Знать, чтобы предвидеть...

To know so that to foresee...

УДК 101.8:316.3(043.3)

ОНТОЛОГИЧЕСКИЕ ОСНОВАНИЯ ФИЛОСОФСКО-СОЦИОЛОГИЧЕСКОГО ОСМЫСЛЕНИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ

Е. М. БАБОСОВ [1)]***, Ю. Л. БАНЬКОВСКАЯ*** [2)]

[1)] *Институт социологии НАН Беларуси, ул. Сурганова, 1, корп. 2, 220072, г. Минск, Беларусь*
[2)] *Белорусский государственный аграрный технический университет, пр. Независимости, 99, 220023, г. Минск, Беларусь*

Аннотация. Отмечается, что в условиях развития и распространения информационно-коммуникационных технологий все большую актуальность приобретает поиск новых механизмов поддержания стабильности в функционировании социума. Выявляются онтологические основания такого феномена, как информационная война. Отмечаются онтологические, антропологические и социально-аксиологические факторы конституирования нового пространства информационных войн. Подчеркивается, что информационное противостояние приводит к неустойчивости развития общества. Перечисляются качественные признаки сетевых структур: горизонтальная организация, неустойчивость, опосредованность, динамичность, анонимность, мгновенность трансляции информации, отсутствие географических и темпоральных границ, бесконтактность.

Ключевые слова: информационная война; конфликт; информация; сетевые структуры; безопасность.

Образец цитирования:
Бабосов ЕМ, Баньковская ЮЛ. Онтологические основания философско-социологического осмысления информационной войны. *Журнал Белорусского государственного университета. Социология.* 2024;2:29–34.
EDN: TUHGNA

For citation:
Babosov EM, Bankouskaya YuL. The ontological foundations of the philosophical and sociological understanding of the information war. *Journal of the Belarusian State University. Sociology.* 2024;2:29–34. Russian.
EDN: TUHGNA

Авторы:
Евгений Михайлович Бабосов – доктор философских наук, академик НАН Беларуси, профессор; главный научный сотрудник.
Юлия Леонидовна Баньковская – кандидат философских наук, доцент; доцент кафедры социально-гуманитарных дисциплин инженерно-технологического факультета.

Authors:
Evgenii M. Babosov, doctor of science (philosophy), academician of the National Academy of Sciences of Belarus, full professor; chief researcher.
babosov@yandex.ru
Yuliya L. Bankouskaya, PhD (philosophy), docent; associate professor at the department of social and humanitarian disciplines, faculty of engineering and technology.
ulia_bank@tut.by
https://orcid.org/0000-0001-9287-7261

Журнал Белорусского государственного университета. Социология. 2024;2:29–34
Journal of the Belarusian State University. Sociology. 2024;2:29–34

THE ONTOLOGICAL FOUNDATIONS OF THE PHILOSOPHICAL AND SOCIOLOGICAL UNDERSTANDING OF THE INFORMATION WAR

E. M. BABOSOV[a]***, Yu. L. BANKOUSKAYA***[b]

[a]*Institute of Sociology, National Academy of Sciences of Belarus, 1 Surganava Street, 2 building, Minsk 220072, Belarus*
[b]*Belarusian State Agrarian Technical University, 99 Niezaliezhnasci Avenue, Minsk 220023, Belarus*
Corresponding author: Yu. L. Bankouskaya (ulia_bank@tut.by)

Abstract. It is noted that in the context of the development and spread of information and communication technologies, the search for new mechanisms for maintaining stability in the functioning of society is becoming increasingly relevant. The ontological foundations of such a phenomenon as information warfare are revealed. The ontological, anthropological and socio-axiological factors of the constitution of the new space of information wars are noted. It is emphasised that information confrontation leads to instability in the development of society. The qualitative features of network structures are listed: horizontal organisation, instability, mediation, dynamism, anonymity, instantaneous transmission of information, absence of geographical and temporal boundaries, contactlessness.

Keywords: information warfare; conflict; information; networks; security.

Сегодня, в условиях ухудшения мировой геополитической обстановки, значительно увеличилось количество информационных угроз, затрагивающих государственные интересы. Увеличение объема информации и обеспечение широкого доступа к ней, с одной стороны, способствуют большей осведомленности граждан о происходящих в мире событиях, позволяя им сформировать свое мнение о той или иной проблеме, а с другой стороны, приводят к манипулированию общественным сознанием.

Одним из следствий развития и распространения информационно-коммуникационных технологий (ИКТ) является интенсификация информационных войн. В границах сетевого пространства разворачиваются многочисленные конфликты. Угрозой мирового масштаба является киберпреступность. Сеть можно рассматривать «и как способ бытия и сознания человека (группы людей, общества, мира), и как самопорождение человека, в том числе на ментальном и духовном уровнях» [1, с. 52].

Информационная война представляет собой сложный процесс социально-политических и военно-технологических взаимодействий, направленный на качественное изменение сложившегося мироустройства посредством использования ИКТ. Результатом комплексного использования информационного оружия является достижение определенных экономических, политических и социокультурных целей. Конфликтующие стороны предпринимают действия, направленные на дестабилизацию информационной системы противника, и одновременно принимают меры по укреплению и защите собственной информационной системы [2, с. 69].

Онтологическим основанием информационной войны являются сведения, распространяемые в средствах массовой коммуникации и интернете. Они способны не только влиять на общественные процессы, но и формировать социальное бытие человека. Сетевизация и цифровизация общества обусловили появление новых возможностей для обработки, хранения, накопления, передачи и создания информационных потоков. По критерию эффективности и стоимости современное информационное оружие значительно превосходит другие виды вооружения [3, с. 13]. По степени воздействия на массовое сознание оно сопоставимо с оружием массового поражения на поле боя [4, с. 79]. Интернет, являясь «глобальным коммуникационным медиумом, который впервые сделал возможным общение многих людей со многими другими в любой момент времени и в глобальном масштабе» [5, с. 15], содействовал включению человека в глобальное информационное пространство, которое изменило сложившуюся модель взаимоотношений акторов и привычную коммуникативную среду. Социальные сети и иные виртуальные сообщества, обладая возможностями для мгновенной трансляции информации, способны манипулировать общественным мнением.

Действенность той или иной информации обеспечивается благодаря акторам, которые создают, транслируют, воспроизводят, нейтрализуют и контролируют данные. Специфика проявления этих акторов в интернете обусловлена наличием у них атрибутов индивидуальности и социальности. В виртуальном пространстве отражено все многообразие социальных взаимоотношений, характер которых определяется как индивидуальными характеристиками субъектов, особенностями их мировосприятия, так и актуальными социальными процессами. Акторами в данном случае могут выступать дискретные индивидуальные, корпоративные или социальные объединения, например группы людей, подразделения в системе государственных учреждений, национальные государства и т. д. [6, p. 17].

Онтологическим основанием конституирования той или иной сети является механизм создания и выстраивания социальных отношений между акторами. Сетевые связи действуют как трансляторы информа-

ции, знаний, материальных ресурсов [7, p. 389–390]. Осуществляя определенную деятельность и используя коммуникационные, информационные и финансовые ресурсы [8, с. 35], актор удостоверяет свое местоположение. Французский философ и антрополог Б. Латур отмечал, что действие такого актора представляет собой инструмент, направленный на трансформацию информационного поля. Соответственно, актором становится любой носитель информации, представляемый компьютерной программой, вирусом и являющийся «источником действия» [9, с. 182]. По мнению М. Грановеттера, актор, как действующее лицо [10, p. 1422], выступает в качестве неопределенного феномена, создающего и изменяющего свою сущность в процессе взаимодействия с интернет-структурами.

Качественными признаками сетевых структур выступают горизонтальная организация, неустойчивость, опосредованность, динамичность, анонимность, мгновенность трансляции информации, отсутствие географических и темпоральных границ, бесконтактность.

Сети конституируют новые возможности для деструктивного использования информации. Информационные сетевые структуры оказывают сильнейшее давление на органы чувств человека [11, с. 284]. Недостоверность, фрагментарность и разрозненность сведений о той или иной проблеме приводят к тому, что человек лишается возможности составить ее целостный образ. Российские исследователи С. М. Виноградова и И. А. Михальченко отмечают, что манипулирование индивидуальным и общественным сознанием на первоначальном этапе может усиливать существующие в нем идеалы и нормы поведения, а впоследствии трансформировать взгляды на события и кардинальным образом изменять жизненные установки [12, с. 49].

Взаимоотношения сетевых элементов выстраиваются на основании формальных и неформальных связей, продуцируемых социальной практикой, ценностями, потребностями и ресурсами общества. Российский исследователь Н. И. Бритвин трактует социальную сеть как «социальную структуру, состоящую из узлов / акторов (примерами узлов могут быть отдельные люди, группы людей или сообщества), связанных между собой одним или несколькими способами (главным образом нецентрализованного типа) посредством социальных взаимоотношений» [13, с. 46]. Американские ученые А. Марин и Б. Веллмен акцентируют внимание на структурной организации сети, характеризуя данный феномен как «набор узлов, связанных одним или более типом отношений»[1] [14, p. 11]. Таким образом, содержательными элементами сетевой структуры являются акторы, расположенные в ее точках или вершинах и взаимодействующие между собой посредством объединения в клики или узлы. Оказывая влияние на внутренний мир человека, его ценности, представления и убеждения, сетевые структуры формируют определенную модель взаимоотношений между акторами, обусловливают специфику их деятельности в сетевом образовании, занимаемое ими положение, характер их взаимосвязей с другими сетевыми элементами и т. д. Они могут существовать как в форме универсального социального механизма, оказывающего давление на социальное окружение в целях формирования того или иного видения проблемной ситуации, так и в форме структурного компонента, ориентированного на обеспечение стабильности социального развития.

Сетевая структура формируется таким образом, что у каждого узла существует множество связей с другими кликами. Благодаря этому повышается вероятность накопления информации, создается множество источников ее трансляции, распределения, концентрации и интеграции. Центральные узлы могут оказывать значительное воздействие на проблемную ситуацию, поскольку акторы, находящиеся на периферии сетевой структуры, потребляют сведения, предоставляемые им центральными кликами. В то же время периферийные акторы могут распространять недостоверные сведения и влиять на процессы, происходящие в социальной реальности.

Процесс распространения информации в интернете сложно регулировать и контролировать, поэтому риск разгорания информационных войн в виртуальном пространстве постоянно растет. Наличие нескольких узловых точек, представленных множеством периферийных акторов, которые распространяют информацию и содействуют формированию новых кликов, приводит к тому, что нивелировать или снизить степень деструктивного воздействия узлов на определенную ситуацию становится невозможным. В случае блокировки или исчезновения одних влиятельных центров возникнут новые, потенциально взаимозаменяемые лидеры. Следовательно, сетевые структуры обладают способностью к самоорганизации, позволяющей им сохранить условия своего функционирования и снизить риск деструктивных последствий. Близость связей между акторами содействует расширению возможностей координации их действий в конфликтной ситуации. Вместе с тем формируются дополнительные механизмы для манипулирования общественным мнением.

Асимметрия власти и влияния приводит к тому, что периферийные элементы могут оказывать значительное воздействие на конфликт. Расширение возможностей доступа населения к информации повышает уровень его адаптивности к социальным и политическим условиям, но в то же время продуцирует новые риски. Применение периферийных элементов вызвано необходимостью увеличения числа взаимосвязей узлов в целях более быстрого нахождения и трансляции информации. Установление дополнительных

[1] Здесь и далее перевод наш. – *Е. Б., Ю. Б.*

связей между узлами расширяет возможности акторов, а именно позволяет им влиять на протекание и разрешение информационного противостояния. Посредники, связывая между собой акторов, координируя их действия и влияя на их приоритеты и установки, создают условия для динамики конфликта.

Следствием сетевизации и цифровизации общества стало искусственное конституирование новых смыслов, которые не укладываются в объективную реальность. Виртуализация ментальности привела к тому, что на восприятие человеком событий, происходящих в обществе, все более значимое воздействие начали оказывать образы. Использование новых инструментов для психологического давления на общественное мнение привело к тому, что информационные войны приобрели гибридную форму. Информационные атаки направлены на изменение человеческого сознания. Они «используются как психотропное оружие, как эффективный инструмент ведения широкомасштабных информационно-психологических войн» [15, с. 209].

Традиционно войны были ограничены определенными географическими рамками. С распространением ИКТ война обрела новые формы. Сегодня информационное противостояние выходит за географические границы государств. При этом снижается значимость гендерных и возрастных характеристик акторов. Их физическая дистанцированность создает иллюзию безнаказанности за совершаемые действия. Открытый доступ к информации в условиях отсутствия эффективных мер по ее защите нередко приводит к использованию тех или иных данных в преступных целях.

Информационная война может быть анонимной. Анонимность создает «эффект расслабления» [16, p. 43–52] и вседозволенности. Данные обстоятельства, с одной стороны, способствуют развитию креативности личности, расширяют возможности для продуктивного обсуждения противоречий и принятия эффективного решения, но с другой стороны, увеличивают пространство информационного противостояния вследствие привлечения новых акторов. Сложность идентификации людей, распространяющих недостоверную информацию, и большие временные затраты на опровержение сфальсифицированных данных не позволяют противостоять дезинформированию. Возникают ситуации, при которых акторы, не обладая истинным знанием о проблеме, начинают действовать в соответствии с имеющимися у них искаженными представлениями. Возможность анонимного общения приводит к тому, что «без угрозы наказания и социального одобрения люди говорят и делают такие вещи, которые бы не стали говорить и делать под своим именем, позволяют себе гораздо больше, чем привыкли в обычной жизни, где они несут ответственность за свои поступки и высказывания» [17, с. 186].

Основным методом ведения информационной войны выступает производство фейков. Они являются ключевым инструментом для манипулирования поступками и действиями людей. Фейковые сообщения ориентированы как на привлечение внимания разных социальных групп, так и на их побуждение к определенным действиям. Спамеры могут распространять недобросовестную рекламу, нелегальный контент, внедрять в компьютеры пользователей вредоносные программы, а также получать доступ к личной информации [18, с. 97].

Можно выделить следующие способы формирования фейковых данных:

- создание и распространение недостоверной информации о событиях, имеющих социальное или политическое значение (данные действия направлены то, чтобы посеять панику, страх и смятение среди граждан, побудить их к протестам);
- использование старых видео- и фотоматериалов для экстраполяции данных на настоящую ситуацию;
- ложная интерпретация фотографий;
- проведение постановочных съемок;
- использование фрагментов фильмов, видеоигр и иных видеокадров для видеомонтажа.

В настоящее время страны Западной Европы, прежде всего входящие в блок НАТО, ведут информационную войну против России и Беларуси. Объектом информационного воздействия, как отмечают исследователи, выступают «войска Российской Федерации, которые участвуют в проведении специальной военной операции на Украине… основные группы населения России и Беларуси… политические деятели и население стран Запада, политические деятели и население незападных и антизападных стран» [19, с. 20]. Одним из передовых подразделений белорусской армии является рота информационных технологий, задача которой состоит в обеспечении информационной безопасности государства.

Кибертерроризм, как оружие гибридной войны, направлен на подрыв политической, экономической, социальной и военной стабильности общественного развития. Существуют следующие формы кибертерроризма:

- атаки на банковские и коммерческие структуры, учреждения сферы здравоохранения, образования и т. д.;
- социально-психологическое давление на людей путем инициации злонамеренных тревожных слухов, продуцирующих широкий общественный резонанс;
- использование компьютерных вирусов (взлом и повреждение серверов, кража личной информации, а также данных, имеющих государственную важность);
- атаки на систему безопасности, управленческие структуры государства.

Сегодня обеспечение информационной безопасности государства становится необходимым условием национальной безопасности. Новые угрозы требуют разработки действенных правовых норм,

касающихся распространения информации, а также формирования новой системы ценностей, отвечающей современным условиям развития общества.

Перед государством стоит ряд вопросов, связанных с безопасным использованием ИКТ. Распространяемая в интернете информация должна быть объективной и не должна противоречить государственной политике.

Таким образом, информационные войны становятся новой угрозой для современного общества. Следствием развития и распространения сетевых технологий стало повышение риска информационных атак. Пространство ведения информационной войны постоянно расширяется, в результате чего в противостояние вовлекается все больше государств. Исследование онтологических оснований и факторов информационной войны приобретает высокую социально-политическую значимость.

Сетевые структуры оказывают двойственное влияние на информационную среду. С одной стороны, они снижают уровень информационной неопределенности, создавая конструктивные условия для разрешения противоречий. С другой стороны, деструктивное использование сведений приводит к конфликтам. Применение информационного оружия позволяет контролировать огромные территории, оказывать воздействие на социальные, политические и экономические процессы во многих государствах. Эффективность данного инструмента обусловлена полифункциональностью его применения, отсутствием темпоральных и географических границ, расширением пространства использования, мультимедийностью, трудностью верификации и незначительными финансовыми вложениями. В связи с этим обеспечение информационной безопасности выступает одним из ключевых условий сохранения государственности.

Библиографические ссылки

1. Шенцева ЕА. Сетевой подход: истоки и перспективы. *Идеи и идеалы.* 2012;2(12):48–57.
2. Расторгуев СП. *Информационная война*. Москва: Радио и связь; 1998. 415 с.
3. Расторгуев СП. *Математические модели в информационном противоборстве: экзистенциальная математика.* Москва: АНО ЦСОиП; 2014. 259 с.
4. Новосельцев ВИ, Тарасов БВ. *Системная теория конфликта*. Москва: Осипенко А. И.; 2011. 333 с.
5. Кастельс М. *Галактика Интернет: размышления об интернете, бизнесе и обществе.* Матвеева А, переводчик; Харитонов В, редактор. Екатеринбург: У-фактория; 2004. 327 с.
6. Wasserman S, Faust K. *Social network analysis: methods of applications*. Cambridge: Cambridge University Press; 1994. 825 p.
7. Pallotti F, Lomi A. Network influence and organisational performance: the effects of tie strength and structural equivalence. *European Management Journal.* 2011;5(29):389–403. DOI: 10.1016/j.emj.2011.02.005.
8. Анисимова НА, Добаев ИП. *Сетевые структуры террористов на Северном Кавказе*. Москва: Редакция журнала «Социально-гуманитарные знания»; 2016. 143 с.
9. Латур Б. Об акторно-сетевой теории. Некоторые разъяснения, дополненные еще большими усложнениями. *Логос*. 2017;1(27):173–197. DOI: 10.22394/0869-5377-2017-1-173-197.
10. Granovetter M. Threshold models of collective behaviour. *The American Journal of Sociology*. 1978;6(83):1420–1443.
11. Романов ОА. *Восточнославянская цивилизация в горизонте открытой истории*. Гродно: Гродненский государственный университет имени Янки Купалы; 2018. 334 с.
12. Виноградова СМ, Михальченко ИА. Информационный обмен. Информационные войны. В: Вус МА, редактор. *Информационное общество. Информационные войны. Информационное управление. Информационная безопасность.* Санкт-Петербург: Санкт-Петербургский государственный университет; 1999. с. 25–68.
13. Бритвин НИ. Социальные сети как прообраз общественного устройства. *Власть*. 2008;1:45–49.
14. Marin A, Wellman B. Social network analysis: an introduction. In: Scott J, Carrington PJ, editors. *The SAGE Handbook of Social Network Analysis.* London: SAGE Publications Ltd.; 2011. p. 11–25.
15. Кириченко АВ. Информационно-психологические войны: современные тенденции и технологические возможности. *Акмеология*. 2015;4(56):209–214.
16. Green MC. Trust and social interaction on the Internet. In: Joinson A, editor. *Oxford Handbook of Internet Psychology*. New York: Oxford University Press; 2007. p. 43–52.
17. Бочавер АА, Хломов КД. Кибербуллинг: травля в пространстве современных технологий. *Психология. Журнал Высшей школы экономики*. 2014;3(11):177–191.
18. Красовская НР, Гуляев АА. К вопросу о контроле фейков, дипфейков, фейковых аккаунтов в интернете. *Вестник Удмуртского университета. Серия: Социология. Политология. Международные отношения.* 2021;1(5):96–99. DOI: 10.35634/2587-9030-2021-5-1-96-99.
19. Журавлева ЛА, Зарубина ЕВ, Ручкин АВ, Симачкова НН, Чупина ИП. Современная информационная война. *Образование и право*. 2022;9:18–26. DOI: 10.24412/2076-1503-2022-9-18-26.

References

1. Shentseva EA. Network approach: origins and prospects. *Idea and ideals*. 2012;2(12):48–57. Russian.
2. Rastorguev SP. *Informatsionnaya voina* [Information war]. Moscow: Radio i svyaz'; 1998. 415 p. Russian.
3. Rastorguev SP. *Matematicheskie modeli v informatsionnom protivoborstve: ekzistentsial'naya matematika* [Mathematical models in information warfare: existential mathematics]. Moscow: ANO TsSOiP; 2014. 259 c. Russian.
4. Novosel'tsev VI, Tarasov BV. *Sistemnaya teoriya konflikta* [The systemic theory of conflict]. Moscow: Osipenko A. I.; 2011. 333 p. Russian.

5. Kastel's M. *Galaktika Internet: razmyshleniya ob internete, biznese i obshchestve* [Galaxy Internet: reflections on the Internet, business and society]. Matveeva A, translator; Kharitonov V, editor. Ekaterinburg: U-factoria; 2004. 327 p. Russian.

6. Wasserman S, Faust K. *Social network analysis: methods of applications*. Cambridge: Cambridge University Press; 1994. 825 p.

7. Pallotti F, Lomi A. Network influence and organisational performance: the effects of tie strength and structural equivalence. *European Management Journal*. 2011;5(29):389–403. DOI: 10.1016/j.emj.2011.02.005.

8. Anisimova NA, Dobaev IP. *Setevye struktury terroristov na Severnom Kavkaze* [Terrorist network structures in the North Caucasus]. Moscow: Redaktsiya zhurnala «Sotsial'no-gumanitarnye znaniya»; 2016. 143 p. Russian.

9. Latyr B. [About actor-network theory. Some clarifications, supplemented by even greater complications]. *Logos*. 2017;1(27):173–197. Russian. DOI: 10.22394/0869-5377-2017-1-173-197.

10. Granovetter M. Threshold models of collective behaviour. *The American Journal of Sociology*. 1978;6(83):1420–1443.

11. Romanov OA. *Vostochnoslavyanskaya tsivilizatsiya v gorizonte otkrytoi istorii* [The East Slavic civilisation in the horizon of open history]. Grodno: Yanka Kupala State University of Grodno; 2018. 334 p. Russian.

12. Vinogradova SM, Mihal'chenko IA. [Information exchange. Information wars]. In: Vus MA, editor. *Informatsionnoe obshchestvo. Informatsionnye voiny. Informatsionnoe upravlenie. Informatsionnaya bezopasnost'* [Information society. Information wars. Information management. Information security]. Saint Petersburg: Saint Petersburg University; 1999. p. 25–68. Russian.

13. Britvin NI. [Social networks as a prototype of the social structure]. *Vlast'*. 2008;1:45–49. Russian.

14. Marin A, Wellman B. Social network analysis: an introduction. In: Scott J, Carrington PJ, editors. *The SAGE Handbook of Social Network Analysis*. London: SAGE Publications Ltd.; 2011. p. 11–25.

15. Kirichenko AV. Informational-psychological war: modern trends and technological capabilities. *Akmeologiya*. 2015; 4(56):209–214. Russian.

16. Green MC. Trust and social interaction on the Internet. In: Joinson A, editor. *Oxford Handbook of Internet Psychology*. New York: Oxford University Press; 2007. p. 43–52.

17. Bochaver AA, Khlomov KD. Cyberbullying: harassment in the space of modern technologies. *Psychology. Journal of the Higher School of Economics.* 2014;3(11):177–191. Russian.

18. Krasovskaya NR, Gylyaev AA. On controlling fakes, deepfakes, fake accounts in the Internet. *Bulletin of Udmurt University. Sociology. Political science. International Relations.* 2021;1(5):96–99. Russian. DOI: 10.35634/2587-9030-2021-5-1-96-99.

19. Zhyravleva LA, Zarybina EV, Rychkin AV, Simachkova NN, Chypina IP. Modern information warfare. *Obrazovanie i pravo.* 2022;9:18–26. Russian. DOI: 10.24412/2076-1503-2022-9-18-26.

Статья поступила в редколлегию 16.03.2024.
Received by editorial board 16.03.2024.