Радевич Екатерина Владимировна, аспирантка кафедры философии и методологии науки, Белорусский государственный университет, г. Минск, Беларусь.	*Феномен информационной безопасности в ракурсе социально-философского анализа*.

ФЕНОМЕН ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАКУРСЕ СОЦИАЛЬНО-ФИЛОСОФСКОГО АНАЛИЗА.

Радевич Е. В.
Белорусский государственный университет

Современный мир не мыслим без новейших информационных технологий, которые во многом определяют характер и темп нашей жизни, формы занятости, способы осуществления профессиональной и досуговой деятельности.

Новые технологии обеспечивают необходимый объем социальной памяти, в которой сохраняются произведенные смыслы, а также позволяют наращивать систему коммуникаций, что создает возможность для возникновения новой организации общества. По мере того, как расширяется сеть Интернет и мобильная телефония, многие сферы человеческой деятельности стремительно переносятся в поле дистанционной коммуникации. «Изменяется привычный порядок взаимодействия, как на уровне институтов, так и на уровне индивидуальных интеракций, то есть новые технологии превращаются в основание системы коммуникаций современного общества» [1, с. 132]. Трансформируются «основные категории, в рамках которых люди привыкли мыслить и действовать – пространство и время, труд и досуг, право и национальное государство» [2, с. 25].

Новые глобальные информационные технологии не просто открывают невиданные ранее возможности для развития человека, но одновременно ставят перед человеком и культурой сложнейшие проблемы общефилософского характера.

Одной из таких проблем является проблема информационной безопасности, которая очень остро встала перед человечеством в процессе глобальной информатизации. «В современных условиях глобальной информатизации и повсеместного распространения информационных технологий заметно возрастает значение обеспечения информационной

безопасности. Остро заявляет о себе проблема эффективного использования информационных ресурсов. При этом необходимо подчеркнуть, что в условиях глобализации информационного пространства и обостряющего информационного противоборства проблема обеспечения информационной безопасности наряду с технико-технологической ее составляющей все более приобретает социально-политический характер» [3, с. 72-73]. Информация уже носит ярко выраженный антропологический характер – например, информация о личной жизни. В связи с этим неминуемо встает вопрос о том, что эту информацию необходимо защищать, и современные информационные здесь имеют решающее значение. Наличие современного программного обеспечения, способного «взломать» систему защиты практически любого компьютера, грозит не только тем, что персональная информация может стать достоянием общественности, будучи размещенной в глобальной сети, но и стратегически важная государственная, военная и даже научная информация может быть рассекречена. Возможность получать доступ к такого рода данным может иметь серьезные, а иногда и фатальные последствия. В данном случае речь идет о деятельности террористических организаций или финансовых махинациях, сообщения о которых все чаще появляются в СМИ. Отсюда напрашивается вывод о том, что необходимо уделить особое внимание развитию высоких технологий именно в этом направлении. Однако у этой проблемы есть две стороны. На ряду с необходимостью усилить контроль над информацией, которая циркулирует в глобальной сети, на сколько это возможно, встает вопрос о праве на частную жизнь: ведение личной переписки. Где должны заканчиваться границы личной свободы и начинаться сфера легального контроля? Это еще один вопрос общефилософского характера, который встает перед современным человечеством. Следует ли государству ввести ограничения по шифрованию передаваемых данных, что позволит хоть в какой-то мере контролировать потоки информации, либо снять все ограничения, тем самым предоставив больше свободы для развития экономики, товарооборота, но существенно ослабить контроль над обмениваемой информацией? Парадокс этой ситуации состоит в том, что наличие ограничений, казалось бы, будет ущемлять права людей, контролировать их деятельность в киберпространстве, но с другой стороны, это как раз позволит обезопасить их жизнь, т.к. когда будут сняты ограничения на шифрование, государство не сможет контролировать обмен данными, в том числе военного и экономического

характера, что несет в себе потенциальную угрозу для граждан, их личной жизни.

Одним из неотъемлемых составляющих любой войны, в том числе и информационной, является оружие, в данном случае информационное. Следует отметить, что в настоящее время понятие «информационное оружие» относится к разряду дискуссионных. «В широком смысле под информационных оружием понимаются способы целенаправленного информационного воздействия на противника, рефлексивного управления им с целью изменения его замысла на проведение стратегических или тактических действий в нужном направлении. В более узком смысле под информационным оружием понимается комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника и вмешательства в работу его телекоммуникационных систем, систем управления и разведки, аппаратного и программного обеспечения в целях выведения их из строя, нарушения процесса нормального функционирования, получения или модификации содержащихся в них данных, а так же целенаправленного продвижения выгодной информации (или дезинформации)» [3, с. 208]. К такого рода информационному оружию можно отнести и различного рода фальсифицированную информацию, напечатанную в прессе, и так называемый «черный ПР», и активную пропаганду и агитацию против конкурентов.

Анализируя сложный и противоречивый феномен информационной войны, автор не умоляет достоинств современных информационных технологий, к которым можно отнести огромные потоки осваиваемой информации, скорость изменения информационных обликов, возникновение возможности диалога с современными системами искусственного интеллекта, возможность преодолеть пространственно-временные ограничения, переход к глобальному управлению поверх государственных границ, появление возможности глобальной коммуникации. Однако не следует забывать и о том, что концентрация огромного массива информации в одних руках может вести к манипуляции человеческим сознанием, возможностью лоббировать свои интересы одним предпринимателем-монополистом и т.д.

В заключении следует отметить, что находящиеся на современном этапе развития информационные технологии и сложившиеся условия в обществе создают благоприятные условия для существования

информационных войн, для преодоления которых необходима комплексная, системная деятельность общества в целом.

Литература.

1. Иванов, Д. В. Императив виртуализации: Современные теории общественных изменений / Д. В. Иванов. – СПб., 2002.

2. Бек, У. Общество риска. На пути к другому модерну / У. Бек. – М., 2000.

3. Манойло, А. В Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – М., 2003.