

Думов А.В., Кудашов В.И.

Новации сложностного подхода к организации информационной безопасности в сетевом пространстве

Аннотация: Стремительное развитие информационных технологий влечет за собой усложнение коммуникативных сетей и значительное возрастание скорости взаимодействия социальных акторов. Это определяет необходимость переосмысления теоретических оснований информационной безопасности личности, общества и государства. Большое значение для совершенствования современных технологий осуществления информационной безопасности в сетевом пространстве приобретает концепция сложного мышления, позволяющая разрабатывать сложностные подходы к исследованию сетевой реальности и коммуникативных процессов. Рассмотрены существующие новации и перспективы развития сложностных подходов к разработке концепций информационной безопасности в сетевом пространстве.

Ключевые слова: сложность, информация, безопасность, сетевой, коммуникация

В условиях возрастающего усложнения сетевого пространства коммуникативного взаимодействия развитие и совершенствование технологий обеспечения безопасности социальных практик предполагает исследование «экологии» сложных виртуальных систем в качестве необходимого условия эффективности. Поскольку сетевые процессы информационного взаимодействия носят глобальный характер, представители структур обеспечения безопасности более не могут занимать позицию «стороннего наблюдателя» в исследовании сетевых процессов: статус актора виртуального пространства предполагает вовлеченность в поле взаимодействий. По замечанию К. Майнцера, способность управлять сложностью современных обществ решающим образом зависит от эффективных коммуникационных сетей [1]. Между сетевыми структурами и взаимодействующими в них акторами наблюдается онтологическая взаимосвязь: существование и эффективное функционирование коммуникативных сетей детерминируется деятельностью акторов коммуникации, тогда как

особенности внутрисетевых процессов определяют образ действия акторов.

Востребованность концепта сложного мышления в сфере разработки технологий обеспечения информационной безопасности обусловлена двумя его важными особенностями. Сложное мышление предполагает переход от мышления в терминах устойчивых структур к парадигме отношений и свойств, что является крайне необходимым для успешной деятельности в мире усложняющихся коммуникативных связей. Отмеченная Т.В. Владимировой необходимость практического переход от действия в мире вещей к схватыванию «вещей-процессов» [2] может быть осуществлена только при условии изменения когнитивной стилистики действия через взаимодействие со сложностью сред информационной реальности. Вторая значительная особенность концепта сложного мышления заключается в том, что оно предполагает творческий, конструктивный характер осмысления действительности. Плюралистический характер сложного мышления, его имманентная релятивность предполагает «парадигмальную свободу» исследователя [3]. Следствием этого становится потенциальная возможность разработки множества стратегий практического взаимодействия со сложностью, адаптированных к различным моделям поведения системы.

Положительным свойством сложного мышления для использования в сфере разработки стратегий взаимодействия со сложностью виртуальной реальности является его методологический плюрализм. Авторитарные модели управления и воздействия, подходящие для иерархических структур, могут оказаться совершенно неэффективными применительно к коммуникативным средам с сетевой организацией. Вопрос о соотношении коммуникативной и административной составляющей во взаимодействии со сложными системами справедливо решается видным философом — исследователем проблематики познания сложности Э. Мореном в пользу коммуникативной составляющей [4], поскольку в отношении подобных систем жесткая регуляция является неэффективной. Аналогичным образом исчерпывает себя и практика планирования, направленного на создание ограниченного числа стратегий взаимодействия: хаос не допускает никакой устойчивой стратегии решения задач [1]. Тенденции

упорядочивания виртуального пространства выражаются в контекстуализации норм, определяющих форму и содержание практик социального действия в сети.

Сложностный подход предполагает диалогический характер взаимодействия иерархических административных структур с сетевыми образованиями информационной реальности. Например, А.В. Олескин в наиболее общем виде предполагает либо совместное формирование структуры-медиатора, позволяющего осуществлять компромиссные сценарии сосуществования, либо взаимопроникновение сетевых и иерархических структур, приводящее к формированию властного узла в сети, определяющего направление развития всего сетевого пространства в целом [5]. Применительно к рассмотрению процессов взаимодействия государственных структур, целью которых является обеспечение информационной безопасности посредством нормативного регулирования сферы интернет-коммуникаций, и сетевых структур виртуального пространства, нельзя сказать об эффективности второго варианта: развитие виртуальных структур осуществляется гораздо быстрее, чем их нормативная оценка. Как следствие, возможность прямого регулятивного воздействия на акторов и структуры киберпространства оказывается ограниченной. Достижение консенсуса по вопросу об обеспечении информационной безопасности в сети подразумевает содействие государственных структур и сетевых образований как виртуальных проявлений деятельности гражданского общества.

Деятельность по обеспечению информационной безопасности, согласно Т.В. Владимировой, осуществляется по двум направлениям: защита информации и защита от информации [2]. Перспективный характер использования концепции сложного мышления заключается в возможности органичной реализации данных двух аспектов без нарушения баланса между ними. Плюралистичность сложностного подхода может позволить осуществлять многоаспектную оценку уязвимостей информационных ресурсов, подлежащих защите. Для этого необходима организация диалога исследовательских интерпретаций, что подразумевает оценку опыта ряда акторов сетевого взаимодействия. Сфера обеспечения информационной безопасности как реализации интересов личности, общества и

государства в виртуальном пространстве должна стать полем диалога позиций различных акторов социального действия в сети: коммерческих и государственных структур, гражданских объединений и официальных организаций. Не существует единого облика виртуальной реальности: множество акторов порождает множество различных, но коррелирующих между собой сетевых пространств и соответствующих образов действия и коммуникации [6].

Сложностный подход к обеспечению защиты от информации, имеющей деструктивный характер для развития общества, личности и государства также подразумевает консенсусный, диалогический характер. Легитимация противодействия созданию и распространению подобной информации должна быть осуществлена на трех уровнях — личном, общественном и государственном и представлять собой согласие между взаимосвязанными потребностями в защите личных интересов, сохранении и поддержании комфортных условий среды социальных взаимодействий, стабильном и эффективном функционировании административного аппарата. Обеспечение информационной безопасности как проявление адаптивности социальных акторов в пространстве виртуальных сетей должно быть адекватно возрастающей информационной и коммуникативной сложности. Поэтому концепция сложного мышления может стать основанием для формирования современных путей решения проблем обеспечения информационной безопасности в сетевом пространстве.

Литература:

1. *Майнцер К.* Сложносистемное мышление: материя, разум, человечество. Новый синтез. Пер.с англ. / Под ред.и с предисл. Г.Г. Малинецкого. — М.: Книжный дом «ЛИБРОКОМ», 2009. — 464 с.
2. *Владимирова Т.В.* Социальная природа информационной безопасности: монография. — М.: Издательский дом «Научное обозрение», 2014. — 239 с.
3. *Арзуманян Р.* Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века. — М.: Издательский Дом «Регнум», 2012. — 600 с.

4. *Морен Э.* Метод: природа природы / Пер. с фр. Е. Н. Князевой.— М.: Прогресс-Традиция, 2005. – 464 с.
 5. *Олескин А. В.* Сетевые структуры в биосистемах и человеческом обществе. — М.: Книжный дом «ЛИБРОКОМ», 2017.— 304 с.
 6. *Dekker S., Cilliers P., Hofmeyr J.-H.* The complexity of failure: implications of complexity theory for safety investigations // *Safety Science*, vol.49, 2011. – P. 939-945.
-