html.

демо-версий происходящих событий»[3]. Таким образом, усиление конфликтогенных моделей отношений между государствами диктует, с одной стороны, необходимость укрепления позиций России в глобализирующемся мире, с другой стороны, требует формирования устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве. СМИ играют ключевую роль в воздействии на общество и потому для решения задач включаются в качестве одного из основных элементов информационной безопасности.

Воздействие медийных технологий на безопасность личности и общества. В последнее десятилетие XX в. произошло крушение биполярной геополитической модели мироустройства, коренным образом изменилась геополитическая ситуация во всем мире под воздействием таких дестабилизирующих факторов, как усиление вестернизации глобальных процессов, деятельность международных террористических организаций, активизация сепаратизма[4], функционирование всевозможных транснациональных сетей (в том числе и незаконных, но неотличимых от законных; местоположение штабов и руководителей которых часто невозможно определить). Как следствие, обострилась борьба между отдельными странами за глобальное и региональное лидерство и обладание природными ресурсами. «Формы этой борьбы различны, но ее ожесточенность и бескомпромиссный характер свидетельствуют об актуализации вопросов обеспечения национальной безопасности для каждого государства в отдельности, проблем выживания и развития в новом тысячелетии»[5]. В условиях глобальных вызовов главным стратегическим национальным ресурсом, определяющим экономическую и оборонную мощь государства, в данном случае — России, являются информация и информационные технологии, от которых в решающей

---

[3] *Карякин В.* В. Информационные войн и угрозы безопасности // NEO. Новое Восточное Обозрение. Исследования 2.13.07.10. URL: http://ru.journal-neo.org/2013/10/03/informatsionny-e-vojny-i-ugrozy-bezopasnosti/.

[4] *Кохтюлина И. Н.* Международные аспекты информационной безопасности в условиях глобализации: автореф. дисс. … канд. полит. наук. — М., 2010; *Никонов С.* Б. 1) Глобализация информационного пространства: объективная закономерность развития человеческого общества // Вестн. С.-Петерб. ун-та. Сер. 9. 2007. Вып. 2. С. 156; 2) Ноополитика как инструмент продвижения экономических интересов государств // Мир и политика. № 1 (64). 2012. Январь; The Rise or European Security Cooperation. Cambridge; n. Y.: Cambridge University Press, 2007. 301 p.

[5] *Бубнов А. В.* Глобальная информатизация и безопасность России / Под ред. В. И. Добренькова. М.: Изд-во Моск. гос. ун-та, 2001. С. 3.

степени зависят все сферы жизнедеятельности российского общества: производство и управление, оборона и энергетика, транспорт и связь, банковское дело и финансы, наука, образование и многие другие. При этом недостаточная защищенность информационных ресурсов приводит к утечке важнейшей политической, экономической, научной, военной информации. Активизировались информационные и информационно-психологические войны между отдельными странами, используется сетевая экспансия против России, сопровождаемая попытками установить полный контроль Запада над ситуацией в России. Нападение осуществляется трансгранично, без военной техники, с помощью негосударственных субъектов [1]. «Главный смысл и элемент сетевой модели войны — владение и обмен информацией, главная задача — развернуть пятую колонну в стране воздействия и так далее. Главная цель — полное господство над страной воздействия!» [2] Пятой колонной в системе российских СМИ ряд политологов называют такие печатные издания и аудиовизуальные СМИ, как «Эхо Москвы», «Грани.ру», «Ежедневный журнал», телеканал «Дождь», «Газета.ру», «Слон.ру», разные радио-ФМ, «Серебряный дождь». По мнению депутата Государственной думы Сергея Маркова, «критическую информацию о российской власти можно всегда почерпнуть из переводов публикаций иноязычной прессы на сайтах "ИноПресса.ру", "ИноСМИ.ру", а также, как и в "лучшие" времена холодной войны, из радиопередач тех же "Голоса Америки", БиБиСи, "Радио Свобода", "Немецкая волна" и других по-прежнему откровенно враждебных "голосов", как российских по местонахождению, так и зарубежных» [3].

На Западе неоднократно обвиняли Россию в «неизбирательном применении тяжелого вооружения в Сирии и убийстве мирных жителей страны», в том числе в городе Алеппо. Российская сторона эти обвинения отвергает и настаивает, что борется в Сирии с боевиками запрещенных в России террористических группировок ДАИШ («Исламское государство», ИГ, ИГИЛ) и «Джебхат ан-Нусра». В западных СМИ появляются циничные

---

[1] Инновационные направления современных международных отношений / Под ред. А. В. Крутских, А. В. Бирюкова. М.: Аспект Пресс, 2010. 295 с.

[2] *Черкасов А.* Информационно-психологическая безопасность в условиях глобализации. 27.04.2011 // Русская народная линия. URL: http://ruskline.ru/analitika/2011/04/27/informacionnopsihologicheskaya_bezopasnost_v_usloviyah_globalizacii/?commsort=votes.

[3] Цит. по: *Панов В.* Аватары для «избранных». Сетевые технологии и оппозиционное движение в России // Русская народная линия. Информационно-аналитическая служба. 26.03.2016. URL: http://www.ruskline.ru/monitoring_smi/2016/03/2016–03–26/avatary_dlya_izbrannyh.

публикации, в которых проявляется откровенная радость по поводу человеческих трагедий: убийство российского посла в Турции сравнивают с неонацистским послом, представляют убийство как возмездие за действия России в Сирии (россияне виноваты и посол виноват). Аналитики утверждают, что именно доступность негативной информации провоцирует сексуальную распущенность, огромное количество абортов, рост самоубийств, падение рождаемости, криминализацию школ, наркоманию, снижение уровня образованности. В целом ряде развитых европейских стран НИС привела к тому, что каждый третий член так называемого индустриального общества вынужден пользоваться услугами психотерапевта или психиатров [4]. Эти явления чреваты угрозами своевольного манипулирования текстами, нарушения прав человека на приватность информации, интеллектуальную собственность в различных формах, включая компьютерное пиратство и терроризм.

Профессор Военного университета Министерства обороны Российской Федерации генерал-майор А. В. Черкасов предостерегает как от огульного обвинения СМИ в нарушении правил информационной безопасности, так и от снобизма и высокомерия в опровержении этих обвинений. «Я не поддерживаю ни первое, ни второе. Сами СМИ, как автомат, пистолет, бомба и любое другое оружие, могут служить и добру, и злу. СМИ и информация опасны не сами по себе, а своим воздействием на психику, сознание, душу человека и самочувствие всего человечества. А зависит это воздействие от вполне конкретных людей, в чьих руках эти средства находятся, которые ими владеют, управляют и в них работают. Именно эти люди представляют очень большую опасность международной и национальной безопасности. И степень этой опасности определяется лишь одним критерием, их духовностью и наличием у них совести» [5].

Ряд исследователей подчеркивают, что информационные воздействия потенциально влияют на протестное поведение как отдельных социальных групп, так и индивидов, что создает угрозу политической стабильности и является вызовом национальной безопасности [6]. Разработанные в 2000-е гг. теории

---

[4] ИНЕТ-зомбирование. 2706.2012. URL: http://www.ligainternet.ru/hotline//5000/abuse.png.

[5] *Черкасов А.* Информационно-психологическая безопасность в условиях глобализации. 27.04.2011 // Русская народная линия. http://ruskline.ru/analitika/2011/04/27/informacionnopsihologicheskaya _bezopasnost_v_usloviyah_globalizacii/?commsort=votes.

[6] *Рахно Н. В.* 1) Информационная безопасность: сущность, концепты, принципы реализации // Социально-гуманитарные знания. 2010. № 7. С. 338; 2) Политическая коммуникация в контексте современной безопасности // Политическая идеология,

роения, описывающие информационное поведение сетевых сообществ, уже неоднократно проверены практикой политической борьбы в современном мире[1]. Основной феномен новой войны Аркилла и Ронфельдт видят в том, что раньше воспринималось как обычные партизанская война и мятежи, а теперь плавно переходит в форму социальной сетевой войны и становится глобальной войной — в пределе: мировой гражданской войной[2].

Американские авторы Джон Аркилла и Дэвид Ронфельдт в своей популярной книге «Наступление сетевой войны: подготовка к конфликтам в информационную эпоху», написанной в конце 90-х г. XX в., акцентировали внимание на специфике современных сетевых войн, цель которых достигается «совокупностью действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны». Именно эти авторы показали в дальнейшем, как меняется характер информационных войн, как обычные партизанские войны и мятежи плавно переходят в сетевые войны. Для адекватного описания форм ведения борьбы в социальных сетевых войнах Джон Аркилла применяет термин «роение» (swarming), проявляемое в множественных «микродействиях», «тычках» и «стычках»: в выступлениях в СМИ, в вооруженных и невооруженных физических столкновениях, в разного рода демонстрациях и презентациях, в навязываемых диалогах и переговорах с официальными лицами и пр.[3] Как заявил он же в своем выступлении на выпуске в военно-морской школе в 2014 г., сегодня вовсю идет война: «Мы находимся внутри мировой войны. Если взять вместе все соперничество, перед нами первый глобальный конфликт между государствами и сетями. Некоторые из этих сетей, хотя они и широко разбросаны, действуют для достижений общих целей. Другие стремятся к отдельным, собственным целям, во многом как Германия и Япония,

---

модернизация и безопасность — факторы устойчивого развития России: сборник научных статей. — Ставрополь, 2010. С. 254–261. URL: http://www.pandia.ru/text/78/018/23441.php.

[1] *Bonabeau Eric, Meyer Christopher*. Swarm Intelligence // Harvard Business Review, May 2001. P. 107–114; *Johnson Steven*. Emergence: The Connected Lives of Ants, Brains, Cities, and Software // N.Y., 2001 (on «swarm logic»); Andy Oram. ed., Peer-to-Peer: Harnessing the Power of Disruptive Technologies.: O'Reilly Media. 2001. 448 p.

[2] *Ronfeldt David F., Arquilla John, Fuller Graham E., Fuller Melissa.* The Zapatista «Social Netwar» in Mexico. RAND, 1998. URL: http://www.bookap.info/okolopsy/kalashnikov5/gl5.shtm.

[3] Networks and Netwars: The Future of Terror, Crime, and Militancy / John Arquilla and David Ronfeldt, editors. RAND, 2001. URL: http://www.rand.org/publications/MR/MR1382/.

которые хотя и были номинальными союзниками во время Второй мировой войны, мало работали в рамках прямо координированных, взаимно поддерживаемых действий. Сети определяются своими плоскими, децентрализованными организационными формами» [4]. И далее совершенно справедливо заявлял, что иерархиями трудно побеждать сети:

- надо становиться сетью, чтобы воевать с сетями,
- освоивший сетевую форму первым и наилучшим образом получит основные преимущества [5].

Роение базируется на двух требованиях. Во-первых, для атаки по многим направлениям надо иметь много малых единиц, маневренных и интернет-связанных. Во-вторых, эти единицы должны одновременно вести разведку, передавая информацию на самый верх. Поведение сетевых информаторов, называемое роение, сравнивается с поведением пчел, волков, гиен, а также вирусов и бактерий [6].

Перспективы России в современном мировом противостоянии, которые рисуют военные аналитики, имеют трагические очертания. «Сначала будет мощная пропагандистская кампания, живописующая ужасы геноцида, устроенного русскими криминальными милитаристами на Кавказе. Противодействовать ей Кремлю уже сегодня нечем — чего уж там говорить о 2015 годе? Когда весь Запад будет считать нас отпетыми нацистскими подонками, на Россию обрушатся всякие беды. В ход пойдут ионосферное, психотронное и агробиологическое оружие. Нам обеспечат и эпидемии, и голод, и стихийные бедствия. А в финале рванут и атомный заряд в Москве». Прогнозы выглядят зловеще и в других высказываниях: «В случае нападения на Россию натовцы станут бомбить не Казань, Нальчик, Йошкар-Олу или, например, Уфу — главный удар придется по великорусским городам. Так, чтобы заполучить на свою сторону этнократическую верхушку и подогреть сепаратизм» [7].

Обеспечение МИБ невозможно без знания о потенциальных и реальных опасностях и угрозах, возникающих в процессе функционирования СМИ, о степени реакции на эти угрозы, их восприимчивость. Вместе с тем пространство опасностей и угроз для МИБ громадно — от неразвитости

---

[4] Цит. по: *Почепцов Г.* Первые исследования в сфере информационных войн: от прошлого к современности. URL: http://psyfactor.org/psyops/infowar38.htm.

[5] *Arquilla J.* To build a network // Prism. 2014. Vol. 5. N1. P. 22–33.

[6] Networks and Netwars: The Future of Terror, Crime, and Militancy / John Arquilla and David Ronfeldt, editors. RAND, 2001. URL: http://www.rand.org/publications/MR/MR1382/.

[7] *Калашников М., Крупнов Ю.* Гнев орка. URL: http://www.bookap.info/okolopsy/kalashnikov5/gl50.shtm.

системы СМИ и информационных служб до сбоев в доставке информационных продуктов потребителям, от непонимания журналистами их места в системе демократии, гуманистических императивов ориентации их деятельности до нежелания и неумения вести социальный диалог. Опасности и угрозы, таким образом, могут возникнуть в любой сфере и на любом этапе журналистской деятельности и массово-информационного процесса [1]. Раздаются голоса ученых о необходимости ревизии информационных ресурсов России. Так, в статье профессор Я. Н. Засурский еще в 2001 г. предложил вести следующую работу:

- уточнение параметров информационных ресурсов России;
- определение роли государственных, частных и общественных средств массовой информации, способов их взаимодействия, а также методов преодоления угроз плюрализму и опасности монополизма в информационной сфере;
- разработка моделей доступа граждан к информации и определение угроз целостности информационного пространства нашей страны;
- разработка модели угроз информационной безопасности Российской Федерации и путей их преодоления в структурном, техническом, экономическом, правовом и политическом аспектах;
- создание модели возможных ограничений доступа к информации в целях защиты национальной безопасности, общественного порядка, предотвращения преступных и террористических акций, защиты частной жизни человека;
- определение ключевых направлений национальной политики в сфере массовой информации и коммуникаций. Таким образом, доктрина информационной безопасности в части, касающейся СМИ, нуждается в обновлении, прежде всего потому, что новые геополитические реалии требуют усиления роли государства в совершенствовании системы информационной безопасности, в том числе системы российских СМИ.

В связи с этим возникает необходимость научной разработки совершенствования структуры и системы средств массовой информации России в целях удовлетворения конституционных прав граждан. В этих целях предлагается провести мониторинг средств массовой информации, в результате которого будут разработаны:

- параметры информационных ресурсов России;

---

[1] *Мельник Г. С., Никонов С. Б.* Медийный компонент в доктрине информационной безопасности // Управленческое консультирование. 2014. № 1. С. 20.

- роль государственных, частных и общественных средств массовой информации, их взаимодействие, угрозы плюрализму и опасность монополизма в информационной сфере;
- модель осуществления доступа граждан к информации и угроз целостности информационного пространства России;
- модель угроз информационной безопасности РФ и путей их преодоления в структурном, техническом, экономическом, правовом и политическом аспектах;
- модель возможных ограничений доступа к информации в целях защиты национальной безопасности, обороны, международных отношений, общественного порядка, предотвращения преступных и террористических акций, защиты частной жизни и критериев их оценки; будут очерчены контуры национальной политики в сфере массовой информации и коммуникации [2].

Несмотря на то, что государством и общественными институтами много сделано в этом направлении, остается необходимость корректировать модели доступа и ограничений граждан к информации в целях защиты национальной безопасности, обороны, международных отношений, общественного порядка, предотвращения преступных и террористических акций. Доктрина показала, что спектр угроз сегодня переместился в сферу цифровых технологий. В последнее десятилетие усилился интерес медиаисследователей к изучению тактических медиа (tacticalmedia), представляющих собой информационные ресурсы, используемые субъектами сетевой коммуникации для побуждения к политическим действиям протестного характера и приведения в активное состояние политической системы для достижения какой-либо разрушительной задачи в реальной борьбе, чаще всего направленной против государственной политики.

Рассмотрение деятельности тактических медиа в связи с проблемой информационно-психологической безопасности объясняется тем, что этот корпус новых медиа позиционирует себя как исключительно радикальный и оппозиционный, направленный на критику политического режима. В целеполагании функционирования этого корпуса СМИ заложены идеи расслоения общества, разрушения глобальных социальных структур. Программные документы Tacticalmedia (TM) неизменно декларируют необходимость борьбы «с устойчивой тенденцией

---

[2] *Засурский Я. Н.* URL: http://www.emag.iis.ru/arc/infosoc/emag.nsf/BPA/5b9c943f52706569c3256c4e00495e6a.

к репрессиям, эксплуатации, изоляции, отчуждениями и корпоратизацией». Нередко ТМ маркируют себя как «медиа кризиса, критики и оппозиции». Информационная деятельность тактических медиа имеет продолжение в радикальных акциях, митингах, уличных беспорядках, которые могут длиться несколько дней. Выражение виртуального протеста в Интернет перетекает в ритуальные действия с непременной декламаций, лозунгами, символикой и отрежиссированными столкновениями с полицией.

Тактические медиа, претендующие на общественный контроль за действиями власти, меняют конфигурацию классической политики, подрывая нормативную властную систему информационными атаками. Используя стратегии и техники продвижения в аудитории политических идей протеста, инакомыслия и бунта, программ, символов, тактические медиа мобилизуют аудитории на проведение небезопасных социальных перфоменсов и политических флэшмобов («Оккупай Абай» и др.). Уже сами названия изданий несут в себе энергетический заряд («Наперекор», «Община», «Прямое действие», «Свобода или смерть», «Новый Свет», «Петроградец», «Намерение», «Удар», «Тротиловый эквивалент», «МедиаУдар») и указывают на их подрывную деятельность. «Достоверность» отображаемых событий достигается публикацией множества фотографий и скан-копий документов, видеозаписей в оперативном режиме. Международные информационные платформы «МедиаУдар», IndyVideo не только публикуют записи акций, но и обучают всех желающих пользоваться камерой и монтировать видео. Нередко эти медиа выступают средством координации действий в организации «умных толп» против глобальных организаций (G8, G20, WTO) и корпораций (Microsoft, Pepsi, Nike и др.).

Тактические медиа стали структурным информационным компонентом в таких важных политических процессах, как пробуждение радикального ислама, парад «цветных революций», порождение «арабской весны» и «майданов». Как коллективный актор медиа в этих процессах с успехом реализовали функции мобилизации, подрыва, разрушения. Локальные по месту образования, тактические медиа становятся глобальными по воздействию, создавая сети активистов, позволяющих ускорять распространение опробованных техник и влиять на политические ситуации. Тактические массмедиа можно было бы рассматривать в одном ряду с такими видами новой сетевой журналистики, как гражданская, социально-активная, партизанская журналистика, коллаборативная и комьюнити-журналистика. Все эти типы журналистики можно назвать альтернативными. Тактические медиа несут на себе частично черты всех перечисленных типов

журналистики — провозглашают себя независимыми, альтернативными, СМИ для «*Do it yourself*» *(«Сделай сам»),* привлекают единомышленников, обучают их профессиональной журналистике (например, делать телесъемки или создавать газету). Однако ориентация исключительно на протест и мобилизацию читателей для решения политических задач заставляет выделить их в особый сегмент сетевых СМИ.

Одна из отличительных особенностей различных протестов, в которых участвуют тактические медиа, — это не просто принятие конкретной тактики (особенно для занятия публичных городских площадей), но и сознательное взаимоувязывание событий по мере их разворачивания. Так, например, итальянские активисты движения Unicommons были физически связаны с бастующими студентами в Тунисе, а египетские блоггеры и арендаторы площади Тахрир связаны с активистами в Испании, которые, в свою очередь, выражали солидарность и даже инициировали транснациональные действия с активистами в Соединенных Штатах и других странах [1].

С конца 2000-х гг. разрастаются сети «Индимедиа-Питер», «Индимедиа-Сибирь» и «Индимедиа-Кубань», украинская и белорусская «Индимедиа», которые размещают 15–20 тыс. страниц в день под рубрикой «Час Ч» [2]. Базируясь на ранее принятых художественных принципах, сотрудники тактических медиа пытаются определять новую медийную культуру, внедряя в информационное поле не только свои ценности, но особый «революционный» язык. Идеологи протестных медиа выдвигают программы новой организационной логики транснациональных горизонтальных сетей, которые считают основополагающими: территории, полномочия и права; настаивают на создании конкретных пространственно-временных связей на основе общих интересов, но и вокруг аффективных связей, по большому счету внеинституциональных, в основном в неформальном секторе; предлагают движение в обход сложенных иерархий вертикально интегрированных силовых структур в горизонтальные конфигурации социальной организации; используют связывание всего многообразия местных групп, сайтов, сетей, географических и культурных контекстов и особенностей в сетевом пространстве в новую пограничную зону. Структурно оформленные в огромную сеть тактические медиа становятся

[1] Charting Hybridised Realities. 2012. 15 April. URL: http: //www.blog.tacticalmediafiles.net/index.php/2012/04/15/charting-hybridised-realities.

[2] От «Кинопоезда» до «Прямого действия»: Анархия в Интернете, в газетах, в литературе и на видео // Новая газета. 2009. 3 апреля. URL: https://www.novayagazeta.ru/articles/2009/04/03/43332-ot-kinopoezda-do-pryamogo-deystviya.

очень влиятельными. Таким образом, тактические медиа выступают как эффективный информационный, идеологический, мобилизационный, организационный и синхронизирующий ресурс, где аккумулируются разрушительные идеи и формируется база оппозиционных коммуникативных практик, где быстро достигаются политические задачи при ограниченных временных, финансовых и эмоциональных затратах. При этом такие медиа «описывают и смакуют порок, разврат, не замечают, не хотят замечать добро и добродетели. Они обрушивают на людей сплошной негатив, постоянные водопады негативной, подавляющей, разрушающей психику информации, не замечая ничего хорошего в людях, в народе, в обществе, в стране, в живом и неживом мире» [1]. Информационно-психологическая угроза безопасности тактических медиа заключается в том, что они без меры расширяют критическое пространство, увеличивают степень конфликтогенности политического взаимодействия в условиях глобализации, ориентируют социум на деструктивные (дестабилизация, дезорганизация, дезинтеграция) действия. Тактические средства массовой информации распространяют идеи против гнета, эксплуатации, изоляции, отчуждения и тем самым увеличивают риск вовлечения человека в деструктивные политические кампании.

В новых геополитических условиях общество вынуждено вырабатывать защитные механизмы от деструктивного воздействия, разрушающего систему гуманитарных ценностей. Сторонники всеобщего медиаобразования совершенно правильно предлагают подход, построенный не на защите от СМИ, а на формировании у человека критического восприятия медийного мира [2], способности к «развенчанию» мифов, псевдоценностей и стереотипов, пропагандируемых в СМИ. К сожалению, понятие «информированность» не используется в «Доктрине», хотя, как представляется, должно бы стать ключевым при характеристике сущности информационно-психологической безопасности.

---

[1] *Черкасов А.* Указ. соч.

[2] *Левицкая А. А.* Синтез медиаобразования и медиакритики в процессе подготовки будущих педагогов: монография / А. А. Левицкая, А. В. Федоров, Е. В. Мурюкина и др.; под общ. ред. А. А. Левицкой. Ростов-на-Дону, Изд-во Южноурал. ун-та, 2016. 574 с.; *Федоров А. В.* Медиаобразование: вчера и сегодня. М.: Изд-во ЮНЕСКО «Информация для всех», 2009. 234 с.

Глава 4. Роль качества сообщений массмедиа в обеспечении информационно-психологической безопасности человека

Применение различных средств и технологий информационно-психологического воздействия сегодня становится обычным явлением в повседневной жизни, экономической конкуренции и политической борьбе. От качества информации во многом зависит степень адекватности реагирования человека на происходящие вокруг события, а также его психическое и физическое здоровье.

В связи с этим в современной науке обозначен широкий круг проблем от медико-психологических особенностей восприятия информации до понятия психологической травмы или формулирования критериев корректности информационного воздействия [3]. Понимание угроз информационно-психологической безопасности личности, механизмов их действия и возможностей психологической защиты становится не только теоретической проблемой, но и потребностью социальной практики и повседневной жизни человека [4].

---

[3] Проблемы медиапсихологии. Материалы секции «Медиапсихология» Международной научно-практической конференции «Журналистика в 2000 году: Реалии и прогнозы развития» / Сост. Пронина Е. Е. М.: МГУ, 2001.

[4] *Самуйлова И. А.* Проявление феномена информационно-психологической безопасности в политической коммуникации // От истоков к современности: 130 лет организации психологического общества при Московском университете: Сборник материалов юбилейной конференции: В 5 тт. Т. 2 / Отв. ред. Богоявленская Д. Б. М.: Моск. психол. о-во, 2015. Т. 2. С. 454–456; *Тер-Акопов А. А.* Безопасность человека:

Информационно-психологическая безопасность системы социально-политических отношений информационного общества представляет собой такое состояние системы информационно-психологических отношений, в котором она способна успешно, устойчиво и непрерывно развиваться в условиях внешних и внутренних информационно-психологических конфликтов, носящих как стабилизирующий, так и деструктивный характер.

Будем исходить из понимания информационно-психологической безопасности как состояния защищенности индивидуальной, групповой и общественной психологии и, соответственно, социальных субъектов различных уровней общности, масштаба, системно-структурной и функциональной организации от воздействия информационных факторов, вызывающих дисфункциональные социальные процессы [1]. На уровне личности, информационно-психологическая безопасность проявляется в состоянии защищенности психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-ориентировочной основы социально-политического поведения человека, а также адекватной системы его субъективных отношений к окружающему миру и самому себе [2]. К факторам, усиливающим угрозы негативных информационно-психологических воздействий, относятся [3]:

1) политические факторы:

— изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, формирования новых национальных интересов;

Социальные и правовые основы. М.: Норма, 2005. 272 с.; *Сулакшин С. С., Сазонова Е. С., Хвыля-Олинтер А. И.* Государственная политика защиты нравственности и СМИ. М.: Наука и политика, 2014. 360 с.

[1] *Грачев Г. В.* Информационно-психологическая безопасность личности. М.: Изд-во РАГС, 1998.

[2] *Рощин С. К., Соснин В. А.* Психологическая безопасность: новый подход к безопасности человека, общества и государства // Российский монитор. 1995. № 6.

[3] См.: *Грачев Г. В., Мельник И. К.* Приемы и техника манипулятивного воздействия в массовых информационных процессах / Проблемы информационно-психологической безопасности (сборник статей и материалов конференций). М.: Изд-во РАГС, 1996; *Самуйлова И. А., Шлионский А. Л.* Информационно-психологическая безопасность отношений Власть-СМИ-Общество // Материалы участников научно-практического семинара «Журналистика и мир-2008. Журналистика в мире технологий» // Ред-сост. М. Н. Ким. СПб.: Роза мира, 2008. С. 204–210.

— становление государственности на основе принципов демократии, законности, информационной открытости;
— разрушение ранее существовавшей командно-административной системы государственного управления, политико-идеологической сферы, а также сложившейся системы обеспечения безопасности страны;
— информационная экспансия со стороны ряда развитых стран, осуществляющих глобальное информационно-пропагандистское воздействие в целях распространения мировоззрения, политических и духовных ценностей и идеалов западного мира;
— усиление международного сотрудничества на основе максимальной открытости сторон;
— низкий уровень политической, правовой и информационной культуры в обществе.

2) социально-экономические факторы:
— трудности переходного периода к рыночной экономике;
— инфляция и падение жизненного уровня населения, появление в стране слоя обездоленных;
— рост явной и скрытой безработицы;
— дезинтеграция прежней социальной структуры;
— разрушение многих форм общностей, выполняющих ранее функции законодателей норм и критериев оценки различных типов информационных воздействий;
— имущественная поляризация в обществе;
— рост депопуляции населения, превышение смертности над рождаемостью;
— эскалация преступности, алкоголизма и наркомании, проституции, криминализация общественных отношений;
— ухудшение показателей здоровья нации, угроза ее генофонду;
— рост межэтнической напряженности.

3) духовные факторы:
— кризис государственной идеологии, деформация системы норм, установок и ценностей и как следствие утрата критериев адекватной оценки информационно-пропагандистских воздействий;
— появление новых форм и средств воздействия на индивидуальное, групповое и массовое сознание, в том числе новых технологий СМИ, компьютерных технологий и т. п.;
— недооценка национальных и культурно-исторических традиций и проникновение в общественное сознание шаблонов западной массовой культуры;

— появление и рост новых форм мифологического сознания;
— деструктивная роль нетрадиционных религиозных конфессий, рост религиозного сектантизма и экстремизма;
— ослабление важнейших социокультурных институтов государства — науки, образования, воспитания и культуры;
— неразработанность системы этических норм в сфере информационной деятельности.

В целом можно отметить, что характерными чертами процесса информационно-психологической безопасности являются [1]:

— связь с состояниями, чувствами и переживаниями человека по поводу своей защищенности;
— обеспечение через полное или частичное ограничение доступа к вредоносной информации, которая имеет конкретные свойства (качества).

Обеспечение информационно-психологической безопасности в средствах массовой информации подразумевает, в первую очередь, психологическую безопасность индивида, включенного в массовую коммуникацию. А именно:

— свободу от попыток контроля сознания, морального давления, дискриминации;
— защиту психического здоровья от некорректного воздействия;
— контроль качества информации, исключение возможностей заведомого искажения реальности, фальсификации фактов, целенаправленного введения в заблуждение [2].

В общем виде психологические последствия влияния СМИ обычно связываются с понятием «эффективность СМИ». Западные исследователи массовой коммуникации, как правило, говорят не об эффективности, а об отдельных эффектах [3]. Анализ эффектов предполагает изучение трансформаций в оценках и поведении людей, происходящих под воздействием МК. На современные исследования по изучению информационных технологий на человека серьезное влияние оказали: Ф. Фентон, французский исследователь Г. Тард, ученые различных американских университетов (К. Ховленд, П. Лазарсфельд, С. Стауффер, Д. Уэплс, К. Левин). В настоящее время исследования

[1] *Рыдченко К. Д.* Понятие, сущность и содержание информационно-психологической безопасности // Административное право и процесс. 2009. № 4.

[2] Проблемы медиапсихологии. Материалы секции «Медиапсихология» Международной научно-практической конференции «Журналистика в 2000 году: Реалии и прогнозы развития» / Сост. Пронина Е. Е. М.: МГУ, 2001.

[3] *Богомолова Н.* Н. Социальная психология массовой коммуникации. М.: Аспект Пресс, 2008.

на обозначенную тему активно ведутся в Германии (медиапсихология, Винтер-Шпурк), Великобритании (политическая коммуникация, Лиллекер), США (социальное влияние, Ф. Зимбардо; психология влияния, Р. Чалдини), России (М. М. Вершинин, А. И. Соловьев, Г. В. Грачев, Н. М. Ракитянский, М. В. Гаврилова, Д. А. Леонтьев и др.).

Результаты многих научных исследований показывают, что влияние средств массовой коммуникации на человека может быть когнитивным (воздействовать на мышление и обучение), поведенческим или эмоциональным; что медиавоздействие может быть также прямым, непрямым, кратковременным, долговременным, перемежающимся или совокупным [4]. Таким образом, в основном, психологическое воздействие сообщений масс-медиа (эффект от информационного потока) осуществляется на когнитивные (познавательные), аффективные (эмоциональные) и поведенческие структуры человека (группы людей). Это, соответственно, находит свое отражение в психических процессах, состояниях и свойствах, которые актуализируются у аудитории при взаимодействии с данными материалами: формирование установок, расширение представлений людей, формирование чувств обеспокоенности, страха, влияние на моральное состояние и степень отчуждения в обществе, активизация (или отмена активизации) какой-либо деятельности и др.

При анализе информационно-психологической безопасности в масскоммуникационных ситуациях важен учет следующих критериев:

— доверие к информации: убедительная информация, дающая новые критерии и формы поведения;
— заинтересованность в/актуальность информации: информация, без наличия которой невозможно достижение цели системы;
— полнота информации: исключающая утрату любой части сведений об объекте; достоверность, доказанная научными методами;
— понятность/непротиворечивость информации: переформулирование исходных сведений в информацию, ясную для всех членов общества, читабельную, понятную и убедительно дающую новые алгоритмы и стереотипы поведения.

Во взаимодействии аудитории с материалами СМИ могут актуализироваться такие психологические защиты личности, как [5]:

---

[4] См., например: *Брайант Дж., Томпсон С.* Основы воздействия СМИ. М.: Изд. дом «Вильямс», 2004. 432 с.

[5] *Грачев Г. В.* Информационно-психологическая безопасность личности. М.: Изд-во РАГС, 1998. 125 с.

— уход: отключение от определенных каналов СМИ, от просмотра конкретных теле- и радиопрограмм, отказ от чтения некоторых газет, статей, рубрик и т. п.;
— блокировка (ограждение, преграда): повышение негативизма, критичности, эмоциональная отчужденность, также используются психологические барьеры, принижение источника (внутреннее осмеяние, развенчание авторитета и т. п.), невнимательность (отвлечение и переключение внимания на другие объекты, не связанные с содержанием воздействия) и т. д.;
— управление: изменение рейтинга популярности определенных каналов телевидения, сокращения или увеличения покупаемости периодических изданий и т. п.;
— затаивание (маскировка): отсрочка реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием (для последующего рационального и взвешенного анализа с привлечением дополнительных данных).

Следует отметить, что, несмотря на попытки выстроить всеобъемлющую теорию коммуникации, до сих пор существует дефицит теоретических психологических моделей, которые могли бы соответствовать уровню развития новых технологий, а также объяснить характер их социального и психологического воздействия на человека. Традиционно процессы коммуникации иллюстрируются множеством графических моделей (линейная, интерактивная, транзактная). Для описания же различных видов и уровней воздействия коммуникативных средств используются модели микро- и макроаналитического типа (модель когнитивной обработки Торнсона, модель медиазависимости М.Л. де Флера и С. Болла-Рокича, 1985; теория обработки социальной информации Фалка и Стенфилда, 1987; и др.) [1].

На кафедре политической психологии СПбГУ процесс массовой коммуникации изучается системно и комплексно: рассматриваются как сами медийные сообщения (с точки зрения их эффективности, содержательности, наполненности) во взаимосвязи с особенностями их презентации и выявления сопутствующих эффектов, так и особенности декодирования этих сообщений различными социальными группами [2]. В последние годы на кафедре активно ведутся теорети-

[1] См. об этом: *Брайант Дж., Томпсон С.* Указ. соч.; Психологическое воздействие в межличностной и массовой коммуникации // Под ред. А. Л. Журавлева, Н. Д. Павлова. Сер. Труды Ин-та психологии РАН. М., 2014. 400 с.

[2] *Анисимова Т. В., Самуйлова И. А.* Коммуникация как научное направление

ческие и эмпирические исследования оценки качества социально-политических сообщений (объективность, полнота, понятность, непротиворечивость, практичность и др.), циркулирующих в СМИ, как с точки зрения анализа их психологического содержания, так и с точки зрения изучения представлений аудитории.

Так, например, выявлены связи представлений аудитории СМИ о различных качествах социально-политических сообщений: 1) с психологическими защитами, которые актуализируются у человека в масс-коммуникационных ситуациях (избегание, управление, затаивание, блокировка); 2) с психическими состояниями (критичность, тревожность, напряженность, утомленность, любопытство, возмущение и др.); и 3) с другими критериями (потеря доверия к источнику информации, уменьшение способности конструктивного мышления и т. д.) [3].

Результаты проводимых эмпирических научных исследований показывают, что ощущение неполноты предоставляемой информации и невысокая степень доверия к сообщениям СМИ могут актуализировать стремление аудитории прервать контакт с информацией, чтобы оградить психику от нежелательного внешнего воздействия. Ясность информации для респондентов не исключает возможности формирования серии критических суждений о ней и ее распространителях, а также ее оценки как недостаточной, неправдоподобной, подрывающей доверие к носителям иной позиции [4]. Таким образом, мы видим, что аудитории СМИ сегодня отводится деятельная, целевая роль, являющаяся результатом коммуникативного процесса. Отношение к содержанию медийных текстов зависит от отношения к источнику информации и соблюдению правил презентации сообщений в условиях массовой коммуникации. По результатам проведенных теоретических и эмпирических исследований на факультете психологии СПбГУ разработана модель репрезентации российской политической коммуникации современными СМИ (2011), созданная на основе единства трех ключевых структурообразующих факторов: методологического, методического и практического [5].

политической психологии(по материалам доклада) // Вестник С.-Петерб. ун-та. Серия 16. Психология. Педагогика, 2015. № 1. С. 90–97.

[3] *Самуйлова И. А.* Психологические последствия репрезентации политической коммуникации в СМИ // Вестник С.-Петерб. ун-та. Серия 12. Вып. 1. 2011.

[4] Там же.

[5] *Анисимова Т. В., Кузнецова И. В., Самуйлова И. А.* Психологическое моделирование репрезентации российской политической коммуникации в современных СМИ // В мире научных открытий. 2011. № 11(23). С. 48–60.

Данная модель включает в себя следующие положения: 1) соблюдение психологических законов презентации социально-политической информации в СМИ; 2) соблюдение качества социально-политической информации, распространяемой в СМИ; 3) реализация социально-психологических функций политической коммуникации в СМИ; 4) психологические эффекты, производимые социально-политической информацией на индивидуальном и групповом уровнях; 5) психологические особенности аудитории СМИ; 6) степень соответствия социально-политической информации критериям информационно-психологической безопасности. Соблюдение психологических законов презентации социально-политической информации в СМИ предполагает, прежде всего, учет законов функционирования таких психических процессов, как восприятие, внимание, память, мышление [1]. Соблюдение качества социально-политической информации, распространяемой в СМИ, предполагает удовлетворение таких требований, как организованность, системность, конкретность, практичность, объективность, достаточность, понятность [2].

Реализация социально-психологических функций политической коммуникации в СМИ предполагает удовлетворение потребностей и мотивов обращения аудитории к материалам СМИ [3].

Психологические эффекты, производимые социально-политической информацией на индивидуальном и групповом уровнях, означают, что сообщение, передаваемое с помощью СМИ, может быть трансформировано как на индивидуальном, так и на групповом уровнях [4]. Это должно быть учтено в целях понимания последствий распространения социально-политической информации определенного содержания.

Психологические особенности аудитории СМИ (установки, отношение, интересы, типы и т. д.) трансформируют сообщения в соответствии с ее психологической структурой и во многом определяют восприятие, понимание, интерпретацию и воспроизведение информации.

---

[1] См. об этом, например: *Шерковин Ю. А.* Психологические проблемы массовых информационных процессов. М.: Мысль, 1973. 215 с.

[2] См.: *Юрьев А. И.* Введение в политическую психологию. СПб., 1992. 232 с.

[3] *Богомолова Н. Н.* Социальная психология массовой коммуникации. М.: Аспект Пресс, 2010. 191 с.

[4] См. об этом: *Назаров М. М.* Массовая коммуникация в современном мире: методология анализа и практика исследований. Ин-т социол. образования Рос. центра гуманитар. образования, Ин-т социологии Рос. акад. наук. 3-е изд., стер. М.: Едиториал УРСС, 2003. 239 с.

Степень соответствия социально-политической информации критериям информационно-психологической безопасности объясняет, в какой степени сообщению удалось преодолеть барьеры непонимания, недоверия, недостаточности и равнодушия к обсуждаемым в СМИ событиям. Обеспечение информационно-психологической безопасности предполагает организацию и осуществление защитных мер, которые в самом общем виде целесообразно выделить в следующие основные группы, характеризующиеся определенной организационной самостоятельностью и используемыми механизмами[5]:

1) регулирование, в частности, ограничение информационных потоков: введение определенных процедур проверки достоверности распространяемой информации (например, влияющей на принятие управленческих решений); ограничение распространения определенных сведений (например, способствующих возникновению агрессивных слухов, паники и т. д.) в чрезвычайных ситуациях; введение военной цензуры в условиях боевых действий и т. п.;
2) организация информационных потоков (в том числе инициирование распространения определенной информации): парирование (в первую очередь упреждающее) и нейтрализация воздействия определенных информационных факторов, которые могут психологически негативно воздействовать на людей (так, например, при возникновении слухов используется распространение сведений, нейтрализующих их влияние);
3) распространение способов и средств обработки и оценки информации: через системы образования, подготовки и переподготовки кадров, распространения социокультурных ценностей, традиций, социальных норм и т. д.;
4) формирование коллективной или групповой социально-психологической защиты: основывается на механизмах идентификации человека с определенными социальными общностями и объединениями людей и включенности в реальные социальные группы;
5) формирование индивидуальной психологической защиты или психологической самозащиты личности: в процессе приобретения

---

[5] *Грачев Г. В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС, 1998. 125 с.; *Самуйлова И. А.* Проявление феномена информационно-психологической безопасности в политической коммуникации // От истоков к современности: 130 лет организации психологического общества при Московском университете: Сборник материалов юбилейной конференции: В 5 тт. Т. 2. / Отв. ред. Богоявленская Д. Б. М.: Когито-Центр, 2015. Т. 1. 473 с., 2015. Т. 2. С. 454–456.

опыта информационно-коммуникативного взаимодействия (в том числе обучения с использованием специализированных форм психологической подготовки, проведения тренинговых занятий по специально разработанным методикам).

Первые две из указанных выше групп защитных мер связаны с изменением «внешней» для личности информационной среды. Последующие три определяются изменением механизмов и способов взаимодействия человека с «внешней» информационной средой. Из рассмотренных выше направлений обеспечения информационно-психологической безопасности личности первые четыре зависят от внешних для человека условий, деятельности других социальных субъектов, функционирования различных социальных институтов, других людей. Пятое направление в первую очередь зависит от самой личности. В обеспечении должного уровня информационно-психологической безопасности заинтересованы не только личность и конкретные социальные группы, но и государство в целом, так как ущерб последнему причиняется через нанесение вреда первым двум.

Глава 5. Моделирование процессов противодействия информационно-психологическим операциям

Информационно-психологическая безопасность, будучи одним из аспектов информационной безопасности, обособилась как отдельная предметная область в проблематике информационной безопасности. Но лишь в новой «Доктрине информационной безопасности Российской Федерации» [1]в пункте 12 информационно-психологические воздействия явно сформулированы в составе второго по порядку из девяти комплексов угроз, что указывает на важность отводимого им места в системе угроз. Понятно, что данный термин подразумевает не только узкоспециальные методы и средства, а широкий спектр разнообразных воздействий на психологическое состояние, как на индивидуальном, так и групповом уровне. Наряду с нижним, собственно психологическим аспектом сюда, надо полагать, включаются трудно определяемые и не измеряемые, но объективно существующие и крайне важные аспекты безопасности, выражаемые на ментальном, интеллектуальном, культурном, аксиологическом, духовном уровнях. Нельзя сюда не включить и так называемый «человеческий фактор», собирательный термин, обозначающий комплекс угроз безопасности в человеко-машинных, социо-технических системах, связанный с разнообразными проявлениями поведенческих особенностей людей во взаимодействии с технологической средой. Вместе с тем, хотелось бы отметить, что даже такое внимание не вполне отражает системный характер информационно-психологического аспекта в широком

[1] Доктрина информационной безопасности Российской Федерации // Российская газета. 2016, 6 декабря.

смысле этого слова. Все аспекты информационной безопасности проявляются в поведении людей, то есть в психологической сфере, и наоборот, психологическое состояние общества, коллектива, индивида оказывает влияние на все остальные сферы деятельности. Это естественно, поскольку понятие безопасности субъективно по своей природе [1], вне контекста человеческой деятельности вряд ли имеет смысл, а все ее результаты есть продукт коммуникаций, осуществляемых исключительно по информационным каналам, даже если имеют материальное воплощение.

В самом деле, экономические диверсии вполне могут быть инспирированы информационными провокациями панических настроений, террористическая деятельность по своей сути направлена на психологическое подавление властей и общества, моральное состояние вооруженных сил непосредственно влияет на обороноспособность, снижая боевой потенциал даже при материально-техническом превосходстве. Этот ряд очевидных примеров легко можно продолжить. Причем аналогичные явления не обязательно рассматривать в глобальном масштабе, их вполне можно редуцировать в иных терминах на более низкий, например, корпоративный уровень. Скажем, неудовлетворенность своим статусом администратора информационной системы роковым образом может повлиять на безопасность информационных активов и, соответственно, экономическое положение организации.

Если абстрагироваться от деталей, то все риски нарушения безопасности имеют системный техно-гуманитарный характер, в связи с чем уместно еще раз обратиться к положениям принятой «Доктрины информационной безопасности», которая в своем первом пункте определяется именно как «*система* официальных взглядов на обеспечение национальной безопасности», а не «*совокупность*», как в прежней версии.

Во-первых, информационно-психологической безопасность предстает как не вполне определенная система взаимодействий и взаимовлияний разнородных факторов с многочисленными обратными связями, что в результате может дать неожиданные эффекты как в информационно-психологической сфере, так и в любой другой. Поэтому для исследования данной проблематики необходим адекватный ее сложности методический аппарат и инструментарий, которые способны учесть неопределенность и разнородность исходной информации, давая обоснованные метрически сравнимые оценки всему спектру угроз. Только тогда, имея оценку

---

[1] *Иващенко Г. В.* О понятии «безопасность» // Теоретический журнал CREDO. 2000. № 24(6). URL: http://www.credo.osu.ru/024/004.shtml, www.orenburg.ru/culture/credo/

их значимости, можно будет целенаправленно и эффективно противодействовать им, причем не исключено, что, решая информационно-психологические проблемы, придется искать их решение в техносфере, и, наоборот, технические или иные, далекие от гуманитарной сферы вопросы найдут свое решение именно в ней. При этом нельзя забывать и иметь методическую возможность учитывать то обстоятельство, что любые меры противодействия угрозам могут иметь двойственный характер в том смысле, что их применение способно одновременно с желаемым результатом по отношению одних факторов вызвать негативные последствия относительно других [2].

Во-вторых, есть еще одно направление, которому пока не уделяется достаточного внимания в теоретическом осмыслении и на практике, что связано с преобладанием «защитного» подхода к обеспечению информационной безопасности. Ее проблемы по-прежнему рассматриваются преимущественно с позиций безопасности информации, которая часто сводится к еще более узкой проблематике — практическим вопросам защиты информации. Для подтверждения этого тезиса достаточно посмотреть перечень специальностей по направлению «Информационная безопасность», в котором преобладает слово «защита». Вопросы защиты «от информации», которые долго оставались на втором плане, конечно, расширяют круг проблем, неизбежно включая сюда и проблематику информационно-психологической безопасности, но в целом подходы к обеспечению безопасности остаются все же преимущественно оборонительными.

Однако за последние годы сложилась тенденция: обеспечение информационной безопасности на различных ее уровнях и в разных аспектах приобретает черты противоборства и становится непрерывным процессом. Ориентация лишь на защиту ресурсов становится недостаточной для поддержания безопасности, технология ее обеспечения требует уже тех или иных атакующих или упреждающих воздействий на потенциального противника. Это обусловлено тотальной информатизацией социо- и техносферы, всех систем обеспечения жизнедеятельности и управления, самого образа жизни подавляющей части населения, перевод конфликтов в информационное пространство. Даже ставший тривиальным сетевой

[2] *Шишкин В. М.* Двойственность средств обеспечения безопасности и оценка их конечной результативности // Анализ, моделирование, управление, развитие экономических систем: сборник научных трудов IX Международной школы-симпозиума АМУР-2015, Севастополь, 12–21 сентября 2015 / Под ред. А. В. Сигала. Симферополь: ТНУ им. В. И. Вернадского, 2015. С. 416–421.

криминал можно интерпретировать как социотехническое противоборство, а так называемые «информационные войны» глобального уровня вполне могут быть масштабированы до межкорпоративных конфликтов. При этом информационная и материальная, гуманитарная и технологическая составляющие конфликтов стали неразрывно связанными, из чего следует, что мы имеем дело с процессами, которые могут быть описаны и исследованы в терминах динамических моделей.

Итак, первое из обозначенных направлений связано с выявлением профиля риска, т. е. определением и оценкой значимости некоторого спектра разнородных угроз, не обязательно лежащих в информационно-психологической сфере, с целью выработки наиболее эффективных мер противодействия, и соответствующие данной предметности модели будут сводиться к дискретному оцениванию. Второе направление– это моделирование непрерывных процессов во времени с целью выявления некоторых качественных тенденций или закономерностей, проверки сценариев при вариации начальных условий, коэффициентов, пространства фазовых переменных, представляющих разнородные факторы.

Оба эти направления, внешне разные (в одном случае — оценка состояния, в другом — наблюдение процесса), объединяет то, что объектом исследования являются слабо структурированные, трудно формализуемые системы с разнородными элементами и плохо измеряемыми показателями. Объединительным для указанных подходов может являться также используемое в англоязычной литературе понятие «Holistic security» (*букв.* «безопасность целостного», т. е. подход, ориентированный на интеграцию всех элементов, предназначенных для защиты организации, рассматривая их как сложные и взаимосвязанные системы) [1].

Разумеется, обозначенные вопросы активно изучаются, обсуждаются, но чаще их анализ сводится к вербальным рассуждениям, не допускающим объективной оценки, когда на всякое обоснованное мнение найдётся другое не худшее и не менее обоснованное. Таким образом, есть потребность в применении формального аппарата, позволяющего если не сформулировать тот или иной вывод или обосновать рекомендацию, то, по крайней мере, согласовав базовые утверждения модели, объективно проверить результаты экспериментов на ней для различных сценариев и начальных условий. Ниже представленные модели в какой-то мере удовлетворяют эти требованиям, показав в эксперименте правдоподобные

[1] См. подробнее: http://www.whatis.techtarget.com/definition/holistic-security.

результаты и потенциальную применимость в исследовании проблем информационно-психологической безопасности и смежных вопросов.

Модель анализа рисков. Понятие риска неоднозначно и имеет множество различных, порою не совпадающих, определений в различных предметных областях. Для пояснения особенностей нашей модели и важности для нее структурной составляющей заслуживают внимание два варианта («двухмерный» и «трехмерный») предельно простой абстрактной математической модели риска [2], в которую укладываются практически все его разумные определения.

Согласно первому варианту риск $\tilde{R} = \left(\mu_1, \tilde{H}_R\right)$, есть пара, где μ_1 — мера частоты (вероятности) событий риска, и $\tilde{H}_R$ – оценка ущерба. Большинство определений риска представляют этот вариант, связывая вероятность наступления события риска, т. е. события, наступление которого непосредственно производит ущерб, и его величину. Не будем здесь обращать внимание на то, что чаще всего в практических расчетах игнорируется зависимость этих событий и, соответственно, необходимость учета их корреляции, оценить которую далеко не всегда возможно, но без чего полученные оценки окажутся некорректными.

Важнее другое обстоятельство: если оценка риска не самоцель, а средство выявления факторов, не обязательно являющихся событиями риска, но косвенно их порождающих, и противодействие которым позволит снизить риск наиболее эффективным образом. В таком случае необходимо оценивать уже не собственно события риска, а элементы некоторой структуры факторов, которые к ним приводят. Похожая ситуация возникает, если событие риска редкое, и вероятность μ_1 стремится к 0, либо ее трудно получить или обосновать. Тогда вводится еще один компонент μ_2, косвенно закладывающий вероятность события риска в структуре предшествующих событий или сценариев, определенных тем или иным способом, и тогда $\tilde{R} = \left(\mu_1, \mu_2, \tilde{H}_R\right)$.

Данная модель представляет последний вариант, где риск определяется, прежде всего, на основе системы факторов, предшествующих

---

[2] *Северцев Н.* А. Безопасность и защита сложных систем. М.: ТНУ им. В. И. Вернадского, 2015. С. 416–421.

возникновению событий риска, которые образуют произвольно сложную связную причинно обусловленную структуру, являющуюся разновидностью так называемых когнитивных карт [1], ориентированной, в отличие от большинства случаев их применения, на количественный анализ ситуаций и получившей некоторое физическое обоснование применимости.

Одной из методических основ разработки послужило структурное моделирование, в частности, в ней можно усмотреть некоторую внешнюю аналогию с методом путевого или причинного анализа [2]. В то же время в ней много общего с так называемым когнитивным моделированием [3], получившим существенное развитие в работах Института проблем управления РАН. Рассмотрим метамоделирование как построение причинно-обусловленных структур, допускающее в качестве интерпретаций различные математические модели. Метамодель [4] построена на дихотомической оппозиции: «защищаемый объект» — потенциально враждебная «среда». Использование универсального субъектно-объектного подхода позволило минимизировать число классов факторов риска, ограничив их источниками угроз (субъектами воздействия на объект защиты), компонентами объекта и угрозами его безопасности, определяемыми как события, через реализацию которых прямо или косвенно осуществляется воздействие на объект, приводящее к ущербу для его безопасности. Процесс рискообразования тогда может быть сведен к потокам событий, генерируемых источниками угроз, на произвольно сложной причинно обусловленной структуре (сети) факторов риска. Таким образом, выделяются три непересекающихся непустых подмножества факторов риска:

— независимые активные субъекты, «источники угроз» — множество M_s (threat sources);

— проводники воздействий, события, порождаемые источниками угроз, «угрозы» нарушения безопасности — множество M_e(threat

---

[1] *Плотинский Ю. М.* Модели социальных процессов. Учебн. пособие для высш. учебных заведений. Изд. 2-е, перераб. и доп. М.: Логос, 2001. 296 с.

[2] *Хейс Д.* Причинный анализ в статистических исследованиях. М.: Финансы и статистика, 1981. 354 с.

[3] *Авдеева З. К., и др.* Когнитивный подход в управлении // Проблемы управления. 2007. № 3. С. 2–8.

[4] *Шишкин В. М.* Метамодель анализа, оценки и управления безопасностью информационных систем // Проблемы управления информационной безопасностью: Сборник трудов ИСА РАН; под ред. Д. С. Черешкина. М.: Едиториал УРСС, 2002. С. 92–105.

events), в котором выделяется подмножество $M_r \subseteq M_e$ так называемых «событий риска» — угроз, наносящих непосредственный ущерб объекту;

— «компоненты» объекта — множество M_c (components).

Кроме того вводится условный элемент, представляющий множество состояний объекта в целом — z.

В совокупности все они образуют множество M_0, на котором определяется хотя бы один тип отношений: бинарное отношение непосредственной причинности ρ_w со свойством транзитивности, к которому можно свести многие связи, имеющие импликативный характер. Отношение ρ_w упорядочивает M_0 и задает на нем структуру, фиксирующую каналы распространения потоков угроз от источников до объекта, отображающихся, в конечном счете, на его состоянии, и порождает квадратную матрицу отношения W_0.

Отметим, что сложность образуемой таким образом структуры за счет отсутствия каких-либо ограничений для отношения ρ_w на множестве M_e, кроме запрета рефлексии, может быть очень высокой, формально почти до состояния полного графа, что позволяет моделировать очень сложные объекты.

Роль условного элемента z, соответствующего состоянию объекта в целом, как преобразователя, ограничивается функцией сумматора-интегратора. Тогда на выходе z можно фиксировать результирующий поток $f_z(t)$, интеграл от которого по некоторому интервалу времени является, по сути, мерой риска для объекта, измеряемого ущербом в относительном исчислении, наносимым ему за это время.

Простейшая количественная интерпретация метамодели позволяет отобразить ее в арифметическую матрицу $W = (w_{ij}), \sum_i w_{ij} = 1$, элементы которой можно рассматривать как нормированные весовые коэффициенты в точечном выражении, имеющие смысл меры влияния i-го фактора на j-ый.

В таком случае для каждой пары факторов (i, j) отношения ρ_w должен существовать поток $f_{ij}(t)$ i-ых событий-причин, непосредственно вызывающих события-следствия j, и для каждого потока $f_{ij}(t)$ на некотором

интервале времени T можно будет получить интегральную характеристику $F_{ij}(T)$– количество событий или интеграл от $f_{ij}(t)$ по t для непрерывных моделей потоков, а для каждого j определяется доля или вес $w_{ij} = F_{ij}(T) / \sum_i F_{ij}(T)$, $w_{ij} \in (0,1)$, $\sum_i w_{ij} = 1$, для всех предшествующих i-ых событий как непосредственных причин возникновения события j, которые фактически можно считать оценками статистических вероятностей p_{ij} того, что событие i является причиной события j. При этом w_{ij} оказываются независимыми от интегральных характеристик потоков, предшествующих всем данным i-ым событиям и следующих за j-ым. При таких условиях наша структура имеет право быть интерпретирована как Марковская цепь с поглощающими состояниями, а веса w_{ij} как переходные вероятности p_{ij}, и для расчетов становится применим соответствующий математический аппарат.

Ничего не изменится в определении весов и в случае нелинейного изменения интенсивности потоков на данной паре относительно тех, что были до или будут после нее. Принципиальных отличий не возникнет также, если действие двух или более i-ых факторов на j-ый связаны конъюнкцией, а не только дизъюнктивно — очевидно, соответствующие веса просто будут равными.

Далее рассчитываются показатели v_{ij}, аналогичные по смыслу w_{ij}, но уже с учетом транзитивности отношения ρ_w. В результате определяется арифметическая матрица V, структурно эквивалентная W, согласно матричному преобразованию $V = (I - W)^{-1} - I$, где I — единичная матрица. Последний, всегда не нулевой, z-ый столбец v_z матрицы V содержит искомые показатели $\{v_{iz}\}$ влияния любого i-го фактора риска на состояние безопасности объекта, которые согласно нашему определению представляют профиль риска.

Однако, хотя потоки событий $f_{ij}(t)$объективно существуют, их явная идентификация в сложных гетерогенных структурах проблематична. Тем не менее, поскольку интегральные характеристики $F_{ij}(T)$ определяют значения весовых коэффициентов w_{ij}, но не способ их

идентификации, можно попытаться решить своего рода обратную задачу и, используя любую доступную информацию, их идентифицировать, не связывая себя ограничениями по форме ее представления. Последнее замечание важно, так как процедура извлечения экспертных знаний должна быть максимально комфортной с автоматизированным переводом полученной информации в состояние исходных данных.

Кроме оценок экспертов, преимущественно неколичественных, одновременно при желании можно указать точные арифметические значения w_{ij}, использовать для их определения статистические характеристики, результаты аналитических расчетов и т. д. Допускается частичное или полное отсутствие каких-либо мнений или данных. Спектр представления оценок достаточно разнообразен и может быть расширен. Однако все отмеченное разнообразие представления исходной информации о весовых коэффициентах w_{ij} сводимо к распределениям вероятностей их значений [1], и вся полученная информация может быть в этом смысле гомогенизирована. В результате происходит идентификация w_{ij} уже как зависимых случайных величин $\tilde{w}_{ij}$, связанных в реализациях условием $\sum_i w_{ij}^* = 1$, а числовая матрица W определяется как случайная $\tilde{W}$. Далее, выполняя на ее реализациях указанное выше преобразование $W \to V$ как на обычной числовой матрице, обеспечивается рандомизация V с получением в итоге на множестве реализаций $\tilde{V}$ стохастических оценок профиля риска. Существенным обстоятельством, повышающим применимость данного подхода, является то, что указанный результат, матрицу $\tilde{V}$, можно получить и без трудоемкой непосредственной оценки w_{ij}, определив лишь структуру модели [2].

Таким образом «обратная» задача будет решена, однако необходимо учитывать, что необходимым условием возможности получения стохастических оценок по данной методике является требование

---

[1] *Шишкин В. М.* О возможности получения стохастических оценок по неполной гетерогенной информации // Надежность и качество 2013: труды Междунар. симпозиума: в 2 т. / Под ред. Н. К. Юркова. Т. 1. Пенза: Изд-во ПГУ2013. Т. 1. С. 82–86.

[2] *Шишкин В. М.* Оценка вероятностей угроз по структурной информации при экспертном оценивании // 14-я Междунар. научная школа «Моделирование и анализ безопасности и риска в сложных системах (МАБР-2016)». Материалы, Санкт-Петербург, 25–28 октября 2016. СПб., 2016. С. 197–202.

объективной случайности, в теоретико-вероятностном смысле этого слова, исходных величин. Только в таком случае, независимо от того, как будет представлена информация о них и каким образом она будет преобразовываться для получения результирующих показателей, их стохастическое представление можно считать правомерным. Таким требованиям, безусловно, отвечает рассматриваемая предметная область, где явления, события связаны с поведением людей и поэтому заведомо имеют массовый недетерминированный характер, следовательно, необходимое условие применимости выполняется.

Методика реализована в составе автоматизированной системы и кроме применения в более привычных задачах преимущественно технического характера, например [1], показала применимость для анализа неспецифических для нас вопросов, в частности, социально-психологических аспектов обеспечения национальной безопасности [2] и эпидемиологических рисков [3]. В качестве небольшой иллюстрации использования методики приведем некоторые результаты, полученные на раннем этапе ее развития применительно к анализу только что тогда принятой «Доктрины информационной безопасности» в первой версии 2000 г. и оценку итогов её выполнения с позиций сегодняшнего дня [4]. Несмотря на некоторую условность количественных исходных данных, что определялось экспериментальным характером проделанной работы [5], эта версия Доктрины оказалась вполне конструктивной и показала возможность использования

---

[1] *Гатчин Ю. А., Савков С. В., Шишкин В. М.* Риск-модель угроз безопасности персональных данных // Труды конгресса по интеллектуальным системам и информационным технологиям «IS&IT'11». Научн. изд. в 4-х тт. М., 2011. Т. 2. С. 344–350.

[2] *Шишкин В. М.* Средства системной оценки гетерогенных угроз и контрмер // Социально-психологические аспекты обеспечения национальной безопасности: материалы Междунар. науч.-практ. конф., Минск, 3–4 декабря 2015 года: в 2-х т. / Ин-т нац. безопасности Республики Беларусь; редкол.: С. Н. Князев (гл. ред.) [и др.]. Минск, 2016. Т. 2. С. 113–116.

[3] *Шишкин В. М.* Автоматизированная система риск-анализа в эпидемиологии и терапии социально-значимых заболеваний на базе технологии CUDA // Тезисы докладов IV Всероссийской конференции «Математическое моделирование и вычислительно-информационные технологии в междисциплинарных научных исследованиях» (Иркутск (Россия), 30 июня — 4 июля 2014 г.). Иркутск, 2014. С. 74.

[4] Доктрина информационной безопасности Российской Федерации. 9 сентября 2000 г. № Пр-1895. URL: http://www.scrf.gov.ru/Documents/Decree/09–09.html.

[5] *Шишкин В. М., Юсупов Р. М.* «Доктрина информационной безопасности Российской Федерации» — опыт количественного моделирования // Труды СПИИРАН. 2002. Вып. 1. Т. 1. С. 65–78.

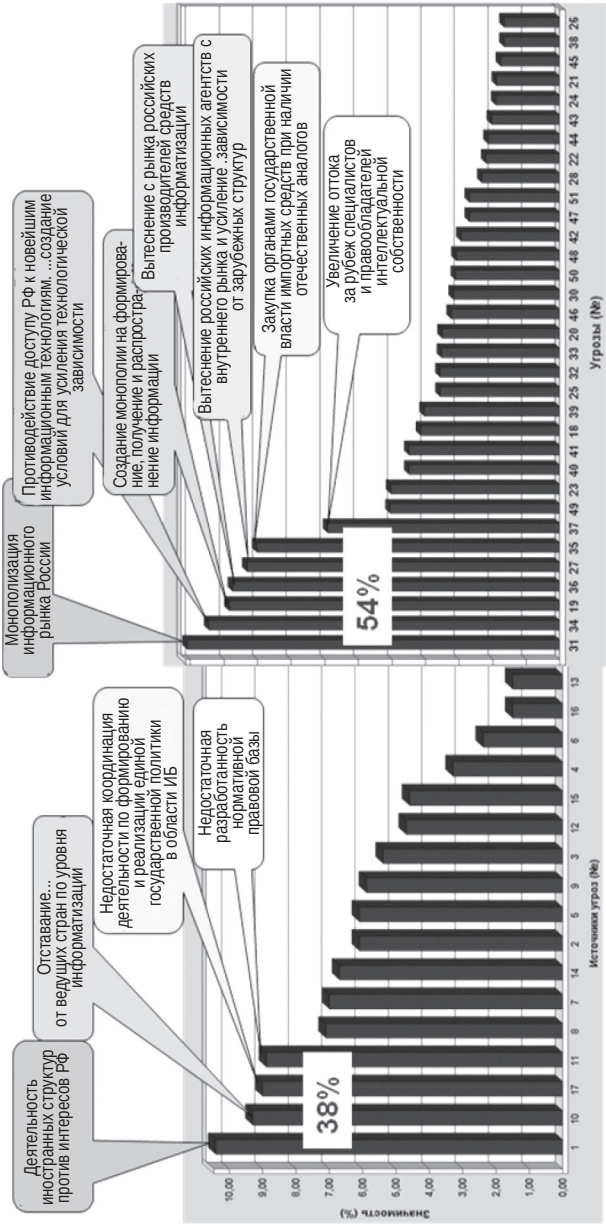


Рис. 29. Оценка значимости факторов, угрожающих национальным интересам в информационной сфере («Доктрина» – 2000 г.)

разработанных средств для решения подобных слабо структурированных задач. На рис. 29 показаны результаты расчета профиля риска для национальных интересов в информационной сфере в формулировках источников угроз и угроз согласно «Доктрине», как это виделось в 2000 г.

Список наиболее значимых факторов оказался довольно правдоподобен, хотя исходные данные использовались весьма приблизительные. Это обстоятельство свидетельствовало, с одной стороны, о том, что «Доктрина» достаточно полно представляла рассматриваемую проблему, а с другой — о применимости использованной для расчетов модели.

В связи с принятием новой «Доктрины» в конце 2016 г. возникло естественное желание сравнить априорную и апостериорную оценки [1], прежде всего результативность контрмер, предусмотренных в прежней версии «Доктрины», поскольку тогда обнаружилось несоответствие значимости факторов риска и результативности контрмер.

Для чистоты сравнения оценка и расчет были проведены на той же модели, в той же среде, не вдаваясь в содержательный анализ и не касаясь последствий революционных изменений в сфере ИКТ, которые произошли за прошедшее время и многое изменили в сфере информационной безопасности. На рис. 30 показано, как видится результативность контрмер в настоящее время.

Разница между верхней и нижней диаграммами невелика. Возможно, потому, что в 2000 г. экспертные оценки прогноза результативности выполнения «Доктрины-2000» были умеренно-пессимистические, а в настоящее время, учитывая разницу в психологической обстановке, наоборот, умеренно-оптимистические. Однако в совокупности формальная оценка итогов довольно правдоподобна, результативность некоторых контрмер снизилась с учетом появления новых факторов риска и негативных эффектов контрмер, других — повысилась, интегральная оценка результативности также несколько увеличилась. Поэтому можно считать, что «Доктрина» в целом выполнена. Разумеется, высокую оценку ее выполнения не следует понимать как решение проблем информационной безопасности. Новые проблемы, новые угрозы будут возникать постоянно, и не исключено, что если аналогичный анализ провести для текущего состояния, факторы информационно-психологического характера окажутся наиболее значимыми.

---

[1] *Шишкин В. М.* Доктрина информационной безопасности Российской Федерации — ретроспектива и перспектива // Проблемы информационной безопасности: Труды III Международной научно-практической конференции, Симферополь–Гурзуф, 16–18 февраля 2017 г. Симферополь: ИП Зуева Т. В., 2017. С. 17–18.

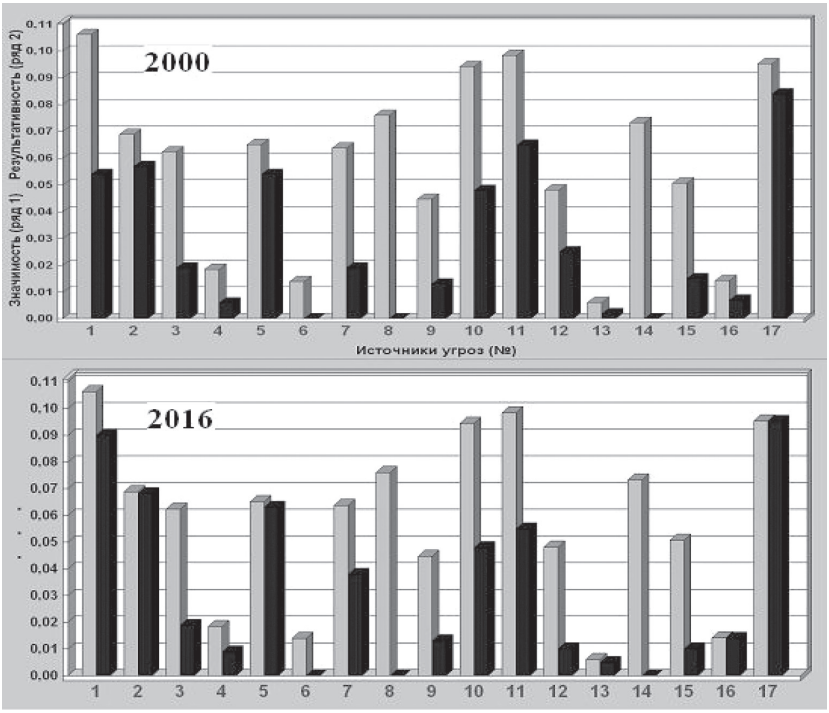


Рис. 30. Соотношения оценок значимости источников угроз и результативности контрмер: итоги

Динамическая модель противоборства. Ранее для исследования взаимодействия развития информационно-коммуникационных технологий (ИКТ) и национальной безопасности (НБ) в качестве эксперимента нами была разработана динамическая модель [2]. Ее основой послужила схема из опубликованной еще раньше работы [3], иллюстрировавшей вербальный анализ процессов взаимодействия развития ИКТ и обеспечения НБ через систему других, разнонаправленно действующих факторов. Даже на такой образной схеме можно было увидеть, что при отсутствии

[2] *Шишкин В. М., Абросимов И. К.* Динамическая модель системы взаимодействия развития ИКТ и обеспечения национальной безопасности // Региональная информатика и информационная безопасность. Сб. трудов. 2015. Вып. 1. С. 230–235.

[3] *Юсупов Р. М., Шишкин В. М.* О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. 2008. Вып. 6. С. 11–23.

сбалансированности составляющих процесса, недооценке угроз, учитывая опосредованные обратные связи, национальной безопасности и в целом социально-экономическому развитию может быть нанесен ущерб.

В первом приближении при разработке модели следует исходить из того, что многие системы, изменение состояния которых согласовано с законами сохранения, могут быть описаны на языке обыкновенных дифференциальных уравнений [1]. Концептуально эту модель можно отнести к классической традиции, заложенной, в частности, работами Дж. Форрестера и Н. Н. Моисеева в области глобальной динамики. С использованием дифференциальных моделей исследовались также вопросы взаимодействия науки и национальной безопасности [2].

Результаты моделирования показали правдоподобное поведение, допускающее содержательные интерпретации. В частности, подтвердилось предположение, что уровень безопасности при угнетении одной из подсистем в пользу другой — обеспечения безопасности или социально-экономического развития, падает при деградации обеих подсистем. Тем самым была еще раз подтверждена возможность применения аппарата обыкновенных дифференциальных уравнений для исследований не только физических или технических объектов, но и для анализа процессов, происходящих в плохо формализуемых системах.

Далее, учитывая отмеченную выше тенденцию к противоборству, на ее основе появилась новая модель, состоящая из двух симметричных автономных противоборствующих систем, аналогичных исходной, но взаимодействующих и управляемых. Модель масштабируема, и без изменения структуры, вложив специфический содержательный смысл в некоторые фазовые переменные, ее можно интерпретировать в широком диапазоне от межгосударственного взаимодействия до, например, внутрикорпоративного уровня или в терминах какой-либо предметной области.

В текущей версии модель представляет собой систему из двенадцати дифференциальных уравнений первого порядка, из которых два описывают динамику использования ресурсов противоборствующих сторон, а остальные десять — фазовых переменных каждой стороны [3]. Система

---

[1] *Моисеев Н. Н.* Универсум. Информация. Общество. М., 2011. 200 с. С. 39.

[2] *Юсупов Р. М.* Наука и национальная безопасность. 2-е изд. СПб.: Монография. 2-е изд., перераб. и доп. СПб.: Наука, 2011. 369 с.

[3] *Шишкин В. М., Колесников К.* В. Исследование динамики симметричного противоборства на дифференциальной модели // Проблемы информационной безопасности: Труды III Международной научно-практической конференции, Симферополь–Гурзуф, 16–18 февраля 2017 г. Симферополь: ИП Зуева Т. В. С. 68–69.

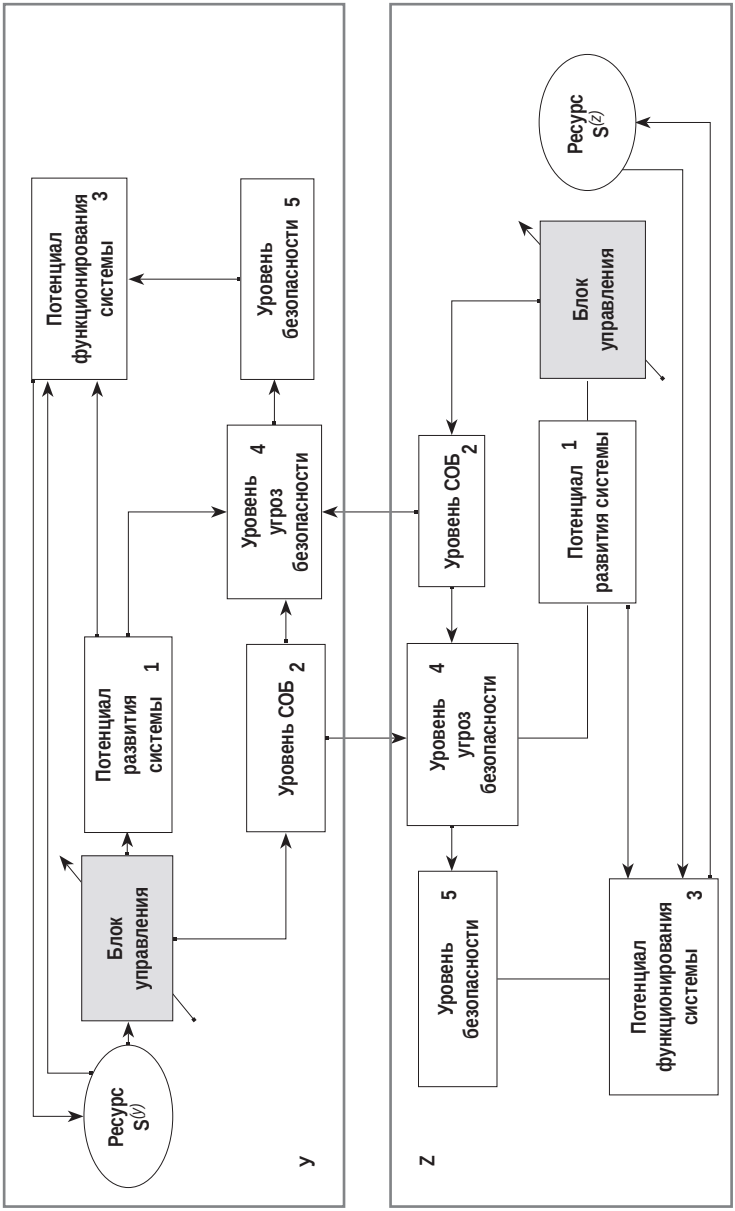


Рис. 31. Структурная схема динамической модели противоборства

управления представлена автономными блоками управления, которые функционируют независимо в соответствии с собственными целями. Блок управления состоит из двух элементов «Решающего устройства», в котором содержится вся логика управления, и «Исполнительного устройства», которое выполняет функцию распределения ресурса между потребляющими переменными. Логика управления строится, исходя из цели управления, и заключается в распределении ресурсов на поддержание уровня соответствующих факторов.

Ресурс понимается в обобщенном, комплексном смысле. Однако в зависимости от назначения и масштаба модели он может пониматься более конкретно, например, как информационный ресурс, включающий не только традиционное содержание, но и технологический, энергетический, кадровый, инфраструктурный ресурсы. В абстрактных универсальных терминах структурная схема модели показана на рис. 31 (аббревиатура СОБ на ней обозначает систему обеспечения безопасности).

Модель состоит из двух симметричных систем Y и Z, которые имеют элементы влияния друг на друга. Фазовые переменные системы y_i и z_i с индексами, соответствующими индексам блоков на схеме, $i = \overline{1,5}$, представляют стороны Y и Z. Переменные $S^{(y)}, S^{(z)}$ представляют ресурсы сторон.

Каждое уравнение строится по следующей схеме:

- в левую часть помещается производная данной фазовой переменной;
- правая часть представляет собой линейную комбинацию постоянных коэффициентов, фазовых переменных и их производных, тех, которые влияют на динамику данной переменной (знаки задаются в уравнениях); допускается, что переменная может влиять на свою динамику;
- если на динамику данной переменной влияет ресурс, то в правую часть добавляется ещё одно слагаемое, которое является произведением количества ресурсов на множитель, который показывает долю ресурса, идущего на данную переменную.

Математическая модель, соответствующая структурной схеме на рис. 29, может быть представлена следующей системой уравнений:

$$\dot{y} = P^T_{(y)} y + Q^T_{(y)} \dot{y} + r^T_{(y)} s^{(y)} + P^T_{(zy)} z,$$

$$\dot{z} = P^T_{(z)} z + Q^T_{(z)} \dot{z} + r^T_{(z)} s^{(z)} + P^T_{(yz)} y,$$

$$\dot{s}^{(y)} = -k^{(y)} s^{(y)} + g^{(y)} y_3,$$

$$\dot{s}^{(z)} = -k^{(z)} s^{(z)} + g^{(z)} z_3,$$

где y, z — вектора фазовых переменных, в качестве которых выступают элементы указанной структурной схемы с соответствующими ей индексами;

$P = \{p_{ij}\}$ — матрица, в которой p_{ij} — коэффициенты влияния y_i на динамику y_j, для $i \neq j$, а на главной диагонали расположены собственные потенциалы i-го фактора p_i (считается, что элемент деградирует, и все коэффициенты p_{ij}, где $i = j$ имеют знак минус);

$Q = \{q_{ij}\}$ — матрица, в которой q_{ij}– коэффициенты влияния динамики y_i на динамику y_i, $i \neq j$, $q_{ii} = 0$;

P_{zy}, P_{yz} — коэффициенты влияния симметричных систем Y и Z друг на друга;

$r_{(y)} = \{r_j^{(y)}\}_{1\times5}, r_j^{(y)} \geq 0$ — коэффициенты, определяющие долю ресурса $S^{(y)}$, идущую на восстановление уровня переменной y_j;

$r_{(z)} = \{r_j^{(z)}\}_{1\times5}, r_j^{(z)} \geq 0$ — коэффициенты, определяющие долю ресурса $S^{(z)}$, идущую на восстановление уровня переменной z_j;

$k^{(y)}, k^{(z)}$ — коэффициенты, определяющие скорость расходования ресурсов;

$g^{(y)}$, $g^{(z)}$ — доля продукта, производимого потенциалом развития системы, идущая на восстановление ресурсов.

С учетом содержательного смысла коэффициентов на них накладываются следующие ограничения:

$$(q_{ij}^{(y)})^2 + (p_{ij}^{(y)})^2 \neq 0; (q_{ij}^{(z)})^2 + (p_{ij}^{(z)})^2 \neq 0; \sum_{j=1}^{5} r_j^{(y)} 1; \sum_{j=1}^{5} r_j^{(z)} 1;$$

$$\sum_{j=1}^{5} r_j^{(y)} k^{(y)}; \sum_{j=1}^{5} r_j^{(z)} k^{(z)}; k^{(y)}, k^{(z)}, g^{(y)}, g^{(z)} > 0.$$

Смысл ограничений заключается в том, что каждая из сторон не может распределить ресурсов больше, чем у нее есть сейчас, и что коэффициент скорости расходования ресурсов больше или равен сумме всех долей распределенного ресурса. Определены три различных варианта критериев управления: подавление, доминирование и паритет. Формально каждая из целей задается следующим образом:

$$F_{пар}(t) = \left| y_5(t) - z_5(t) \right| < \delta,$$
$$F_{дом}(t) = y_5(t) - z_5(t) > \delta,$$
$$F_{под}(t) = z_5(t) < \delta,$$

где, $y_5(t)$ — уровень безопасности системы, применяющей стратегию;

$z_5(t)$ — уровень безопасности системы противника;

δ — пороговое значение, задаваемое пользователем $\delta \geq 0$.

Стратегия будет считаться выигрышной, если ресурс системы не исчерпан, и наоборот, если система потеряла все свои ресурсы, то ее стратегия считается проигрышной.

На данной модели была проведена серия вычислительных экспериментов при различных комбинациях стратегических целей (критериев управления) сторон, результаты которых позволяют ее поведение оценивать как правдоподобное и сделать некоторые полезные выводы.

Приведем один характерный пример, иллюстрирующий динамику взаимодействия сторон, одна из которых применяет стратегию доминирования, а другая — паритета. На рис. 32 показаны траектории для двух переменных — уровня ресурса (левый график) и уровня безопасности (правый), темная линия на графиках относится к стороне Y.

Очевидно, что при равных начальных условиях сторона, выбравшая агрессивную стратегию, полностью подавляет сторону, выбравшую пассивную, миротворческую цель. Стоит обратить внимание также на тот требующий осмысления факт, что уровень безопасности «победившей» стороны со временем после «победы» и его бурного роста в этой фазе в дальнейшем стремительно падает, и совсем не обязательно, что это следствие возможной ошибки в модели. Кроме того, в терминах представленной модели аналитически было доказано, что в случае, если одна из сторон выбирает агрессивную стратегию, другой стороне для достижения паритета необходимо выбрать стратегию не менее сильную. Таким образом,

к сожалению, для агрессивной среды придется признать справедливым известный тезис о том, что «нападение — лучший способ обороны».

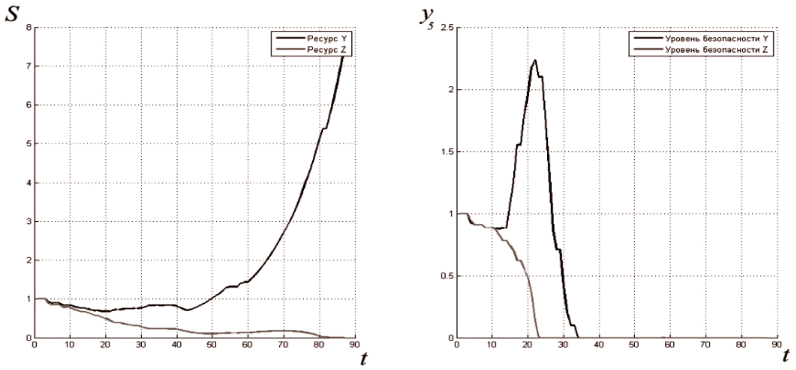


Рис. 32. Доминирование (Y) против паритета (Z)

Итак, для эффективного противодействия угрозам в информационно-психологической сфере необходимо выявление наиболее значимых и актуальных относительно целей безопасности угроз, источники которых могут находиться в далеких от психологической проблематики областях, и, наоборот, решение проблем гуманитарного характера может стать решающим в обеспечении безопасности в материальной сфере.

Успешное противодействие угрозам должно непременно включать активную составляющую, защитные мероприятия невозможны без активного противодействия — оборонительная позиция или пацифизм ведут к поражению. Активное противодействие далеко не всегда предполагает только силовую составляющую, это могут быть организационные меры, педагогические, юридические и другие вполне мирные средства.

Предложенные формальные методы аналитики в исследовании проблем информационно-психологической безопасности являются лишь инструментом и не могут заменить традиционные для данной предметной области подходы и методы. Модели, построенные для решения конкретных задач, должны отражать текущий уровень знания (незнания) экспертов, но оценки, получаемые на их основе, по этой же причине, не должны существенно отличаться от результатов многовариантного вербального обсуждения, имея при этом заведомое преимущество: отсутствие ангажированности и возможность согласования.

Заключение

Проведенный авторами анализ различных аспектов информационно-психологической и когнитивной безопасности представляет собой междисциплинарное исследование и в плане рассмотренных проблем, и по составу авторского коллектива — это философы, психологи, политологи и культурологи, с одной стороны, и специалисты в области медиалогии, компьютерных технологий и информационной безопасности — с другой.

Обобщающим выводом, пожалуй, следует считать признание того, что в условиях наступившей четвертой промышленной революции безопасность человеческого бытия в целом, информационно-психологическая и когнитивная безопасность в особенности, обретают качественно новый статус. Безопасность — это уже не только обеспечение ответных мер по предупреждению стихийных, социальных, политических, военных, информационных и иных опасностей. Безопасность сегодня — это превентивная, упреждающая безопасность, стратегия создания которой должна основываться на природоподобных и нано-технологиях. Если же говорить о собственно информационно-психологической и когнитивной безопасности, то здесь, очевидно, необходимо рассматривать программу создания механизмов и программ превентивной безопасности на наноуровне подобно тому, как на этом уровне закладывались структуры и функции адаптации, устойчивого, прогрессивного развития биологических систем в едином энерго-информационном пространственно-временно́м континууме.

Проблема информационно-психологической и когнитивной безопасности в современных условиях обретает государственный статус. Это довольно четко прослеживается в «Доктрине информационной безопасности Российской Федерации» (от 6 декабря 2016 г.), определяющей задачи и направления стратегического планирования в сфере

обеспечения национальной безопасности Российской Федерации. Из признания (в числе основных информационных угроз) практики внедрения информационных технологий без увязки с обеспечением информационной безопасности в условиях трансграничного оборота информации, пропаганды экстремистской идеологии, а также расширения масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира, следует указание на ряд направлений обеспечения информационной безопасности. Это, во-первых, нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества, — в области обороны страны. Во-вторых, противодействие использованию информационных технологий для пропаганды экстремистской идеологии и нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей, — в области государственной и общественной безопасности. В-третьих, обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности — в области науки, технологий и образования.

Авторский коллектив предложил свой вариант решения проблем обеспечения информационно-психологической и когнитивной безопасности, учитывающий достижения и вызовы новой промышленной революции.

Р. М. Юсупов
И. Ф. Кефели

Сведения об авторах

Баранов Николай Алексеевич, доктор политических наук, профессор кафедры международных отношений Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, профессор кафедры политических институтов и прикладных политических исследований факультета политологии Санкт-Петербургского государственного университета, профессор кафедры международных отношений и зарубежного регионоведения Санкт-Петербургского института внешнеэкономических связей, экономики и права;

Вассоевич Андрей Леонидович, кандидат исторических наук, доктор философских наук, профессор кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета;

Виноградова Светлана Михайловна, доктор политических наук, профессор, заведующая кафедрой теории и истории международных отношений факультета международных отношений Санкт-Петербургского государственного университета;

Забарин Алексей Владимирович, кандидат психологических наук, доцент кафедры психологии служебной деятельности Санкт-Петербургского военного института национальной гвардии и кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета;

Касаткин Виктор Викторович, кандидат технических наук, доцент, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, ученый секретарь Научного совета по информатизации Санкт-Петербурга;

Кефели Игорь Федорович, доктор философских наук, профессор, заслуженный работник высшей школы Российской Федерации, Федерации, директор Центра геополитической экспертизы Северо-Западного института управления — филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, первый вице-президент Академии геополитических проблем, главный редактор журнала «Геополитика и безопасность», эксперт РАН, советник РАРАН;

Ковалев Александр Павлович, доктор технических наук, профессор, лауреат премии Правительства РФ, Заслуженный деятель науки Российской Федерации, Заслуженный испытатель космодрома «Байконур», председатель Совета директоров АО КБ «Арсенал» им. М. В. Фрунзе, генерал-лейтенант;

Колбанев Михаил Олегович, доктор технических наук, профессор кафедры прикладных информационных технологий Санкт-Петербургского государственного экономического университета;

Комлева Наталья Александровна, доктор политических наук, профессор, вице-президент Академии геополитических проблем, директор Центра геополитического анализа Академии геополитических проблем;

Котенко Игорь Витальевич, доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН;

Левкин Игорь Михайлович, доктор военных наук, профессор кафедры международных отношений Северо-Западного института управления — филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, профессор кафедры безопасных информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики;

Мельник Галина Сергеевна, доктор политических наук, профессор кафедры периодической печати Института «Высшая школа журналистики и массовых коммуникаций» Санкт-Петербургского государственного университета;

Мисонжников Борис Яковлевич, доктор филологических наук, профессор, заведующий кафедрой периодической печати Института «Высшая школа журналистики и массовых коммуникаций» Санкт-Петербургского государственного университета;

Нурышев Геннадий Николаевич, доктор политических наук, профессор кафедры международных отношений, медиалогии, политологии и истории Санкт-Петербургского государственного экономического университета;

Осипов Василий Юрьевич, доктор технических наук, профессор, заведующий лабораторией Санкт-Петербургского института информатики и автоматизации РАН;

Плебанек Ольга Васильевна, доктор философских наук, доцент, заведующая кафедрой социально-гуманитарных дисциплин

Межрегионального института экономии и права при МПА ЕврАзЭС, профессор кафедры социально-гуманитарных дисциплин Национального государственного университета физической культуры, спорта и здоровья имени П.Ф. Лесгафта;

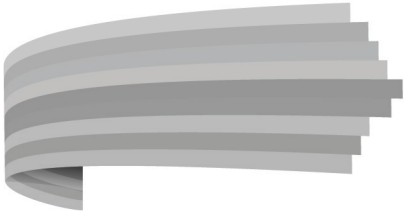
Саенко Игорь Борисович, доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН;

Самуйлова Ирина Алексеевна, кандидат психологических наук, доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета;

Чечулин Андрей Алексеевич, кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН;

Шишкин Владимир Михайлович, кандидат технических наук, доцент, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН;

Юсупов Рафаэль Мидхатович, член-корреспондент РАН, доктор технических наук, профессор, заслуженный деятель науки и техники РФ, директор Санкт-Петербургского института информатики и автоматизации РАН.



Под ред. И. Ф. Кефели, Р. М. Юсупова

Информационно-психологическая и когнитивная безопасность

ООО ИД «Петрополис»
ООО «Геополитика и безопасность»
197101, Санкт-Петербург, ул. Б. Монетная, д. 16,
офис-центр 1, 5 эт., пом. 498, тел. 336 50 34
e-mail: info@petropolis-ph.ru
http://www.petropolis-ph.ru
http://www.petrobook.ru
Подписано в печать 12.09.2017.
Формат 60 × 84 $^{1}/_{16}$. Бумага офсетная.
Печать офсетная. 18,75 п.л.
Тираж 500. Заказ 77.
Отпечатано в типографии «Град Петров»
ООО ИД «Петрополис»
197101, Санкт-Петербург, ул. Б. Монетная, д. 16