DOI: 10.24290/1029-3736-2023-29-4-200-220

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СПЕЦИФИКА ФЕНОМЕНА, МЕТОДЫ И СПОСОБЫ ЕЕ ОБЕСПЕЧЕНИЯ

С.Г. Карепова, канд. социол. наук, ведущий научный сотрудник Объединенного центра социологии и экономики знания Института социологии ФНИСЦ РАН, ул. Большая Андроньевская, д. 5. стр.1, г. Москва, Российская Федерация, 109544*

С.В. Некрасов, научный сотрудник Объединенного центра социологии и экономики знания Института социологии ФНИСЦ РАН, ул. Большая Андроньевская, д. 5. стр.1, г. Москва, Российская Федерация, 109544**

А.Н. Пинчук, канд. социол. наук, доц. кафедры политологии и социологии Российского экономического университета им. Г.В. Плеханова, старший научный сотрудник Объединенного центра социологии и экономики знания Института социологии ФНИСЦ РАН, Стремянный пер., 36, Москва, Российская Федерация, 117997***

Статья посвящена актуальному и востребованному в рамках современных междисциплинарных научных исследований направлению — информационной безопасности, а также специфике данного феномена и методам его обеспечения. В работе отмечается, что в современном социально-научном знании есть понимание важности сохранения информационной безопасности, что отражено в ряде теоретико-методологических и научно-практических исследований советских и современных российских ученых, что также говорит о достаточной научной разработанности феномена. Данное научно-исследовательское направление значительно актуализировано и в стратегических нормативных государственных документах, отвечающих за национальную безопасность страны. Особое внимание в статье уделяется важнейшим характеристикам современной социальной реальности, ее детерминирующим факторам развития, новым тенденциям, инновационным вызовам и рискам, которые являются не только ее характеристиками, но и зонами бифуркаций, требующими учета и предотвращения в будущем. С точки зрения авторов, в данном рисковом континууме решающее значение приобретают именно риски, связанные с информационной составляющей и с разрушением информационной безопасности, в частности. В статье также отмечается ключевая роль социокультурного аспекта в создании желательной для социума современной социальной реальности. Речь идет о сознательном выходе через социокуль-

* **Карепова Светлана Геннадьевна**, e-mail: Svetlran@mail.ru

** **Некрасов Сергей Владимирович**, e-mail: sv_79@inbox.ru

*** **Пинчук Антонина Николаевна**, e-mail: antonina.pinchuk27@bk.ru

турный план на процессы управления индивидуальным и массовым сознанием современного социума. Авторами по результатам проведенного анализа ключевых нормативных документов (Доктрина национальной безопасности РФ, Стратегия национальной безопасности РФ и др.) и научных разработок выявлены наиболее распространенные и применяемые на практике методы и средства обеспечения информационной безопасности и объединены в авторскую схему — классификацию, дающую наглядное представление о научно-практической стороне феномена. В статье отмечается чрезвычайная важность дальнейшего изучения информационной безопасности, как научного направления, обладающего выраженным исследовательским потенциалом и высокой научно-практической востребованностью в будущем. Особую актуализацию в рамках данного направления приобретает организационно-управленческий план и выход на практический уровень сохранения феномена.

Ключевые слова: *информационная безопасность, социальная реальность, сознание, социум, угрозы, методы, способы, социокультурный аспект.*

KEY FEATURES OF THE PHENOMENON, ITS METHODS AND MEANS

Karepova Svetlana G., PhD in Sociology, Leading Researcher, Joint Center of Sociology and Economics of Knowledge, Institute of Sociology of FCTAS RAS, st. Bolshaya Andronievskaya, 5, building 1, Moscow, Russian Federation, 109544, e-mail: Svetlran@mail.ru

Nekrasov Sergey V., Researcher, Joint Center of Sociology and Economics of Knowledge, Institute of Sociology of FCTAS RAS, st. Bolshaya Andronievskaya, 5, building 1, Moscow, Russian Federation, 109544, e-mail: sv_79@inbox.ru

Pinchuk Antonina N., PhD in Sociology, Associate Professor, Political Science and Sociology Chair, Plekhanov Russian Economic University, Senior Researcher, Joint Center of Sociology and Economics of Knowledge, Institute of Sociology of FCTAS RAS, Stremyanny lane, 36, Moscow, Russian Federation, 117997, e-mail: antonina.pinchuk27@bk.ru

This article is devoted to the information security, which is a relevant and demanded research area within modern interdisciplinary scientific studies, key features of this phenomenon and its methods as well. The paper notes that there is an understanding of the importance to maintain information security in social scientific knowledge. This is evidenced by a number of soviet and Russian scientists' theoretical-methodological and scientific-practical studies, which indicate the sufficient research mastery of the phenomenon. This research area has taken on increasing importance in the strategic regulatory state documents, which are responsible for the country's national security. Special attention is paid to the most significant characteristics of social reality, its determining development factors, new trends, innovation challenges and risks. These are not only the characteristics of social reality but its bifurcation zones, which to be taken into consideration and prevented in the future. In the authors' view, namely the risks,

related to the informational component and the undermining of information security in particular, acquire importance. The article notes the key role of a sociocultural aspect in creating a desirable modern social reality for society. This is about a conscious access to manage both an individual and mass consciousness through the sociocultural aspect. Based on the results of analyzing the key regulatory documents, the authors identified methods and means of ensuring information security, which are most widespread and put into practice. They were integrated into the authors' scheme that provides a clear picture of this phenomenon's scientific-practical side. The article notes the extreme significance of further studying information security as a research area that has a great scientific potential and a high scientific-practical demand in the future. The management plan and practical outcome of preserving the phenomenon acquire a particular relevance within this research area.

Key words: *information security, social reality, consciousness, society, threats, methods, means, sociocultural aspect.*

Современная социальная реальность России начала XXI в. ознаменовалась глубинными социетальными (социальными, экономическими, социокультурными и геополитическими) изменениями "тектонического" характера, когда привычные "картины мира" для человека перестали существовать, а новые, призванные сыграть стабилизирующую в социуме роль, еще полностью не сформированы и находятся в непрерывном трансформационном процессе[1].

Ключевой детерминантой, характеризующей специфику современной социальной реальности как на локальном государственном, так и на глобальном международном уровнях, стало состояние ее нестабильности, подвижности и в конечном итоге кризисности. Речь идет о перманентных деформациях на уровне структуры, процессов, функций социетальной системы новой реальности, что вносит изменения в устоявшийся формат функционирования социума и грозит его целостности. Фактически непрерывные трансформационные процессы, происходящие в обществе, обусловливают друг друга и, как следствие, системно друг на друга наслаиваются. Их внутренняя и внешняя нелинейность, неравновесность и неустойчивость содержат выраженный потенциал необратимости. Все это формирует "взрывную", трудно управляемую для социума и внутренне "текучую" изменяющуюся реальность, в которой состояние подвижности становится фундаментальным и основополагающим. Перманентные изменения становятся ее нормой и неотъемлемой частью.

[1] Новая социальная реальность: системообразующие факторы, безопасность, перспективы развития. Россия в техносоциальном пространстве: Коллективная монография. М.; СПб., 2020.

Следует отметить, что "сценарное" развитие современного российского социума первой четверти XXI в. актуализирует и практически формализует обозначенные процессы, которые отражаются, в первую очередь, на ситуативном уровне происходящих событий. В данном ключе разумно вспомнить изменившую мир пандемию COVID-19 и запущенный ею новый непредсказуемый формат функционирования базовых институтов общества (наука, образование, семья и т.д.), отвечающих за стабильность, организацию, регулирование общественной жизни, отношения и стратегии в социуме[2]. Глобальным и необратимым бифуркационным событием для социальной реальности, безусловно, стала спровоцированная Западом и проводимая Россией в Украине специальная военная операция (СВО), повлекшая за собой глубинные трансформационные изменения на всех уровнях современного общества в краткосрочной, среднесрочной и долгосрочной перспективах. Большое значение для дальнейшего вектора цивилизационных изменений, подчас взрывного и непредсказуемого характера, имеют знаковые инновационные достижения в информационной и технологической сферах и т.д. Первоначально кажется, что содержательно данные процессы не имеют ничего общего между собой. Это не так. Все они в условиях нестабильности являются частью единого непрерывного трансформационного процесса социальной реальности, порождающего проявление ее рисковости и распространение широкого спектра новых вызовов и угроз для безопасности страны[3].

В рамках наметившейся цивилизационной парадигмы непрерывного изменения разумно вести речь о таком типе новых рисков, которые обладают и качественно новыми характеристиками, другой природой функционирования и воздействия на социум. Эти риски наделены скрытым отложенным эффектом воздействия на социум[4], что скажется только в будущем, в его среднесрочной и долгосрочной перспективе и на последующих поколениях. Как правило, они не очевидны и их значимость проявляется только по истечении определенного времени. Общество (до настоящего времени технологических и информационных прорывов) с таким

---

[2] Вызовы пандемии и стратегическая повестка дня для общества и государства: социально-политическое положение и демографическая ситуация в 2021 году. Монография / Отв.ред. В.К. Левашов, Г.В. Осипов, С.В. Рязанцев, Т.К. Ростовская. М., 2021. DOI: 10.19181/monogr.978-5-89697-384-3.2021.

[3] Национальная безопасность России в информационную эпоху. Россия в системе глобальных изменений современной цивилизации. 2015–2016 годы. М., 2017.

[4] Risk in the technological society. Boulder, 1982.

форматом рисков практически не сталкивалось. Они отличаются иными, трудно просчитываемыми алгоритмами действия, что, в свою очередь, актуализирует и новые сферы и формы защиты безопасности социума[5].

Новая реальность сформировала и качественно иной запрос как к системе государственного управления, требуя превентивных действий от государства, человека и общества, так и к ключевым сферам научного знания о мире.

Актуальность изучения и сохранения информационной безопасности: социокультурный и правовой аспекты. Наиболее рисковым направлением, с нашей точки зрения, в настоящее время стало агрессивное и беспринципное информационное воздействие на массовое сознание социума[6] или, по сути, развязывание в условиях проведения специальной военной операции открытой информационной войны[7]. Речь идет об актуализации сохранения информационной безопасности для социума.

Информационная война в краткосрочных, среднесрочных и долгосрочных временных периодах, как правило, разворачивается на "социокультурном поле" современного общества, затрагивая его системообразующие институты (семья, образование, наука, вера, мораль и т.д.), благодаря которым в обществе осуществляется основной процесс воспитания. Именно социокультурный план как базовая культурная и социальная среды человека, отвечающие за его нравственное, духовное становление, оказались под информационным воздействием.

Эта война спустилась на максимально глубокие слои человеческой психики, затронула сознание человека и его когнитивный уровень, тот уровень, на котором вырабатывается ценностный ряд, на основании которого человек в частности и общество в целом формируют свои жизненные стратегии и выстраивают так называемые "картины мира".

---

[5] *Горохов В.Г., Сюнтюренко О.В.* Технологические риски: информационные аспекты безопасности общества // Программные системы и вычислительные методы. 2013. № 4(5). С. 344–353.

[6] *Осипов Г.В., Карепова С.Г., Костоломова М.В., Некрасов С.В., Пинчук А.Н.* Информационное воздействие на сознание общества в условиях пандемии: теория и методы исследования // Российское общество и государство в условиях пандемии: социально-политическое положение и демографическое развитие Российской Федерации в 2020 году: Коллект. монограф. / Под ред. Г.В. Осипова, С.В. Рязанцева, В.К. Левашова, Т.К. Ростовской; Отв. ред. В.К. Левашов. М., 2020. DOI: 10.38085/978-5-905790-48-5-2020-1-532.

[7] *Лисичкин В.А., Шелепин Л.А.* Третья мировая информационно-психологическая война. М., 1999. URL: https://www.x-libri.ru/elib/lsshl000/00000001.htm (дата обращения: 07.04.2023).

Чем это опасно для социума? По сути, информационное проникновение извне на глубинный уровень сознания оказывает прямое влияние на построение им ментальных конструкций и их содержание. Подобное внедрение всегда чревато, так как осознанное или неосознанное принятие определенных ценностей, добровольно выбранных или навязанных кем-то извне, порождает возникновение обусловленных ими мотиваций и диспозиций для дальнейших действий и строительства желательной социальной реальности[8]. Речь идет о фундаментальной основе для объективизации на практике субъективной деятельности человечества, как главного актора цивилизационного строительства. Разумно вести речь о том, что весь транслируемый в обществе информационный контент активно впитывается как индивидуальным, так и массовым сознанием, а его содержание и качество являются базисом грядущей парадигмы развития социума.

Как правило, информационное воздействие активно использует особенности и специфику человеческой психики и рассчитано на охват широкой аудитории по принципу чем больше, тем лучше. Итоговый ориентир на массовое сознание в подобного рода воздействиях практичен и точен, так как оно, будучи частью общественного сознания, имеет интегративный характер и вбирает в себя все наработки индивидуальных сознаний и глобального человеческого опыта в целом.

Но в данном случае этот тип сознания в основном связан с деятельностью больших массовых общностей. Он содержательно ориентирован на эмоционально образные суждения и, по сути, очень психологичен и внушаем[9]. Как правило, массовое сознание оперирует архетипами и мифологическими образами. Определяющее значение начинает приобретать человеческий фактор. При этом в массовом сознании налицо присутствие его неспособности к выработке адекватных критических оценок происходящих событий и процессов, новых предлагаемых обществу смыслов. Происходит ослабление его социальной ответственности за счет растворения индивидуального в эффектах "толпы", в которых инерция больших масс нивелирует привычные ограничения и чувство опасности. Искажение видения мира провоцирует людей на неадекватные

[8] *Osipov G.V., Pinchuk A.N., Karepova S.G., Nekrasov S.V., Tikhomirov D.A.* Social reality construction in the techno-social world: new aspects of sociological conceptualization // Revista Inclusiones. 2021. Vol. 8. N. S2–1. P. 615–623.

[9] *Некрасов С.В., Карепова С.Г.* Внушение как метод воздействия на общественное сознание // Социальная политика и социология. 2021. Т. 20. № 3(140). DOI: 10.17922/2071-3665-2021-20-3-126-134.

действия и зарождение в перспективе в социуме широкого спектра деструкций, содержащих в себе трансформацию моральных норм, ценностей и др. Все эти процессы значительно повышают уровень ментальной управляемости и порождают процессы нестабильности в социуме.

По существу, с учетом обозначенных особенностей и тонкостей функционирования массового сознания, в современном социуме развязана так называемая когнитивная война, или война смыслов, нацеленная на захват и негативную трансформацию значимого смыслового континуума и на получение от общества желаемого типа поведения в чьих-то интересах. Как правило, захват смыслового континуума происходит за счет использования широкого спектра инструментария манипуляции сознанием[10], что представляет собой "такой вид управления поведением личности, социальной группы, общества или планетарного социума, при котором используются скрытые методы социально-психологического воздействия на сознание людей в целях обеспечения частных, отличных от собственных, интересов отдельных лиц, социальных групп, институтов, государственных и общественных структур, им противоречащих"[11]. Это скрытый и неочевидный для поверхностного взгляда процесс методологического характера, имеющий расширенный спектр приемов и методов управления индивидуальным и массовым сознанием[12] и включение его в деструктивное состояние "неосознанного выбора разрушительных ментальных моделей и вопреки здравому смыслу"[13]. Фактически по результатам подобных манипуляций мы получаем податливое к информационному воздействию массовое сознание социума, которым при правильной подаче нужной для интересантов информации можно легко управлять. По такому алгоритму формируется нужное общественное мнение и, как было отмечено выше, изменяется вектор развития социума.

Таким образом, наносится "информационный удар" по глубинным цивилизационным ценностям, легитимным алгоритмам поведения, базовым социетальным основам в обществе, сформированным на основе положительного исторического опыта человече-

---

[10] *Кара-Мурза С.Г.* Манипуляция сознанием. М., 2005.

[11] *Староверов В.И., Левашов В.И.* Манипулирование общественным сознанием: социологические аспекты анализа // Социология власти. 2009. № 4. С. 28–42.

[12] *Некрасов С.В.* К вопросу о методах воздействия на общественное сознание // Вестник НГУЭУ. 2020. № 4. DOI: 10.34020/2073-6495-2020-4-184-201.

[13] *Карепова С.Г., Некрасов С.В., Пинчук А.Н.* Пропаганда как метод воздействия на общественной сознание: общий теоретический аспект // Вестник НГУЭУ. 2020. № 4. DOI: 10.34020/2073-6495-2020-4-212-229.

ства. Именно в рамках "информационного удара" перечеркиваются устоявшиеся в социуме стратегии и практики, стабилизирующие его функционирование. В данном случае следует вспомнить, что человек, не ценящий опыта прошлого, всегда остается без своего будущего. Более того, при потере обществом устоявшихся базовых культурно-исторических, социально-психологических скреп, своеобразного "путеводителя", с помощью которого выстраивались его стратегии развития, оно неизбежно вступит на рисковый путь управления им кем-то со стороны и в своих интересах.

В частности, сложившаяся в настоящее время в социуме ситуация ярко иллюстрирует эти процессы на практике, когда сознательно созданный лживый и агрессивный информационный контент, вброшенный в социум, становится не менее опасен, чем фактическое оружие. «Недостоверная информация, декларируемая в СМИ, затрагивает как течение самой спецоперации, так и ее информационное сопровождение в обществе, что, по сути, нацелено на социально-психологическую дестабилизацию социума и подрыв авторитета российского руководства. Распространение ложных фото, видео и печатных материалов как элементов этой войны против России провоцирует общественное сознание на формирование образа "внутреннего врага", повышенной подозрительности, сепарации общества на "своих" и "чужих", недоверие проводимой государством политике и др.»[14].

Правовой или нормативный уровень регуляции вопросов и проблем, связанных с информационной безопасностью, всегда был актуализирован в историческом и современном аспектах законотворческой деятельности на уровне таких ключевых законодательных документов страны, как Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 г. № 149-ФЗ, Стратегия национальной безопасности Российской Федерации от 31.12.2015 г. № 683, Доктрина информационной безопасности от 05.12.2016 г. № 646, Стратегия национальной безопасности Российской Федерации от 02.07.2021 г. № 400, Федеральный закон "О государственной тайне" от 21.09.1993 г. №182, Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. от 31.12.2015 г. № 683 и т.д.

Следует отметить, что чрезвычайная значимость сохранения и поддержания информационной безопасности отражена и в основ-

[14] *Карепова С.Г., Костоломова М.В., Некрасов С.В., Пинчук А.Н.* Информационная безопасность в условиях новой социальной реальности: специфика и способы сохранения // Социальные и гуманитарные знания. 2022. Т. 8. № 2(30). DOI: 10.18255/2412-6519-2022-2-190-203.

ном стратегическом государственном документе страны по общей безопасности. В Стратегии национальной безопасности Российской Федерации от 02.07.2021 г. сформулированы девять основных стратегических приоритетов сохранения национальной безопасности. К ним относится: сбережение народа России и развитие человеческого потенциала, оборона страны, государственная и общественная безопасность, информационная безопасность, экономическая безопасность, научно-технологическое развитие, экологическая безопасность и рациональное природопользование, защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти, стратегическая стабильность и взаимовыгодное международное сотрудничество[15].

На практике системообразующий характер феномена информационной безопасности проявляется в том, что ее вопросы, проблемы и задачи комплексно охватывают анализ и обеспечение всех девяти обозначенных ключевых приоритетов, фактически детерминируя и обусловливая их функционирование.

Таким образом, нарушение приоритета информационной безопасности чревато негативными трансформациями для всей социетальной системы общества в целом, что формирует актуальность данной проблематики как в научном дискурсе, так и в сфере управления обществом на перспективу.

Теоретико-методологическая разработанность феномена информационной безопасности. В современном обществе есть понимание важности сохранения информационной безопасности, что отражено не только на законотворческом уровне, но и в растущем интересе к феномену в научном сообществе. Это нашло свое отражение в ряде теоретико-методологических и научно-практических разработок советских и современных российских ученых.

Данная научно-исследовательская проблематика имеет выраженный междисциплинарный характер и рассматривается на уровне различных социально-научных, технических, юридических и др. областей знания (философия, социология, политология, психология личности, общая психология, юриспруденция, технические науки и т.д.). Феномен рассматривается под разными углами профильных знаний, актуализирующих определенный научно-исследовательский ракурс информационной безопасности.

---

[15] Указ Президента Российской Федерации от 02.07.2021 N 400 "О стратегии национальной безопасности Российской Федерации" // КосультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 07.04.2023).

Базовые социально-философские изыскания в области информационной безопасности нашли свое отражение в работах таких ученых-социологов и социальных философов, как М.Ю. Захаров, С.Г. Кара-Мурза, И.Н. Панарин, А.В. Поликарпов, Л.В. Астахов, Н.Н. Богомолов, В.Ю. Триняк, Т.В. Владимирова, Т.В. Науменко, И.Д. Фомичёв и др. Учеными поднимаются фундаментальные вопросы осмысления сущности феномена и общей специфики его функционирования в современном социуме.

Исследования проблем обеспечения информационной безопасности в области политологического знания связаны с проблемами ее политического и геополитического характера, что также нашло свое воплощение в научном творчестве ученых политологов и геополитиков — Г.Л. Смоляна, И.Ю. Сундиева, А.Ф. Федорова, В.Н. Цыгичко, Д.С. Черешкина, А.А. Кокошина, Е.О. Кубякина и др.

Психологический срез в общем социетальном континууме рассмотрения данного феномена отражен в работах И.К. Мельника, Ю.А. Ермакова, В.Е. Лепского, Г.В. Грачева. Учеными-психологами также рассматриваются различные аспекты и формы защиты психики и психической деятельности человека и социума от вредного массированного информационного воздействия извне.

Междисциплинарный уровень изучения проблем воздействия системы интернет и виртуального пространства на социально-психологический план развития личности отражен в исследованиях А.Е. Войскунского.

Психолого-политологические аспекты проблематики информационных войн отражены в работах Г.Г. Почепцова, С.П. Расторгуева, И.А. Панарина и др.

Юридический аспект научно-исследовательской проблематики представлен профильными исследованиями Ю.М. Батурина, В.В. Крылова, Н.Г. Шурухнова в области противодействия компьютерной преступности на законодательном уровне. Проблемы правового обеспечения защиты сведений, составляющих государственную тайну, стали предметом научного интереса таких авторов-правоведов, как А.Л. Балыбердин, А.А. Фатьянов, М.А. Вус и др. Вопросы совершенствования законодательной системы в области информатизации подняты в материалах А.Б. Агапова, В.А. Копылова и др. Ключевые аспекты регулирования отношений в области доступа к информации отражены в работах И.Л. Бачило, В.Н. Лопатина и др. Широкий спектр вопросов по проблемам охраны прав интеллектуальной деятельности и защиты персональных данных информационной деятельности в правовом российском и между-

народном поле поднят в научно-исследовательских разработках Л.А. Сергиенко, В.А. Рубанова, Л.К. Терещенко, П.У. Кузнецова и др.

Общее направление в области технического и технологического знания в данной области связано с защитой информации в информационных и телекоммуникационных системах от несанкционированного доступа и представлено разработками С.П. Расторгуева, В.Г. Герасименко, Л.М. Ухлинова, М.П. Сычева, Д.П. Зегжды и др.[16]

Безопасность больших промышленных систем в информационной сфере отражена в работах ученых-специалистов в области технических наук В.В. Москвичева, Н.А. Махутова, М.М. Гаденина, Р.С. Ахметханова и др.

Экономический аспект проблем информационной безопасности достаточно полно рассмотрен в материалах научных разработок А.В. Зуева, Л.В. Мясникова и др.

Научная разработанность и изученность информационной безопасности в ее социетальном аспекте не могут считаться исчерпывающими в силу бифуркационного характера как изменяющейся современной социальной реальности, так и специфики самого феномена. Вклад ученых в его разработку трудно переоценить, а актуальность и востребованность дальнейшего изучения информационной безопасности будут только возрастать и актуализироваться.

Основные методы и средства обеспечения информационной безопасности: виды и особенности применения на практике. Обеспечение информационной безопасности — сложный, многофункциональный процесс, зависящий от факторов, детерминирующих современную социальную реальность, в которой общество связано с освоением и использованием новых информационных технологий (виртуальное пространство, интернет, современные квантовые технологии, искусственный интеллект). Особого внимания при изучении информационной безопасности заслуживают вопросы, касающиеся влияния ряда нововведений в области информационных технологий на развитие общества, мировоззрение социума, поведение людей, функционирование их психики, отношение друг к другу и окружающей среде[17]. Все эти современные информационные тренды являются теми потенциально взрывными точками, в которых актуализируются проблемы, регулируемые сферой информационной безопасности.

---

[16] *Стрельцов А.А.* Обеспечение информационной безопасности в России. Теоретические и методологические основы / Под ред. В.А. Садовничего, В.П. Шерстюкова. М., 2002.

[17] *Каптюг И.А.* Проблема информационной безопасности: философский и квантово-физические аспекты. Автореф. дисс ... канд. филос. наук. М., 2009.

Информационная безопасность как социальный феномен, включая в себя разнообразные научные толкования, содержательно введена в общий блок национальной безопасности страны и трактуется как "состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам)"[18], сконцентрированных, в первую очередь, в области информационной сферы. В соответствии с этим основными нормативными направлениями являются[19] противодействие использованию информационных технологий, пресечение деятельности, осуществляемой с помощью информационных технологий специальными службами иностранных государств, повышение защищенности критической информационной инфраструктуры, повышение безопасности объектов информационной инфраструктуры, повышение безопасности функционирования образцов вооружения, повышение эффективности профилактики правонарушений в информационной сфере, обеспечение защиты государственной информации, повышение информационного обеспечения государственной политики РФ, предупреждение информационного воздействия на российские духовно-нравственные ценности.

В рамках широкого охвата данной социетальной проблематики закономерно встает вопрос об использовании эффективных защитных практик.

Целесообразно вести речь о государственно одобряемых и закрепленных в нормативном документе методах[20], содействующих обеспечению информационной безопасности. Как правило, такие методы подразделяются на *два подвида — общие и частные,* используемые в социетальной системе общества, где в каждой из сфер системы существуют правовые, организационно-технические и экономические особенности в обеспечении феномена.

Общие методы подразделяются на правовые, экономические и организационно-технические[21].

Правовые методы работают в поле права и включают в себя законотворчество в области разработки нормативных законодательных актов в информационной сфере, а также профильные методические.

---

[18] Указ Президента Российской Федерации от 05.12.2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 07.04.2023).

[19] Там же.

[20] Там же.

[21] Там же.

Правовое обеспечение информационной безопасности осуществляется в следующих основных направлениях:

- внесение поправок и дополнений в законодательство Российской Федерации в области информационной безопасности;
- разграничение полномочий в сфере информационной безопасности между различными уровнями государственной власти (федеральными и государственными органами власти субъектов РФ);
- формирование правил аккредитации иностранных новостных агентств, СМИ и журналистов на территории РФ;
- разработка правовой основы для региональных структур обеспечения информационной безопасности.

Экономические методы функционируют в рамках осуществления финансовой политики РФ. К ним относится:

- инаучно-исследовательская работа по созданию национальных программ, нацеленных на сохранение информационной безопасности и формирование процедур их финансирования;
- усовершенствование финансирования мероприятий, нацеленных на использование правовых, организационно-технических методов защиты информации и создание системы страхования от информационных рисков.

Организационно-технические методы используются в сфере управления большими и малыми техническими системами и содержательно нацелены на выработку административных и научно обоснованных норм, действий и направлены на:

- создание и улучшение управленческой системы информационной безопасности РФ;
- разработку и применение средств информационной защиты (программное обеспечение, телекоммуникационные системы и т.д.);
- сертификацию и лицензирование средств защиты информации;
- подготовку кадров в области обеспечения информационной безопасности РФ;
- мониторинг индикаторов и показателей информационной безопасности[22].

Но специфика социальной реальности такова, что стратегии ее развития не обладают устойчивостью и предсказуемостью, а бифур-

[22] Указ Президента Российской Федерации от 05.12.2016 г. N 646…

кационный характер диктует необходимость постоянного расширения базовых регулятивных методов. Речь идет о том, что наряду с общими методами защиты государственных интересов в данной сфере применяются и другие — частные методы, нацеленные на решение более узких проблем информационной безопасности.

Частные методы так же, как и общие, охватывают социетальный уровень реальности, включая работу базовых общественных институтов (наука, образование, общество, государство и т.д.) и активно используются на практике.

Частные методы обеспечения информационной безопасности в оборонной сфере нацелены на защиту от угроз, связанных с применением информационных технологий в военно-политических целях. Они применяются в следующих направлениях:

- сдерживание и предотвращение военных конфликтов, разворачивающихся на фоне применения информационных технологий;
- обнаружение и оценка информационных угроз Вооруженным силам РФ в информационной сфере;
- оказание защиты союзникам РФ в информационной сфере;
- устранение информационного воздействия, направленного на подрыв патриотических традиций страны[23].

К частным методам обеспечения информационной безопасности в экономической сфере относится создание конкурентных средств обеспечения в данной сфере. Это осуществляется в следующих направлениях:

- наукоемкое и инновационное развитие самой отрасли информационных технологий;
- развитие и внедрение отечественных разработок в производство;
- повышение конкурентоспособности в области информационных технологий и компьютерной промышленности на практике;
- развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, а также обеспечение потребности внутреннего рынка в данной продукции[24].

Частные методы обеспечения информационной безопасности в области государственной и общественной безопасности регулируют глобальную сферу российской государственности (защита

[23] Указ Президента Российской Федерации от 05.12.2016 г. N 646...
[24] Там же.

суверенитета, политическая и социальная стабильность, территориальная целостность РФ, права и свобода человека, защита информационной инфраструктуры и т.д.) и вопросы социума. Основными методами являются:

- пресечение использования информационных технологий, применяемых в целях пропаганды экстремисткой идеологии и ксенофобии;
- разработка механизмов обнаружения и предупреждения информационных угроз и ликвидация последствий их проявления;
- профилактика правонарушений с применением информационных технологий;
- выявление и устранение негативного информационного воздействия на российские духовно-нравственные ценности[25].

Частные методы обеспечения информационной безопасности в сфере науки, технологий и образования функционируют в поле системообразующих институтов современной социальной реальности и нацелены на поддержку развития системы информационной безопасности, информационных технологий и электронной промышленности. Основными методами являются:

- развитие научно-технического потенциала в области обеспечения информационной безопасности;
- создание устойчивых к различным видам воздействия информационных технологий;
- осуществление научных исследований и создание инновационных информационных технологий обеспечения информационной безопасности;
- развитие кадрового потенциала в данной сфере;
- обеспечение защиты граждан от информационных угроз и воспитание информационной грамотности[26].

К частным методам обеспечения информационной безопасности в сфере стратегической стабильности и равноправного стратегического партнерства, применяемым в геополитической сфере функционирования социума и направленным на устойчивость межгосударственных отношений в информационном пространстве, относятся:

- проведение геополитической экспертизы для реализации национальных интересов в информационной сфере и защиты суверенитета РФ в информационном пространстве;

[25] Указ Президента Российской Федерации от 05.12.2016 г. N 646…
[26] Там же.

– продвижение геополитических и политических интересов РФ в рамках функционирования международных организаций в информационной сфере;
– развитие отечественной системы управления сегментом интернета[27].

Кроме основных методов (общих и частных) защиты информационной безопасности существует набор методов, направленных на защиту самого феномена. Речь идет о группе методов обеспечения самой информационной безопасности. К таким методам относятся: *маскировка, препятствие, управление, регламентация, побуждение, нападение и принуждение*[28].

Метод маскировки предполагает изменение информации, в результате чего она становится недоступной для заинтересованных злоумышленников. К данному методу относятся криптографические приемы преобразования информации, дезинформация, скрытие объекта, создание шумовых полей и др.

Метод препятствия основан на физическом преграждении злоумышленникам доступа к информации (к аппаратуре, к носителям информации и т.д.).

При *методе управления* защита информации осуществляется с помощью программных и технических средств, а также элементов баз данных, включая такие функции защиты, как идентификация пользователей, аутентификация объектов и субъектов, проверка на соответствие регламенту безопасности, регистрация обращений к защищенным ресурсам, реагирование на попытки несанкционированных действий (отключение сигнализации, отказ в запросе и т.д.)[29].

Метод регламентации нацелен на разработку и реализацию комплекса мероприятий, которые направлены на создание условий в информационной системе, препятствующих проявлению и воздействию угроз. К данному методу относятся правила ознакомления с секретной информацией, ее пересылкой, хранением и т.д. и различные способы технической и физической защиты.

Метод побуждения направлен на мотивацию людей соблюдать сложившиеся морально-этические нормы в отношении информации.

Метод нападения используется при наступлении активных действий противоборствующими сторонами с применением информационного оружия при ведении боевых действий или разведки.

---

[27] Указ Президента Российской Федерации от 05.12.2016 г. N 646…

[28] Организация защиты информации. URL: https://edu.tltsu.ru/ (дата обращения: 07.04.2023).

[29] Там же.

При применении *принуждения* как метода обеспечения информационной безопасности возникает необходимость соблюдения правил передачи и использования информации под угрозой наложения административной и уголовной ответственности[30].

Все перечисленные выше методы обеспечения информационной безопасности осуществляются с применением различных средств (законодательные, технические, программные и организационные). По сути, средства являются своего рода инструментарием для работы методов на практике.

К *законодательным средствам* обеспечения информационной безопасности относятся нормативно-правовые акты, направленные на регуляцию деятельности людей, имеющих доступ к закрытым сведениям и содержащие информацию о мере ответственности за неправомочное использование и разглашение данной информации.

Технические средства подразделяются на *физические (*двери, турникеты, замки, теле- и фотосистемы наблюдения и регистрации, биометрические средства защиты и др.*) и аппаратные* (электронные ключи, схемы аппаратного шифрования и т.п.) средства защиты информации.

К *программным средствам* обеспечения информационной безопасности относится программное обеспечение. По своим функциям они подразделяются на средства анализа кодов программ, средства блокирования атак (межсетевые экраны), средства аудита, средства контроля доступа, средства поиска уязвимости (сканеры безопасности)[31].

Организационные средства направлены на разработку и реализацию должностными лицами организационно-технических и организационно-правовых мероприятий[32] в целях эффективной реализации законодательных, технических и программных средств обеспечения информационной безопасности.

Безусловно, обозначенные методы обеспечения информационной безопасности не носят исчерпывающий характер, но позволяют содержательно их объединить в развернутую авторскую классификацию, которая будет трансформироваться в соответствии с актуализацией новых вызовов и угроз современной социальной реальности (рис.).

---

[30] Организация защиты информации.

[31] Там же.

[32] Определены статьей 16 ФЗ от 27.07.2006 г. "Об информации, информационных технологиях и защиты информации".

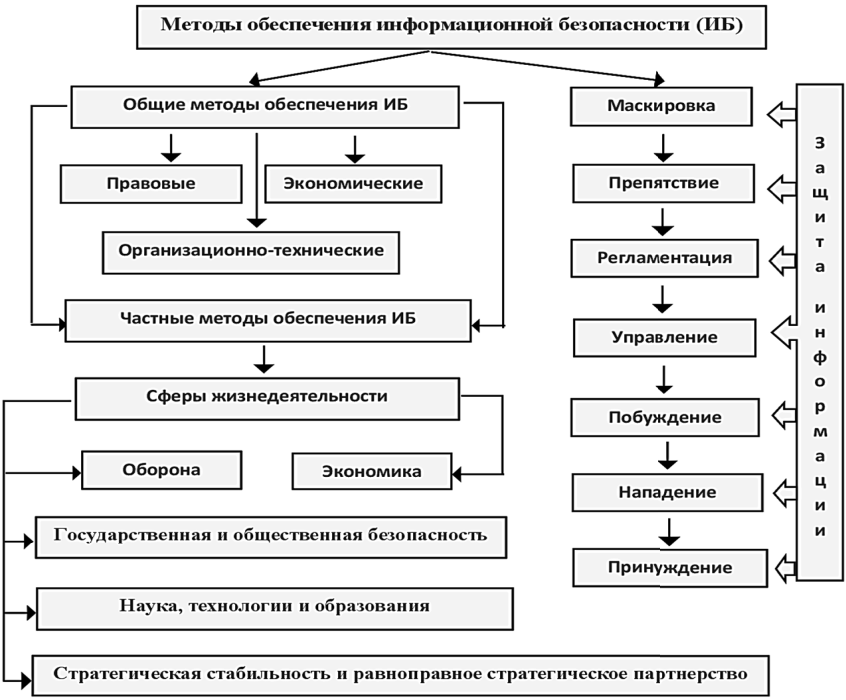

Рис. Методы обеспечения информационной безопасности (ИБ)

Таким образом, актуальность научного изучения феномена информационной безопасности, особенностей его функционирования, а также методов и средств обеспечения будет со временем только возрастать. Это обусловлено тем, что сам феномен, а также методы его сохранения полностью детерминированы процессами функционирования современной социальной реальности и так же, как и она, находятся в состоянии перманентного изменения и развития. Речь идет о его значительном трансформационном потенциале, а, следовательно, о необходимости формирования на перспективу новых и адекватных научно обоснованных методов обеспечения информационной безопасности. Чрезвычайную важность также приобретает формирование в рамках представленных методов и средств новых превентивных мер, нацеленных на безопасное обеспечение жизнедеятельности человека, государства и общества в будущем. В этой связи также разумно акцентировать внимание на организационно-управленческом направлении. Особую роль в данном процессе призваны сыграть системообразующие институты современной социальной реальности — наука, образование, нормотворчество.

СПИСОК ЛИТЕРАТУРЫ

Вызовы пандемии и стратегическая повестка дня для общества и государства: социально-политическое положение и демографическая ситуация в 2021 году. Монография / Отв. ред. В.К. Левашов, Г.В. Осипов, С.В. Рязанцев, Т.К. Ростовская. М., 2021. DOI: 10.19181/monogr.978-5-89697-384-3.2021.

Горохов В.Г., Сюнтюренко О.В. Технологические риски: информационные аспекты безопасности общества // Программные системы и вычислительные методы. 2013. № 4 (5).

Кара-Мурза С.Г. Манипуляция сознанием. М., 2005.

Каптюг И.А. Проблема информационной безопасности: философский и квантово-физические аспекты. Автореф. дисс. ... канд. филос. наук. М., 2009.

Карепова С.Г., Некрасов С.В., Пинчук А.Н. Пропаганда как метод воздействия на общественное сознание: общий теоретический аспект // Вестник НГУЭУ. 2020. № 4. DOI: 10.34020/2073-6495-2020-4-212-229.

Карепова С.Г., Костоломова М.В., Некрасов С.В., Пинчук А.Н. Информационная безопасность в условиях новой социальной реальности: специфика и способы сохранения // Социальные и гуманитарные знания. 2022. Т. 8. № 2 (30). DOI: 10.18255/2412-6519-2022-2-190-203.

Лисичкин В.А., Шелепин Л.А. Третья мировая информационно-психологическая война. М., 1999. URL: https://www.x-libri.ru/elib/lsshl000/00000001.htm (дата обращения: 07.04.2023).

Национальная безопасность России в информационную эпоху. Россия в системе глобальных изменений современной цивилизации. 2015–2016 годы. М., 2017.

Новая социальная реальность: системообразующие факторы, безопасность, перспективы развития. Россия в техносоциальном пространстве: Коллект. монограф. М.; СПб., 2020.

Некрасов С.В. К вопросу о методах воздействия на общественное сознание // Вестник НГУЭУ. 2020. № 4. DOI: 10.34020/2073-6495-2020-4-184-201.

Некрасов С.В., Карепова С.Г. Внушение как метод воздействия на общественное сознание // Социальная политика и социология. 2021. Т. 20. № 3 (140). DOI: 10.17922/2071-3665-2021-20-3-126-134.

Осипов Г.В., Карепова С.Г., Костоломова М.В., Некрасов С.В., Пинчук А.Н. Информационное воздействие на сознание общества в условиях пандемии: теория и методы исследования // Российское общество и государство в условиях пандемии: социально-политическое положение и демографическое развитие Российской Федерации в 2020 году. Коллект. монограф. / Под ред. Г.В. Осипова, С.В. Рязанцева, В.К. Левашова, Т.К. Ростовской; отв. ред. В.К. Левашов. М., 2020. DOI: 10.38085/978-5-905790-48-5-2020-1-532.

Организация защиты информации. URL: https://edu.tltsu.ru/ (дата обращения: 07.04.2023).

Стрельцов А.А. Обеспечение информационной безопасности в России. Теоретические и методологические основы / Под ред. В.А. Садовничего, В.П. Шерстюкова. М., 2002.

Староверов В.И., Левашов В.И. Манипулирование общественным сознанием: социологические аспекты анализа // Социология власти. 2009. № 4.

Указ Президента Российской Федерации от 05.12.2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 07.04.2023).

Указ Президента Российской Федерации от 02.07.2021 N 400 "О стратегии национальной безопасности Российской Федерации" // КосультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 07.04.2023).

REFERENCES

Gorokhov V.G., Syuntyurenko O.V. Tekhnologicheskie riski: informatsionnye aspekty bezopasnosti obshchestva [Technological risks: information aspects of public safety] // Programmnye sistemy i vychislitel'nye metody. 2013. N 4 (5) (in Russian).

Kara-Murza S.G. Manipulyatsiya soznaniem [Mind control]. M., 2005 (in Russian).

Kaptyug I.A. Problema informatsionnoi bezopasnosti: filosofskii i kvantovofizicheskie aspekty [Problems of information security: philosophical and quantum-philosophical aspects]: Avtoref. diss ... kand. filos. nauk. M., 2009 (in Russian).

Karepova S.G., Kostolomova M.V., Nekrasov S.V., Pinchuk A.N. Informatsionnaya bezopasnost' v usloviyakh novoi sotsial'noi real'nosti: spetsifika i sposoby sokhraneniya [Information security in the new social reality: key features and ways of preservation] // Sotsial'nye i gumanitarnye znaniya. 2022. T. 8. N 2 (30). DOI: 10.18255/2412-6519-2022-2-190-203 (in Russian).

Karepova S.G., Nekrasov S.V., Pinchuk A.N. Propaganda kak metod vozdeistviya na obshchestvennoi soznanie: obshchii teoreticheskii aspekt [Propaganda as a method of influence on collective consciousness: general theoretical aspect] // Vestnik of NGUEU. 2020. N 4. DOI: 10.34020/2073-6495-2020-4-212-229 (in Russian).

Lisichkin V.A., Shelepin L.A. Tret'ya mirovaya informatsionno-psikhologicheskaya voina [World Information-Psychological War III]. M., 1999. URL: https://www.x-libri.ru/elib/lsshl000/00000001.htm (data obrashcheniya: 07.04.2023) (in Russian).

Natsional'naya bezopasnost' Rossii v informatsionnuyu epokhu. Rossiya v sisteme global'nykh izmenenii sovremennoi tsivilizatsii. 2015–2016 gody [National security of Russia in the age of information. Russia in the system of global changes of the modern civilization. 2015–2016]. M., 2017 (in Russian).

Novaya sotsial'naya real'nost': sistemoobrazuyushchie faktory, bezopasnost', perspektivy razvitiya. Rossiya v tekhnosotsial'nom prostranstve: kollektivnaya monografiya [New social reality: system-creating factors, security and development prospects: a multi-authored monograph]. M.; SPb., 2020 (in Russian).

Nekrasov S.V. K voprosu o metodakh vozdeistviya na obshchestvennoe soznanie [On the methods of influencing collective consciousness] // Vestnik of NGUEU. 2020. N 4. DOI: 10.34020/2073-6495-2020-4-184-201 (in Russian).

Nekrasov S.V., Karepova S.G. Vnushenie kak metod vozdeistviya na obshchestvennoe soznanie [Suggestion as a method of influencing public consciousness] // Sotsial'naya politika i sotsiologiya. 2021. T. 20. N 3 (140). DOI: 10.17922/2071-3665-2021-20-3-126-134 (in Russian).

Osipov G.V., Karepova S.G., Kostolomova M.V., Nekrasov S.V., Pinchuk A.N. Informatsionnoe vozdeistvie na soznanie obshchestva v usloviyakh pandemii: teoriya i metody issledovaniya [An information influence on the society's consciousness in a

pandemic: theory and research methods] // Rossiiskoe obshchestvo i gosudarstvo v usloviyakh pandemii: sotsial'no-politicheskoe polozhenie i demograficheskoe razvitie Rossiiskoi Federatsii v 2020 godu: kollektivnaya monografiya / Pod red. G.V. Osipov, S.V. Ryazantsev, V.K. Levashov, T.K. Rostovskaya; otv. red. V.K. Levashov. M., 2020. DOI: 10.38085/978-5-905790-48-5-2020-1-532 (in Russian).

Osipov G.V., Pinchuk A.N., Karepova S.G., Nekrasov S.V., Tikhomirov D.A. Social reality construction in the techno-social world: new aspects of sociological conceptualisation // Revista Inclusiones. 2021. Vol. 8. N S2–1.

Organizatsiya zashchity informatsii [The organization of information protection]. URL: https://edu.tltsu.ru/ (data obrashcheniya: 07.04.2023) (in Russian).

Risk in the technological society. Boulder, 1982.

Strel'tsov A.A. Obespechenie informatsionnoi bezopasnosti v Rossii. Teoreticheskie i metodologicheskie osnovy [Information security provision in Russia. Theoretical and methodical foundations] / Pod red. V.A. Sadovnichii, V.P. Sherstyukov. M., 2002 (in Russian).

Staroverov V.I., Levashov V.I. Manipulirovanie obshchestvennym soznaniem: sotsiologicheskie aspekty analiza [Public opinion manipulation: sociological aspect of the analysis] // Sotsiologiya vlasti. 2009. N 4 (in Russian).

Ukaz Prezidenta Rossiiskoi Federatsii ot 05.12.2016 g. N 646 "Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii" [The Russian Presidential Decree of December 05, 2016 N 646 "On approving the information security doctrine of the Russian Federation"]. URL: http://www.kremlin.ru/acts/bank/41460 (data obrashcheniya: 07.04.2023) (in Russian).

Ukaz Prezidenta Rossiiskoi Federatsii ot 02.07.2021 N 400 "O strategii natsional'noi bezopasnosti Rossiiskoi Federatsii" [The Russian Presidential Decree of July 2, 2021 N 400 "On the national security strategy of the Russian Federation"] // Kosul'tantPlyus. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (data obrashcheniya: 07.04.2023) (in Russian).

Vyzovy pandemii i strategicheskaya povestka dnya dlya obshchestva i gosudarstva: sotsial'no-politicheskoe polozhenie i demograficheskaya situatsiya v 2021 godu: monografiya [Pandemic challenges and agenda for the society and country: socio-political and demographic situation in 2021: monograph] / Otv. red. V.K. Levashov, G.V. Osipov, S.V. Ryazantsev, T.K. Rostovskaya. M., 2021. DOI: 10.19181/monogr.978-5-89697-384-3.2021 (in Russian).