https://doi.org/10.23672/SAE.2023.90.54.043

УДК 316

Карепова Светлана Геннадьевна
кандидат социологических наук, ведущий научный сотрудник,
Институт социологии Федерального научно-исследовательского
социологического центра Российской академии наук
svetlran@mail.ru
Пинчук Антонина Николаевна
кандидат социологических наук, старший научный сотрудник,
Институт социологии Федерального научно-исследовательского
социологического центра Российской академии наук
antonina.pinchuk27@bk.ru
Svetlana G. Karepova
candidate of Sociological Sciences, Leading Researcher,
Institute of Sociology of the Federal Center of Theoretical
and Applied Sociology of the Russian Academy of Sciences
Antonina N. Pinchuk
candidate of sociological sciences, leading researcher, Institute
of Sociology of the Federal Center of Theoretical and
Applied Sociology of the Russian Academy of Sciences

К ВОПРОСУ ОБ ОСНОВНЫХ ТЕОРЕТИКО -МЕТОДОЛОГИЧЕСКИХ НАПРАВЛЕНИЯХ ИЗУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ON THE QUESTION OF THE MAIN THEORETICAL AND METHODOLOGICAL DIRECTIONS OF STUDY INFORMATION SECURITY

Аннотация. *Статья посвящена актуальной научно-исследовательской проблематике в области национальной безопасности РФ – основным теоретико – методологическим направлениям изучения информационной безопасности, актуальной и в плане научной теоретизации, и на уровне государственного регулирования. Авторами акцентируется внимание на изучении феномена в рамках современного правового и социально-психологического аспектов. Особое внимание ими уделяется таким основным тематическим научно-исследовательским направлениям, как технологическое (техническое) и гуманитарное, в соответствии с чем,*

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

авторами сформулирован ряд выводов и рекомендаций к научным исследованиям по данной проблематике. В работе использовались первичный анализ материалов, сравнительный анализ научных подходов к пониманию сути феномена, описание, систематизация, обобщение и др. Отмечается значительный научный потенциал и важность изучения информационной безопасности для социума. Среди выводов, которые сделали исследователи в завершение публикации, выделяются такие, как отсутствие общего единого, устоявшегося в гуманитарном, техническом знании определения информационной безопасности; смысловая наполненность феномена в каждой научной парадигме детерминирована ее выраженной спецификой; усиление междисциплинарного подхода к рассмотрению феномена позволит сделать его содержательно наполненным и более изученным; использование системного подхода в исследовании феномена, а также наличие сепарации адекватных методик его сохранения позволит отсекать их недостатки и учитывать положительные стороны в исследованиях; востребована разработка практических методологий (методов, средств, мероприятий, принципов и т.д.) сохранения феномена в различных системах знаний, что позволит вывести его на превентивный уровень.

Annotation. *The article is devoted to the current research problems in the field of national security of the Russian Federation - the main theoretical and methodological directions of studying information security. The article actualizes the study of the phenomenon within the framework of modern legal and socio-psychological aspects. Special attention is paid to such major thematic research areas as technological (technical) and humanitarian. In accordance with what the authors have formulated a number of conclusions and recommendations for scientific research on this issue. The primary analysis of materials, comparative analysis of scientific approaches, description, systematization, generalization, etc. were used in the work. Among the conclusions that the researchers made at the end of the publication, we highlight such as: the lack of a common unified, well-established definition of information security in humanitarian, technical knowledge; the semantic fullness of the phenomenon in each scientific paradigm is determined by its pronounced specificity; strengthening the interdisciplinary approach to the consideration of the phenomenon will make it meaningful and more studied; the use of a systematic approach in the study of the phenomenon, as well as the presence of separation of adequate methods of its preservation, will cut off their shortcomings and take into account the positive aspects in research; There is a demand for the development of practical methodologies (methods, means, measures, principles, etc.) for preserving the phenomenon in various knowledge systems, which will bring it to a preventive level.*

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

Ключевые слова: *информационная безопасность, феномен, социальная реальность, сознание, влияние, социум, понятие, научные подходы.*

Keywords: *information security, phenomenon, social reality, consciousness, influence, society, concept, scientific approaches.*

Введение. Становление новой глобальной социальной реальности, начавшееся на рубеже XX и XXI веков ознаменовалось глубинными социетальными трансформациями, получившими распространение на фоне масштабного развития информационных и цифровых технологий. По сути, речь идет о формировании и развитии в рамках современной социальной реальности, детерминирующего ее высокотехнологичного информационного пространства, пронизанного инновационными информационно-цифровыми технологиями, приносящими социуму как новые возможности, так и латентные разноплановые угрозы в перспективе. Следует отметить новаторские качества данного феномена, которые не только нуждаются в созидательном использовании заложенного в нем потенциала, но и несут в себе новые риски и вызовы, требуют научного изучения, концептуализации и учета в государственной политике. Особое значение для социума начинают приобретать вопросы безопасного развития информационной сферы.

Актуальность изучения информационной безопасности: современный правовой и социальный аспекты. Бифуркационная природа данного феномена в своих рисковых проявлениях осознается социумом и регулируется им на ключевом законодательном уровне управления динамикой социальной реальности. Все порождаемые угрозы и вызовы, включая информационное направление, актуализированы и документально отражены в ряде государственных документов (Стратегия национальной безопасности России от 02.07.2021 г. №400, ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ, Стратегия развития информационного общества в РФ на 2017-2030 гг. от 31.12.2015 г. № 683 и т.д.), как требующие учета и предотвращения.

Информационная безопасность, в рамках нормативного регулирования, является одним из девяти сформулированных в Стратегии национальной безопасности РФ стратегических приоритетов, включенных в систему сохранения национальной безопасности страны. Введение феномена в систему приоритетов обусловлено тем фактом, что именно данные вопросы и проблемы пронизывают остальные приоритеты, являясь системообразующими.

Главным *фактором риска в системе сохранения информационной безопасности является ее социально-психологический аспект.* Речь идет об опасных и агрессивных информационных «атаках», «раскачивающих» и

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

деморализующих коллективное сознание социума, отвечающее за его социально-психологическую стабильность как таковую. Фактически, внешне, информационное воздействие происходит на социокультурной (телевидение, печатные издания и др.) платформе, но внутренне оно влияет на тот базис, что отвечает за формирование и поддержание глубинного устоявшегося в социуме ценностного ряда. Как правило, под так называемый информационный «удар» попадают институты семьи, религии, морали, образования и др. Это тот социокультурный пласт, что отвечает за процесс и качество воспитания не только новых поколений, их взглядов и ценностей, но также стабильное удержание и укрепление социально одобряемого ценностного ряда у остальных социальных групп. Именно это стратегическое основание будущего человечества попадает под негативное информационное воздействие. Можно вести речь о затрагивании глубинных слоев психики общества, его сознания и уровень когнитивных процессов, благодаря которым, в целом, формируются стратегии будущей жизни и «картины мира». Как правило, информационное воздействие использует особенности психики и рассчитано на охват широкой аудитории. В чем кроется опасность? Проникновение извне на глубинный уровень сознания оказывает прямое влияние на содержание и качество когнитивных процессов в нем. Подобное внедрение всегда чревато, так как принятие ценностей, выбранных или навязанных кем-то извне, порождает и изменение цивилизационных ценностей, легитимных алгоритмов поведения и др., сформированных на основе исторического опыта человечества. Так перечеркиваются устоявшиеся в социуме стратегии и практики, стабилизирующие его функционирование. Или фактически, опасность состоит в том, что происходит разрушительное информационное воздействие на процесс конструирования и проектирования социумом желательной для него социальной реальности, или так называемый процесс «…объективизации субъективной деятельности или субъективности как таковой» [1]. То есть, через негативную или позитивную информацию происходит создание новых установок, мотиваций и, как следствие, диспозиций и стратегий, на основании которых будут приниматься значимые для общества решения: Куда и в каком направлении ему развиваться, что для него теперь ценно? и т.д. Именно информационный план как инструмент своеобразной «перекодировки» реальности имеет решающее значение в определении той парадигмы развития, в которой обществу предстоит жить и которую он выберет сам. Предугадать последствия информационного воздействия трудно; эта сфера не только ставит вопросы сохранения ее безопасности, информационных девиаций, но и “аутогеномутацию” социальной жизни как таковой и человека, в целом. На повестке дня «…стоят

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

важные онтологические вопросы, позволяющие осуществить выход на уровень своеобразного информационного «футуризма» [1].

Таким образом, сохранение *информационной безопасности актуально и в плане научной теоретизации, и на уровне государственного регулирования.*

Основные теоретико-методологические направления изучения информационной безопасности в России. Разработка общей дефиниции информационной безопасности – процесс сложный и содержательно вариативный, не имеет единого значения и детерминирован постоянным развитием как социальной реальности (общая перманентная информатизация социума, изменение подходов к системе безопасности страны в нормативных законодательных документах и др.), так и внутренним изменением самого феномена. Несмотря на его выраженную актуализацию и практическую значимость, в рамках различных систем междисциплинарного знания (гуманитарное, техническое, социальное, правовое, психологическое и др.) также осуществляется разнонаправленное осмысление феномена, что усиливает его содержательную многогранность и не способствует целостному пониманию и формулированию единой дефиниции. Феномен не имеет единственно верного устоявшегося в научном знании определения и по-разному раскрывается в научной литературе, законах, технической документации и т.д. Следует выделить несколько основных тематических направлений, объединяющих ключевые подходы к его пониманию. К ним относится технологическое (техническое), гуманитарное, включающее междисциплинарные (социальные, правовые, психологические и др.) подходы.

Технологическое (техническое) направление теоретизирования. Данное направление научного исследования информационной безопасности широко представлено разработками таких советских и российских ученых, как А.Н. Асаул, В.А. Васенин, А.И. Ивлев, М.В. Арсентьев, А.В. Тонконогов и др. Большой тематический блок представлен работами А.Г. Глушкова, А.А. Смирнова, В.В. Цыганова, В. Н. Ясенева, В.В. Кульбы, Н.А. Махутова, М.М. Гаденина и др. Это направление актуализирует скрытые и опасные свойства информационного пространства как такового, где информационная безопасность обеспечивает защиту от информационных воздействий, а также поддерживает инфраструктуру за счет изучения развития индустрии информатизации и ее, практически неограниченных возможностей, представленных социуму. Речь идет о необходимости обеспечения безопасности информационной инфраструктуры (больших технических систем, программного обеспечения и др.) комплексом мероприятий по защите средств передачи и хранения информационного контента государственного и частного формата.

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

Информация предстает, как смысловая часть технической сферы и включена в «....защищённость сферы информационно-технической от программных, разведывательных и радиоэлектронных воздействий, направленных на хищение информации, прекращение функционирования или вывод из строя информационно-технических объектов, информационной инфраструктуры страны, включая системы военного и государственного управления и т.д.» [2]. Особое внимание уделяется методологии защиты (приемы, способы, мероприятия и т.д.) информации, в целом, где осуществляется «...анализ компьютерных программ на наличие уязвимостей, антивирусные технологии, идентификация пользователей с применением электронных ключей и тд. экранирование, фильтрация информации, разграничение доступа пользователей, мониторинг состояния системы и выработки мер реагирования, шифрование и дешифрование информации, проверка целостности информации и др.» [2] .

Отдельное направление исследований - компьютерный терроризм, где феномен отвечает за «...совокупность мер, позволяющих обнаружить и предотвратить действия, способные привести к несанкционированному доступу к охраняемой законом информации, нарушению ее защищенности, к разрушению сети посредством вывода из строя системы управления» [3].

В рамках данной тематики обозначенное направление теоретизирования сводится сугубо к технической и инструментальной роли, но в нем избегаются социально-психологические аспекты информационного взаимодействия или его акторы (человек, социум, государство), средовые социетальные (социальные, политические, правовые и др.) детерминирующие аспекты,

Гуманитарное направление научного рассмотрения феномена базируется на разработках таких социальных ученых, как Г.В. Осипов, М.К. Горшков, С.П. Расторгуев, Р.М. Юсупов, И.Д. Фомичёва и др. Экономический срез представлен работами А.В. Зуева, Л.В. Мясникова. Политический и геополитический план отражен в исследованиях С.Г. Кара-Мурзы, И.Н. Панарина, А.А. Кокошина, Е.О. Кубякина, И.Ю. Сундиева, А.Ф. Федорова и др.

Сторонники данного подхода раскрывают сущность феномена через его социальную природу, объясняя это тем, что помимо его физического существования в мире, где он подвластен изучению посредством инструментария точных наук (механика, физика, математика и др.), информация является и глубоко социальным феноменом, так как создана и существует именно благодаря человеку. В таком формате ее исследуют уже посредством социально-научного знания (психология, философия, право и др.). Такой междисциплинарный ракурс позволяет изучить информационную безопасность с точки зрения проблем, актуализирующих духовно-

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

нравственный аспект общества, его ценностные характеристики, вопросы соблюдения прав и свобод граждан в информационной области, затронуть правовое регулирование сферы, коснуться инструментальных проблем обеспечения информационной безопасности, обеспечение безопасности сознания социума. Речь, безусловно, идет и о выработке мер защиты от информационных воздействий. В отличие от первого направления, социуму предлагается более широкий комплекс мер защиты как на уровне информационной среды, так и самих субъектов информационных взаимодействий. В рамках данной парадигмы следует выделить основные гуманитарные подходы. Речь пойдет о правовом (нормативном), психологическом направлениях его рассмотрения.

Правовой (нормативный) подход представлен исследованиями ученых-правоведов П.У. Кузнецова, Е.К. Волчинской, И.Л. Бачило, Т.Я. Хабриевой, М. И. Дзлиева, А.Л. Романовича и А.Д. Урсула, Г.А. Атаманова и др., чьи работы отражают регулирующую роль нормопрактик в информационном пространстве. Особое значение, как регулятора данной сферы, приобретает свод законов, охватывающих информационную деятельность. Вопросы информационной безопасности всегда были актуализированы в законотворческой деятельности и отражены в таких документах, как Доктрина информационной безопасности от 05.12.2016 г. № 646, Стратегия развития информационного общества в РФ на 2017-2030 гг. от 31.12.2015 г. №683 и т.д. Исключительная значимость информационной безопасности отражена и в Стратегии национальной безопасности РФ от 02.07.2021 г. № 400 и др., где, как уже было отмечено выше, феномен вошел в девять стратегических приоритетов сохранения.

Ученые-правоведы в научных исследованиях, как правило, используют уже закрепленные и устоявшиеся трактовки информационной безопасности, где «…информационная безопасность РФ - 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 РФ, оборона и безопасность государства» [4]. Но данное направление «приняло на себя» формат, предельно общего и содержательно не четкого изложения, свойственного стилистике свода законов и где смысловая обобщенность не позволяет отразить глубинный уровень феномена. В настоящее время наиболее полным определением феномена можно считать его усовершенствованный в рамках междисциплинарного взаимодействия ученых вариант, где «…состояние защищённости личности, общества и государства от внутренних и внешних

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

угроз в данной сфере можно разделить на два вида: безопасность информационно-техническая и безопасность информационно-психологическая». [2]. Феномен рассматривается с точки зрения и первого, и второго подходов, описанных выше, однако дополнен с учетом информационно-технической и информационно-психологической составляющих.

Психологический подход, актуализирующий субъективную социально-психологическую составляющую феномена, разрабатывается такими учеными, как А.Л. Журавлев, А.Е. Войскунский, А.Ю. Добродеев, И.В. Бутусов, Л.В. Астахов и др. Исследователи, учитывая психологическую проблематику феномена, разрабатывают ее через призму ключевого актора социальной реальности – человека с его субъективными особенностями. Как правило, все теоретические концепты выстраиваются вокруг информационного воздействия на человека или социум, в целом, и на его сознание с учетом психологических характеристик. Рассмотрение феномена происходит как некой части, ведущейся в социуме гибридной войны, для которой свойственно наличие борьбы, противника, информационных методов нападения и противоборства и т.д. Речь идет о защите психологического состояния человека, его ментального здоровья и сознания от агрессивного информационного воздействия.

Психологический принцип теоретизирования сводится к тому, что феномен отвечает за «...состояние защищенности субъекта, выражающееся в безопасности информации субъекта и его информационно-психологической безопасности, достигаемое в ходе процессов (создания, передачи, получения, хранения) как на содержательном, так и на представительном уровнях информации» [5] Также, феномен часто рассматривается как система мер, принципов, методов и т.д., обеспечивающая информационные потребности социума и его безопасность от негативного информационного влияния. Это направление активно развивается, что и положило начало новому ответвлению феномена - информационно-психологической безопасности. В обозначенные выше направления теоретизирования также входят и другие научные подходы, дающие углубленный взгляд на данную проблематику. Но все они дополняют и углубляют уже имеющиеся научные парадигмы.

Целесообразно сформулировать ряд выводов и рекомендаций к потенциальным исследованиям по данной проблематике. К ним относятся:

- отсутствие общего единого устоявшегося в гуманитарном, техническом знании определения информационной безопасности;

- смысловая наполненность феномена в каждой научной парадигме детерминирована ее выраженной спецификой;

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

- усиление междисциплинарного подхода к рассмотрению феномена позволит сделать его содержательно наполненным и более изученным;

- использование системного подхода в исследовании феномена, а также наличие сепарации адекватных методик его сохранения позволит отсекать их недостатки и учитывать положительные стороны в исследованиях;

- востребована разработка практических методологий (методов, средств, мероприятий, принципов и т.д.) сохранения феномена в различных системах знаний, что позволит вывести его на превентивный уровень;

- актуализирована просветительская работа с социумом по формированию устойчивого коллективного сознания с использованием социально-психологических методов, позволяющих отсекать негативное воздействие;

- ориентир на разработку проблематики безопасности сознания социума через мировоззренческие ориентиры, ценности, диспозиции, что позволит сформировать навыки безопасного поведения в информационной среде и иметь готовность к информационному противоборству в случае необходимости и т.д.

Вывод. Безусловно, обозначенные направления научного осмысления информационной безопасности, а также выводы и рекомендации к возможным научным исследованиям нельзя считать исчерпывающими, поскольку постоянно изменяется как сама социальная реальность, в которой развивается феномен, так и информационная безопасность, детерминируемая ею, а также методы ее сохранения. Следует отметить выраженную для социума важность данных исследований и весомый научно-исследовательский вклад ученых в их разработку. Актуальность научного изучения феномена будет только возрастать.

Конфликт интересов

Не указан.

Рецензия

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

Conflict of Interest

None declared.

Review

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

Литература

1. Карепова С.Г., Пинчук А.Н, Некрасов С.В. Национальная безопасность: тенденции, перспективы, научно-практическая основа для укрепления – система показателей и индикаторов. Гуманитарные, социально-экономические и общественные науки. 2018 №9. - С. 36.

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru

2. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Понятийный аппарат национальной и международной безопасности. Науч. рук. член-корр. РАН Махутов Н.А. - М.: МГОФ «Знание», 2022. - 960 с., ил.

3. Васенин В.А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности. – М.: МЦНМО, 2004. - С. 80.

4. Доктрина информационной безопасности РФ от 05.12.2016 г. № 646

5. Астахова Л.В. Информационная безопасность: герменевтический подход. – М.: РАН, 2010. - С. 22.

Literature

1. Karepova S.G., Pinchuk A.N., Nekrasov S.V. National security: trends, prospects, scientific and practical basis for strengthening – a system of indicators and indicators. Humanities, socio-economic and social sciences. 2018 No. 9. p. 36.

2. Security of Russia. Legal, socio-economic, scientific and technical aspects. Conceptual apparatus of national and international security. Scientific supervisor Corresponding member of the Russian Academy of Sciences Makhutov N. A. - M.: Moscow State Educational Institution "Knowledge", 2022. — 960 p., ill.

3. Vasenin V. A. Information security and computer terrorism // Scientific and methodological problems of information security. - Moscow: ICNMO, 2004. - p. 80.

4. Information Security Doctrine No. 646 dated 05.12.2016

5. Astakhova L. V. Information security: hermeneutical approach. - Moscow: RAS, 2010. - p. 22.

ISSN 2220-2404 (печать) ISSN 2221-1373 (On-line)
https://online-science.ru