УДК 316.3/.4

СОЦИОЛОГИЧЕСКОЕ ЗНАНИЕ И БЕЗОПАСНОСТЬ В СЕТЕВОМ ПРОСТРАНСТВЕ

Т. В. Владимирова (Новосибирск)

В статье ставится проблема понимания информационной безопасности в связи с развитием сетевых коммуникаций. Излагается видение основных групп угроз, которые исходят от сетевого коммуникативного пространства. С точки зрения автора, наличие компетенции, связанной с ориентацией в сети, является одной из важнейших сторон обеспечения информационной безопасности. Такого рода компетенция обеспечивает социологическое образование.

Ключевые слова: *сетевые коммуникации, информационная безопасность, угрозы безопасности, профессиональная компетенция.*

SOCIOLOGICAL KNOWLEDGE AND THE SAFETY IN THE NETWORK SPACE

T. V. Vladimirova (Novosibirsk)

The article poses the problem of understanding of information safety in connection with the development of network communications. There are described the main groups of dangers originating from the network communicative space. From the point of view of the author, the presence of the competence connected with the orientation in the network is one of the main parts of ensuring the informational security. Theses competencies are provided by sociological education.

Key words: *network communications, information safety, safety threats, professional competence.*

В современном обществе все большее количество социальных коммуникаций принимает сетевой характер. Благодаря сетевым коммуникациям любая информация максимально быстро распространяется в обществе. Интенсивность и частота взаимодействий между двумя и более коммуницирующими субъектами выше, когда они выступают в качестве узлов одной деловой сети, нежели тогда, когда они принадлежат разным сетям, а тем более не принадлежат к какой-либо сети. Включение в сетевые структуры или исключение из них, а также контуры сетевых потоков, которые задают информационные технологии, стремительно становятся доминирующими тенденциями, формирующими современный мир.

Такая особенность общества становится причиной многих серьезных проблем, связанных с безопасностью. Разрастание сетевых структур со-

Владимирова Татьяна Валерьевна – кандидат философских наук, доцент кафедры социологии ГОУ ВПО «Новосибирский государственный технический университет».

630092, г. Новосибирск, пр. К. Маркса, д. 20.

E-mail: t-vlad@ngs.ru

провождается увеличением интенсивности сетевых коммуникаций. Увеличиваются скорость и многообразие коммуникаций, их временный характер. В этих условиях изучение и прогнозирование такого рода социальных взаимодействий действительности становится необходимостью [9, 10].

Цель предлагаемой работы заключается в формулировании утверждения о том, что информационная безопасность как безопасность в условиях современного коммуникативного пространства возможна благодаря формированию общих и профессиональных компетенций, связанных с ориентацией в современном сетевом коммуникативном пространстве. Именно социологическое образование сегодня может сформировать также компетенции. В настоящей статье с позиции социологического анализа рассматриваются особенности сетевого пространства и выделяются основные группы информационных угроз безопасности для современного общества, генерируемых в сетевых коммуникациях.

Под сетью мы понимаем децентрализованный комплекс взаимосвязанных узлов открытого типа, способный неограниченно расширяться благодаря включению все новых звеньев (коммуникаций), что придает сети гибкость и динамичность. Таковы сети Интернета, сети финансовых потоков, сети СМИ. Сетевая структура характеризует управление ТНК, бизнес–структур, финансово–промышленных групп, политических партий. В основании организации глобальной\информациональной экономики лежит сетевое предприятие. Это специфическая форма предприятия, система средств которого составлена путем пересечения сегментов автономных систем целей. Так, компоненты сети одновременно автономны и зависимы. Компоненты одной сети могут быть частью других сетей, а следовательно, других систем средств, ориентированных на другие цели.

В большинстве работ, посвященных влиянию Интернета на общество, в основном характеризуются чисто технические особенности Интернет–среды [2]. Между тем понимание смысла такого глобального явления, как сеть, может быть достигнуто только благодаря включению его в общий контекст мировой цивилизации, раскрытию связей с различными социальными структурами. Для более глубокого понимания социальных процессов, протекающих в сетевом пространстве, необходимо уделять внимание «социологическому измерению» Интернета: культурным, языковым и психологическим особенностям социального взаимодействия, закономерностям формирования и характеристикам функционирования общностей, принципам самовыражения личности и изменению сетевой идентичности.

В целом сетевые потоки (глобальные метасети) способны подчинять себе большие группы людей. Сегодня все чаще человек связывает свою профессиональную деятельность, образование, досуг, пользование услугами с сетевыми организационными структурами. Ярким примером тому является активное развитие сетевого маркетинга: страховой бизнес, различные сети по распространению продуктов и услуг и др. С развитием сетевого информационного пространства образуется разрыв между информационной сетью и большинством видов традиционной управленческой деятельности. Территориальные организационные структуры начинают претерпевать серьезные реконструкции. Частично они становятся дисфункциональными. И. А. Василенко отмечает, что отдельные виды политичес-

кой деятельности не исчезают, меняется их прежнее структурное значение в поле социального, политического управления, оно переходит в новую логику информационного сетевого пространства [3, с. 15].

Информационные угрозы обычно рассматриваются в контексте проблемы обеспечения информационной безопасности. В российских нормативно-правовых актах информационная безопасность определяется как состояние защищенности информационной среды. Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, а также несанкционированных и непреднамеренных воздействий на защищаемую информацию. Соответственно, информационная безопасность государства определяется как состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере [8]. На наш взгляд, в нормативно-правовых актах преобладает понимание информационной безопасности в ее технологическом и правовом аспектах. Информационная безопасность раскрывается как защита конфиденциальности (обеспечение доступа к информации только авторизированным пользователям), целостности (обеспечение достоверности и полноты информации и методов ее обработки) и доступности (обеспечение доступа к информации и связанным с ней активам авторизированных пользователей по мере необходимости) информации. Защита целостности и доступности предполагает наличие соответствующих информационных и аналитических ресурсов пользователя. Но в большей степени в документах находит отражение аспект, связанный с защитой аппаратного, программного обеспечения и обеспечения связи (коммуникации).

Важно отметить, что защищенность собственных информационных ресурсов не гарантирует информационной безопасности для субъекта, поскольку даже достигнутое преимущество в обладании той или иной информацией может быть оценено только в соотношении с информационными ресурсами другого субъекта. В силу этого другая сторона информационной безопасности заключается в предельно возможной степени ориентации во всей информационной сфере. Другими словами, недостаточность информированности может привести к принятию неадекватных управленческих решений и в этом смысле правильно трактовать состояние субъекта, принимающего такое решение, как находящегося в информационной опасности. Информационная угроза возникает тогда, когда субъект по каким-либо причинам не может воспользоваться циркулирующей в информационном пространстве информацией, необходимой для принятия соответствующих управленческих решений. Само же отражение возникающих угроз, при их осознании субъектом, связано лишь с наличием или отсутствием у него средств их отражения [1].

В рамках социологического знания можно выделить основные группы угроз безопасности современного общества, связанных с особенностями сетевых коммуникаций. В частности, наиболее опасным источником угроз интересам личности называется существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг него индивидуального «виртуального информационного пространства», а также возможности использования различных технологий воздействия

на его психическую деятельность. Другим опасным источником угроз интересам человека является использование во вред его интересам персональных данных, накапливаемых как органами государственной власти, так и частными аналитическими структурами, а также расширение возможности скрытого сбора информации, составляющей его личную и семейную тайну.

Сетевые коммуникации сегодня являются условием качественно новой возможности концентрации средств массовой информации в руках небольшой группы собственников, и прежде всего зарубежной. Этот процесс предполагает слияние и приобретение различных медийных средств (СМИ), в результате чего большинство их сосредотачивается в руках относительно небольшого числа владельцев. Современное сетевое информационное пространство характеризуется медиаглобализацией. В этот процесс включено относительно небольшое число экономических субъектов: речь идет о таких транснациональных корпорациях, как, например, Тайм Уорнер, Сони, Уолт Дисней Компании, Мацушита и др., которые создают новые – глобальные или региональные – медиаканалы: Би-Скай-Би, Си-Эн-Эн, MTV. Новые электронные медиа обладают почти безграничными возможностями передачи любой информации любым ее отправителем в различных направлениях, но медийные информационные потоки формируются в интересах владельцев транснациональных информационных агентств. Подобные обстоятельства приводят к угрозам манипулирования общественным мнением по отношению к тем или другим значимым событиям и, что еще более серьезно, к деформации моральных устоев общества, его национальной культуры путем навязывания ему чужих ценностей. Разумеется, сетевые коммуникации сами по себе являются просто эффективной технологией для успешного развития бизнеса владельцев транснациональных информационных агентств. Западный бизнес не ставит своей целью разрушение нормативно-ценностной системы нашего общества. Но он стремится распространить свои «правила игры», свою логику экономического, социального действия с тем, чтобы реализовывать свои коммерческие проекты в адаптивной для себя среде. Попутно им выполняются заказы, продиктованные ведущими геополитическими игроками. Ярким тому примером является мощная подача заведомо ложной информации о нападении России на Грузию в августе 2008 г.

Важнейшей группой угроз безопасности общества, личности и государства, исходящих от сетевых коммуникаций, является расширение масштабов отечественной и международной преступности за счет роста компьютерных преступлений. Угрозы могут проявляться в виде попыток осуществления мошеннических операций с использованием глобальных или отечественных информационных телекоммуникационных систем, отмывания финансовых средств, полученных противоправным путем, получения неправомерного доступа к финансовой, банковской и другой информации, которая может быть использована в корыстных целях. По данным аналитиков, число опасных Интернет-ресурсов в текущем году увеличилось в 3 раза. Эксперты по Интернет–безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Пятикратно увеличился объем спама. Во многих стра-

нах отмечается увеличение объемов утечки данных, при этом только около 20 % происходит из-за атак хакеров. По данным МВД, в 2008 г. в России произошло 14 тыс. киберпреступлений. Это на 2 тыс. больше, чем в 2007 г. [4].

Сетевые структуры и коммуникации эффективно используются организациями в условиях конспирации. Их главным козырем становятся молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя политические нормы и традиции, нарушая законы, расшатывая политическую систему.

Наиболее опасными источниками угроз интересам государства и общества в информационной сфере являются неконтролируемое распространение информационно-психологического оружия и развертывание гонки вооружений в этой области, ведение информационных войн. Такие войны идут на разных уровнях – в корпорациях, регионах, государствах, мировом сообществе. Информационно-психологическое оружие используется в глобальных сетях гражданского назначения и свободного доступа с целью ведения информационной войны. Оно представляет собой совокупность средств, методов и технологий, обеспечивающих возможность воздействия на информационную сферу противника с целью разрушения его информационной инфраструктуры, системы управления государством, снижения обороноспособности и безопасности. «Информационное оружие» особенно опасно в условиях почти монопольного положения компаний небольшого количества стран мира на рынке информационных технических продуктов, так как способно спровоцировать желание использовать имеющееся превосходство для достижения тех или иных политических целей.

Существует мнение, что повышение уровня оперативности обмена информацией, «прозрачности» и доступности последней для всех субъектов политического процесса, уникальная возможность генерировать информационные потоки в обход государственных структур – все эти и другие очевидные свойства сетевого пространства Интернета могут являться важнейшими предпосылками становления посттоталитарного устройства общества. Информационно-технологическая революция несет с собой не только новые возможности, но и целый ряд угроз, чреватых дестабилизацией существующих демократических режимов. И. Л. Морозов выделяет два блока угроз, ведущих к подрыву политических режимов – системные и периферийные угрозы [6]. Угрозы первого типа носят целенаправленный, структурированный и централизованный характер и являются следствием упорядоченных действий в сетевом пространстве властных и околовластных структур. Так, возможны скоординированные информационно-психологические атаки на конкретную политическую систему или ее сегмент со стороны конкурирующего государства (цивилизации, транснациональной структуры) или деструктивных акций внутригосударственных квазиэлит, проводимых соответствующими методами.

Не менее серьезную опасность представляют угрозы второго типа, которые связаны с деятельностью широкого спектра внесистемных сил – от

международных террористических организаций до всевозможных хакерских групп. Неструктурируемость, диффузность и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной стратегии защиты от них.

На наш взгляд, можно выделить следующие основные группы угроз безопасности личности, общества и государства, обусловленных сетевыми коммуникациями:

– угрозы безопасности, связанные с расширением возможностей манипулирования сознанием человека;

– угрозы использования во вред человеку его персональных данных (расширение возможностей скрытого сбора персональной информации);

– угрозы, связанные с развитием сетевого принципа управления средствами массовой информации, что влечет за собой рост возможностей манипулирования общественным мнением;

– угрозы, связанные с эффективностью сетевых структур и сетевых коммуникаций в плане расширения масштабов отечественной и международной преступности и терроризма;

– угрозы неконтролируемого распространения информационно-психологического оружия и его применения в информационных войнах;

– угрозы стабильности существующих политических режимов власти – системные и периферийные, также обусловленные сетевой логикой многих социальных процессов в обществе.

Анализ подобной классификации групп угроз может отвечать различным профессиональным задачам специалистов, занимающихся проблемами безопасности. В Доктрине информационной безопасности РФ от 2000 г. выделяются три основные группы методов обеспечения информационной безопасности: правовые, организационно-технологические и экономические. На наш взгляд, необходимо говорить и о формировании общих и профессиональных компетенций в области работы в сетевом коммуникативном пространстве как о важнейшей группе методов обеспечения информационной безопасности. В данном случае под компетенциями мы понимаем знания сетевого пространства, навыки и умения работы в сети. Отечественное социологическое образование должно ответить на вызовы развивающегося сетевого виртуального пространства системным созданием условий, обеспечивающих формирование подобных компетенций, дающих возможность для безопасной самореализации и развития личности, общества и государства в контексте всего многообразия сетевых коммуникаций.

СПИСОК ЛИТЕРАТУРЫ

1. **Арсентьев М. В.** К вопросу о понятии «Информационная безопасность» // Информационное общество. – 1997. – № 4–6. – С. 48–50.
2. **Белинская Е. П.** Человек в информационном мире. – URL: http//psynet.carfax.ru/texts/bel3.htm.
3. **Василенко И. А.** Политическая философия : учеб. пособие. – М. : Гардарики, 2004. – 240 с.

4. **Интервью** с первым заместителем председателя комитета по Безопасности Государственной Думы РФ М. И. Гришанковым // ФСБ «за» и «против». – 2009. – № 2. – С. 21.
5. **Кастельс М.** Информационная эпоха: экономика, общество и культура / пер. с англ. М. Кастельс ; под ред. О. И. Шкаратана. – М. : Гос. ун-т Высш. шк. экономики. – 2000. – 607 с.
6. **Морозов И. Л.** Информационная безопасность политической системы // Полис. – 2002. – № 5. – С. 134–144.
7. **Ревич Ю.** Реалии виртуальности. Нужен ли России специальный закон об Интернете? // ФСБ «за» и «против». – 2009. – № 2.– С. 27–30.
8. **Доктрина** информационной безопасности РФ // Рос. газ. – URL: http://www.rg.ru/oficial/doc/min_and_vedom/min_bezop/doctr.shtm
9. **Иванкина Л. И.** Критерии безопасного образовательного пространства // Философия образования. – 2006. – № 1(15). – С. 118–123.
10. **Камашев С. В.** Некоторые аспекты взаимосвязи национальной безопасности и российского образования // Философия образования. – 2006. – № 2(16). – С. 165–169.