Механизмы регулирования сетевых конфликтов

УДК:101.8:316.3(043.3)

Юлия БАНЬКОВСКАЯ, кандидат философских наук, доцент

Юлия БАНЬКОВСКАЯ. Механизмы регулирования сетевых конфликтов. Неконтролируемость, анонимность, отсутствие единых ценностных ориентиров и строгой системы контроля за трансляцией информации, многоканальность, гипертекстуальность, быстрота создания и исчезновения сетей, их открытость для включения новых элементов, интерактивность сетевой коммуникации обуславливают неконтролируемость конфликтов, представляют угрозу социальной безопасности личности и стабильности общественного развития. Необходима разработка комплекса мер по разрешению противоречий, снижению степени их деструктивного воздействия на функционирование общества.
Ключевые слова: сетевые структуры, социальные сети, взаимодействие, конфликт, регулирование.

Yulia BANKOVSKAYA. Mechanisms to regulate network conflicts. Uncontrollability, anonymity, lack of common value guidelines and strict system of control over information flow, multichannel capacity, hypertextuality, fast emergence and disappearance of networks, their openness to new elements, the interactivity of network communication allow for uncontrollable development of conflicts and pose a threat to the social security of an individual and the stability of social development. The author emphasizes the need to develop a set of measures to resolve contradictions and to reduce their destructive impact on the society.
Keywords: Network structures, social networks, interaction, conflict, regulation.

Конституирование новых форм конфликтного противоборства вследствие развития информационно-коммуникационных технологий, изменение социальных взаимосвязей и механизмов социального взаимодействия – все это говорит о необходимости прояснения специфики функционирования сети. Сетевое общество представляет собой новое устройство социальности. Выявление специфики взаимодействия сетевых структур является значимым условием сохранения стабильности и устойчивости развития и функционирования общества и государства. Увеличение информационных рисков, появление новых форм конфликтных противоборств приводит к необходимости выработки новых инновационных подходов к рассмотрению и пониманию сетевых конфликтов.

В настоящее время наблюдается снижение степени воздействия иерархических структур на социальные процессы. Причина данного явления – сетевизация всех сфер жизнедеятельности общества и невозможность их полной регламентации. С одной стороны, регулирование конфликтов в иерархических системах является менее затратным и достаточно эффективным по причине значимого влияния властного фактора на возникшую проблемную ситуацию.

ОБ АВТОРЕ

БАНЬКОВСКАЯ Юлия Леонидовна.

Родилась в Минске.

Окончила факультет философии и социальных наук Белорусского государственного университета (2001), аспирантуру этого же вуза (2004).

С 2001 по 2007 год – преподаватель, с 2007 года – старший преподаватель, с 2016 года – доцент кафедры философии и истории Белорусского государственного аграрного технического университета. С 2018 года – докторант Института философии НАН Беларуси.

Кандидат философских наук (2013), доцент (2016).

Автор около 100 научных и научно-методических работ, в том числе монографии.

Сфера научных интересов: конфликтология, сетевые структуры, социальная коммуникация, тенденции развития и функционирования социальной системы, процессы ее трансформации.

Данные системы характеризуются большей степенью стабильности и устойчивости, наличием ценностно-нормативных стандартов, регулирующих взаимодействие людей и способы информационно-коммуникативного обмена. С другой стороны, медленные и часто несоответствующие необходимости меры по разрешению конфликта замедляют процесс принятия решений. В иерархических системах затруднена циркуляция информации, что приводит к отсутствию быстрого реагирования со стороны подсистем на проблемную ситуацию.

Конфликтность является следствием конфигурации сетей, к которой принадлежат акторы, и они сами оказывают непосредственное воздействие на стабильность функционирования сетевых структур. Сеть структурирована таким образом, что в ней заложены механизмы, допускающие возможность ее постоянного расширения, вовлечения в процесс большого количества людей. Данные аспекты формируют новые конструктивные возможности для развития системы: включение большого количества элементов, для которых присуще свое видение проблемной ситуации, создает уникальную ситуацию комплексного рассмотрения противоречия, интеграции разнообразных структур и синхронизации их действий. Увеличение объема контента, привлечение внимания к проблеме как представителей небольших социальных общностей, так и мирового сообщества в целом способствует повышению ответственности конфликтующих сторон за осуществляемые ими действия. От качества и объема информации, необходимых для принятия соответствующих решений, зависит эффективность регулирования конфликтов. Вовлеченность в противоборство большого количества людей создает дополнительные возможности для получения более полной информации о существующей проблеме, продуцируя условия, в рамках которых невозможно полностью скрыть или нивелировать данные о противоречии.

Условием безопасности сетевого коммуникативного сообщества является соблюдение норм и правил использования, обмена и распространения информации. Защита прав и свобод личности должна быть гарантирована соответствующими законодательными и нормативно-правовыми документами. Неконтролируемость и динамичность сетевого коммуникативного пространства «определяют формирование социальной безопасности личности в ее условиях как целенаправленную совместную деятельность государственных и общественных институтов, а также людей (пользователей), участвующих в выявлении, предупреждении и минимизации различных сетевых рисков и угроз социальной безопасности личности» *[1, с. 27]*. Важным условием обеспечения социальной безопасности является понимание того факта, что создание абсолютно надежной защиты невозможно.

Профессор права в Гарвардском университете Л. Лессиг полагает, что существуют следующие способы сетевого регулирования противоречий. Во-первых, это утверждение законов и нормативных актов, устанавливающих механизмы сетевого взаимодействия. Во-вторых, нормы, выработанные акторами в рамках определенного сетевого образования и предусматривающие наличие соответствующих санкций за их несоблюдение или нарушение. В-третьих, код, предусматривающий использование артефактов для процесса регуляции. В-четвертых, рынок, регулирующий взаимодействие людей посредством назначения цен, корректирующих использование ресурсов, доступ к информации и другие факторы *[2, с. 27–54]*.

Нормативно-правовое регулирование сетевого взаимодействия в нашей стране регламентируется Законом Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации», Указом Президента Республики Беларусь от 25 октября 2011 года № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информации», Указом от 8 ноября 2011 года № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь», Указом Президента Республики Беларусь от 16 декабря 2019 года № 460 «Об общегосударственной информационной системе». Основополагающая роль отводится Кодексу Республики Беларусь об административных правонарушениях, предусматривающему ответственность за несанкционированный доступ к компьютерной информации, за нарушение правил ее использования, хранения и уничтожения и Уголовному кодексу Республики Беларусь, предполагающему установление уголовной ответственности за преступления, связанные с деструктивным использованием компьютерных данных и технологий. Следовательно, нормативно-правовые аспекты регулирования противоречий в условиях развития информационно-коммуникационных технологий представляют собой совместную деятельность акторов, государства и социальных институтов, направленную на минимизацию киберпреступлений.

Концепция национальной безопасности была принята Указом Президента от 9 ноября 2010 года № 575 и дополнена Концепцией информационной безопасности Республики Беларусь от 18.03.2019 года № 1. В ней подчеркивается необходимость защиты интересов граждан в информационной сфере, осуществляется правовое закрепление основ

государственного управления по защите национальных интересов. Информационная безопасность рассматривается как «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» *[3, с. 5]*. По мнению белорусского ученого академика Е.М. Бабосова, «важность и сложность обеспечения информационной безопасности обусловлена тем, что медиасфера современного общества представляет собой многокомпонентную, нелинейно и противоречиво развивающуюся целостность коммуникационных сетей и связей между множеством людей, их общностей и организаций, функционирующую в процессе их деятельности по производству, присвоению и использованию информационных ресурсов посредством применения компьютерных технологий» *[4, с. 170]*.

Безопасность может иметь внутреннюю и внешнюю формы. Внутренняя безопасность обеспечивает целостность системы, способность поддерживать устойчивость ее функционирования при возникновении противоречий. Внешняя безопасность проявляется в наличии возможностей у системы при взаимодействии с внешней средой сохранять устойчивость, а при дестабилизации вырабатывать меры по урегулированию противоречий. Показателем безопасности сети являются такие ее свойства, как устойчивость, управляемость. Нарушение данных параметров приводит не только к дестабилизации сети и ухудшению качества ее управления, но и к ее разрушению.

Нормативно-правовые, информационно-технологические и саморегулятивные механизмы способствуют формированию социальной безопасности личности.

Нормативно-правовые регуляторы направлены на минимизацию сетевых рисков и угроз, недопущение эскалации конфликтов, снижение уровня киберпреступности. В рамках нормативно-правовой стороны внимание акцентируется на обеспечении личностной безопасности благодаря эффективной деятельности социальных институтов, использующих административные и правовые ресурсы с целью регуляции конфликтных противоборств. Социальная безопасность гарантируется принятыми мерами по защите интересов, направленными на обеспечение стабильности. Российский ученый доктор философских наук Т.В. Владимирова отмечает, что «система социального контроля в своих функциях коррелирует с работой системы обеспечения социальной безопасности, которую, прежде всего, реализует государство. Обеспечение социальной безопасности призвано сбалансировать конфронтационные и другие интересы различных социальных групп ради удовлетворения общих жизненно важных интересов каждой личности, группы и общества в целом» *[5, с. 41]*. Нормативно-правовые принципы в сети должны соответствовать условиям обеспечения прав и свободы пользователей, равного доступа к информации, правомерного ее использования, включая запрет на противозаконное ее распространение. Необходимо обеспечить защиту персональных данных, минимизировать потребительские риски и повысить качество услуг, предоставляемых в сети.

В рамках информационно-технологических механизмов внимание акцентируется на наличие

риска вследствие неопределенности и анонимности информационного обмена, на невозможность осуществления контроля над всеми событиями, происходящими в системе, что приводит к повышению рискогенности дальнейшей социальной эволюции. Возможность предотвращения преступлений посредством выработанных правовых норм, минимизации социальных рисков и угроз способствует формированию социальной безопасности личности. Современные исследователи выделяют несколько таких групп сетевых рисков:

– контентные риски, обусловленные искажением и недостоверностью предоставляемой информации, использованием личных данных в неправомерных целях, низким уровнем защиты персональных данных, разными формами кибермошенничества;

– коммуникационные риски, связанные с деструктивным влиянием социокоммуникативного межличностного взаимодействия субъектов на их эмоционально-мотивационную и когнитивную сферы благодаря наличию возможности манипулирования сознанием, мышлением и поведением человека, негативным воздействием на его систему ценностей и норм;

– потребительские риски, вызванные осуществляемыми финансовыми операциями.

Механизм саморегуляции сетевого взаимодействия предполагает формирование и эволюцию ценностей и норм на основании суммарного коммуникативного опыта, приобретенного благодаря дискуссии акторов по урегулированию и разрешению конфликтных ситуаций. Сетевые нормы разрабатываются, прежде всего, теми акторами, которые легитимно владеют информационным, ресурсным или ценностным капиталом. Они же и осуществляют контроль за их соблюдением. Остальные же субъекты вынуждены их придерживаться в рамках данного образования. С одной стороны, подобная форма социального контроля является достаточно результативной, ибо она учитывает специфику сети. С другой стороны, отсутствие возможности оказывать влияние на формирование механизмов взаимодействия содействует обострению противоречий.

На наш взгляд, нивелирование сетевых конфликтов возможно при условии реализации следующих мер:

– выработка единых ценностно-нормативных стандартов взаимодействия акторов, универсальных для любого сетевого образования. Их наличие позволит не только скорректировать модель поведения субъектов, но и сформировать ответственность за предоставляемую в сети информацию, ее контент;

– создание условий для осуществления общественного контроля над деятельностью сети и при необходимости – ее коррекции;

– расширение сферы правового регулирования сетевого образования со стороны государства;

– повышение уровня медиаграмотности пользователей сети, направленной на сохранение конфиденциальности информации и на формирование навыка распознавания недостоверных сведений и сфабрикованных фактов;

– формирование ценностно-смысловых ориентаций личности и высоких духовно-нравственных идеалов, подлинной культуры в сети будет содействовать снижению напряженности при возникновении противоречий;

– регулирование доступа людей к информации, пропагандирующей разжигание этнической, религиозной, политической и социокультурной вражды, призывающей к террористическим или военным действиям;

– разработка эффективных мер по противодействию дезинформации граждан и распространению противоправных сведений; предоставление полной и достоверной информации о ситуации с целью недопущения распространения слухов, способствующих возникновению у людей социальной неуверенности, страха, тревоги, паники;

– разработка и совершенствование новых компьютерных механизмов защиты информации от несанкционированного доступа для обнаружения и предотвращения кибератак;

– расширение возможностей транснационального сотрудничества, международной взаимопомощи при возникновении киберугрозы, разработка комплекса мер для оказания взаимопомощи в борьбе с компьютерными преступлениями и кибертерроризмом. Эффективным механизмом борьбы с деструктивными способами воздействия сети «хавала» на социальные процессы является внедрение и развитие альтернативных легализованных сетей, осуществляющих финансовую или ресурсную поддержку сторон конфликта, в рамках которой было бы минимизировано время на оформление соответствующей документации;

– постоянный анализ сетевого контента для раннего выявления потенциальной угрозы, оценки возможных последствий, предотвращения реальных преступлений с целью разработки эффективных мер противодействия сложившейся проблемной ситуации.

Инновационным методом управления процессами, протекающими в сети, является краудсординг. Член Совета директоров Microsoft в России А. Беленький трактовал краудсординг как «использование коллективного разума в решении

разного рода задач» *[6, с. 1]*. Метод направлен на привлечение множества людей к обсуждению некоторой проблемы посредством анализа и отбора необходимой информации, имеющихся знаний.

На основании сказанного можно сделать следующие выводы.

Уничтожение сетевых структур практически невозможно вследствие их гибкости. Высокий уровень приспособляемости повышает регулятивные возможности сети, направленные на сохранение своего функционирования в прежнем виде и качестве. Специфика взаимодействия сетевых структур проявляется в их быстрой адаптации к измененным условиям, в универсальности, предоставляющей множественные возможности для формирования новых форм взаимосвязи. Умение критически оценивать имеющуюся информацию, эффективно ее использовать, объективно рассчитать возможные риски и последствия является главным условием сохранения стабильности сетевого образования.

Можно выделить следующие группы мер, которые необходимо предпринять для стабилизации социальной системы.

Во-первых, это политические меры, заключающиеся в стабилизации общественно-политической обстановки и повышении уровня доверия народа к органам управления. При наличии диалога между органами власти и населением создаются возможности для конструктивного обмена рекомендациями и предложениями по привлечению граждан к решению возникающих проблем. Действенным способом разрешения конфликтов является информирование общества о сущности возникших противоречий. Данное знание позволит человеку объективно оценить сложившуюся ситуацию и выработать собственное мнение о проблеме. Тем самым снижается уровень возможной манипуляции действиями отдельных людей и нивелируются предпосылки для возникновения этнополитического конфликта.

Во-вторых, мероприятия социально-экономического характера, направленные на стабилизацию и улучшение экономического благосостояния, повышение уровня и качества жизни. Их наличие содействует снижению остроты ресурсных противоречий.

В-третьих, правовые меры, заключающиеся в ужесточении уровня ответственности за совершение киберпреступлений, за нарушение социальных норм и правил взаимодействия в рамках сетевого пространства, за провоцирование конфликтов. Выявление противоречий, предотвращение их развертывания является значимым конструктивным способом стабилизации системы.

Статья поступила в редакцию 05.04.2021 г.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мкртчян, Л.М. Механизмы обеспечения социальной безопасности личности в сетевом коммуникативном пространстве / Л.М. Мкртчян. // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 7. – С. 27–29.
2. Lessig, L Code and other laws of cyberspace / L. Lessig. – New York: Basic Books, 1999. – 288 p.
3. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // Национальный правовой интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=P219s0001&p1=1. – Дата доступа: 14.02.2021.
4. Бабосов, Е.М. Роль креативности личности в развитии сетевого общества / Е.М. Бабосов. – Минск: Беларуская навука, 2019. – 300 с.
5. Владимирова, Т.В. Социальная природа информационной безопасности / Т.В. Владимирова. – М.: АНО Изд. дом «Научное обозрение», 2014. – 239 с.
6. Беленький, А. Многоликий краудсорсинг [Электронный ресурс] / А. Беленький // Компьютер пресс. – 2011. – № 10. – Режим доступа: https://compress.ru/article.aspx?id=22501. – Дата доступа: 19.01.2021.