СЕТЕВЫЕ КОММУНИКАЦИИ КАК ИСТОЧНИК ИНФОРМАЦИОННЫХ УГРОЗ

Т. В. ВЛАДИМИРОВА

ВЛАДИМИРОВА Татьяна Валерьевна - кандидат философских наук, доцент кафедры социологии Новосибирского государственного технического университета (E-mail: t-vlad@ngs.ru).

Аннотация. Переосмыслено значение понятия "информационная безопасность", обозначающего защиту от угроз для общества и его граждан, обусловленных развитием сетевых коммуникаций. Наличие компетенций, связанных с ориентацией в сети - важнейший способ обеспечения информационной безопасности.

Ключевые слова: сетевые коммуникации * проблема "социального измерения" сети * информационные угрозы безопасности * компетенции в ориентации в информационном пространстве

Сегодня сетевые коммуникации составляют новую социальную морфологию (структуру) обществ. М. Кастельс назвал современное общество "обществом сетевых структур". Благодаря сетевым коммуникациям оказывается возможным быстро распространять любую информацию, однако ее получение зависит от заинтересованности в ней. Расстояние становится короче, а интенсивность и частота взаимодействий между двумя и более коммуницирующими субъектами выше, если они выступают в качестве узлов одной деловой сети, нежели когда они принадлежат к разным сетям, а, тем более, не принадлежат ни к одной из них. Включение в сетевые структуры или исключение из них, контуры сетевых потоков, которые задают информационные технологии, становятся доминирующими тенденциями, формирующими современный мир.

В современном обществе все большее количество коммуникаций принимает сетевой характер. Разрастание таких структур сопровождается увеличением интенсивности коммуникаций и становится причиной многих серьезных проблем, связанных с безопасностью личности, общества и государства. По сути, речь идет о росте дифференциации социальных процессов, и, соответственно, их усложнении и ускорении. Подобная ситуация требует изучения сетевого коммуникативного пространства.

Социальная действительность усложняется и становится изменчивой "текучей современностью" (З. Бауман). В этих условиях изучение и прогнозирование такого рода социальной действительности становятся необходимостью. В настоящей статье предпринята попытка рассмотреть особенности киберпространства[1] и выделить

[1] Киберпространство - пространство, создаваемое сетевыми коммуникациями Интернета. Термин "cyberspace", введенный в 1984 г. У. Гибсоном, после возникновения всемирной телекоммуникационной Сети стал обозначать создаваемое ею пространство.

основные группы информационных угроз безопасности личности, общества и государства, генерируемых в сетевых коммуникациях.

Большое число работ, посвященных влиянию Интернета на общество, характеризуется направленностью на технические особенности сетевого коммуникативного пространства в ущерб социокультурному контексту [1; 2]. Ю. М. Кузнецова и Н. В. Чудова отмечают, что сеть - это и комплекс распределенных в пространстве технических объектов (что позволяет ставить вопросы о его географии и экономике); и корпус организованных в виде гипертекста текстов (исследуемых с позиции текстологии, архивного дела, журналистики); и объединение активно действующих людей (данному пониманию отвечает социология, психология, политология, педагогика Интернета); и комплексная система (философский и системологический подход); и попытка реализации технических и социальных договоренностей в глобальном смысле (предмет для анализа с правовых и исторических позиций глобалистики) [3, с. 28; 4; 5; 6].

В то же время, развитие сетевого коммуникативного пространства оказывается для общества не только благом. Благодаря сетевым коммуникациям сегодня генерируются самые различные деструкции для личности, общества и государства. Угрозы, исходящие от сетевого коммуникативного пространства, принято именовать информационными. Их обычно рассматривают в контексте проблемы обеспечения информационной безопасности, которая в российских нормативно-правовых актах определяется как состояние защищенности информационной среды и деятельность по предотвращению утечки защищаемой информации, по защите от несанкционированных и непреднамеренных воздействий на нее. Соответственно, информационная безопасность государства определяется как состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере [7]. На наш взгляд, в нормативно-правовых актах преобладает понимание информационной безопасности в ее техническом и правовом аспектах. Как правило, она трактуется 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. Но в юридических документах в наибольшей степени находит отражение аспект, связанный с защитой программного обеспечения и обеспечением безопасности связи (коммуникации) [17].

Однако существующая защищенность информационных ресурсов не гарантирует субъекту его информационной безопасности. Недостаточная информированность в экстремальных ситуациях может привести к принятию неадекватных решений. Мы разделяем подход, который выделяет защиту собственных информационных ресурсов лишь как часть информационной безопасности. На наш взгляд, *определяющим в информационной безопасности личности, общества и государства является ориентация в информации, циркулирующей в сети, а также наличие возможностей и средств отражения возникающих угроз, что предполагает доступ к информации и наличие собственных информационных и аналитических ресурсов.* Отражение возникающих угроз при их осознании субъектом связано с наличием или отсутствием у него средств их отражения.

Предпримем попытку выделить основные группы угроз безопасности для личности, общества и государства, связанных с особенностями сетевых коммуникаций.

Наиболее опасными источниками угроз интересам и здоровью личности считают существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг индивида индивидуального "виртуального информационного пространства", а также возможности использования различных технологий воздействия на его психическую деятельность. Негативным последствием чрезмерного использования сети является информационная перегрузка. В обществе появилась Интернет-зависимость, порождающая психосоциальную депривацию, приводящую "к недостаточному удовлетворению информационно-коммуникативных и других видов

потребностей и, как следствие, к деформации или качественным изменениям личностных, социальных, профессиональных, материальных и семейных ценностей" [8, с. 73]. Н. В. Корытникова отмечает особое проявление депривации в современном обществе - социально-психологическое преследование: "Чтобы больше узнать о другом человеке, повлиять на его действия, получить скрытые и тайные сведения о нем, преследователь подключает богатые на подобного рода информацию Интернет-источники. Он наблюдает за поведением преследующейся личности в сети, вскрывает почтовые электронные ящики для просмотра его переписки, посылает анонимные сообщения на страницы в социальных сетях. Более серьезные формы социально-психологического преследования включают публичную клевету, распространение ложной информации, прямые угрозы через формы Интернет-общение" [8, с. 78]. Источником угроз интересам отдельных людей является сбор и использование во вред им их персональных данных, накапливаемых органами государственной власти, а также расширение возможности для скрытого сбора информации, составляющей его личную и семейную тайну, сведений о его частной жизни.

Сетевые коммуникации и сегодня обеспечивают широкие возможности для концентрации СМИ в руках небольшой группы собственников. В настоящее время отмечается комбинирование традиционных и новых медиа, прежде всего Интернета и телевидения, с целью превращения кабельных каналов в "веб-порталы" и Интернет-магазины, где продаются продукты нового интегрированного рынка. 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. Постепенно формируется новый глобальный медиарынок - информационные супермагистрали. Их называют "новыми электронными медиа", чтобы отделить их от обычных медиа, к которым относятся печать, радио, телевидение [9].

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. Процесс монополизации на медиарынке приводит 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 общества, но стремится распространить свои "правила игры", свою логику экономического, социального действия, с тем, чтобы реализовывать коммерческие проекты в адаптивной для себя среде. Попутно глобальный медиарынок выполняет заказы, продиктованные ведущими геополитическими игроками. Ярким тому примером является мощная подача в информационных международных агентствах 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, неправомерного доступа к финансовой, банковской и другой информации, которая может быть использована в корыстных целях. Как отмечает Ю. Ревич, мировая юриспруденция оказалась абсолютно не готовой к приходу цифровых технологий [10, с. 27]. Это стало очевидно с распространением Интернета. Нет, наверное, никакой другой

области, где бы, как в Интернет-сетях, и пользователи, и хозяева ресурсов, своими действиями если и не вступили в прямое противоречие с законом, то оказались в "серой зоне" правовой неопределённости. Это особенно ярко проявляется в многочисленных коллизиях, связанных с нарушением авторских прав, но областью интеллектуальной собственности противоречия между правом и "виртуальной реальностью" далеко не ограничиваются.

По данным аналитиков, число опасных Интернет-ресурсов за последнее время увеличилось в три раза. Эксперты по Интернет-безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Во многих странах отмечается увеличение объемов утечки данных, при этом только около 20% происходит из-за хакерских атак. По данным МВД, в 2008 г. в России произошло 14 тыс. киберпреступлений. Это на две тысячи больше, чем за 2007 г. [11, с. 21].

Во Всемирной паутине сегодня существуют различного рода закрытые сети. Сетевые структуры эффективно используются организациями в условиях конспирации. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя правовые нормы и традиции, нарушая законы, расшатывая политический строй обществ.

Опасными источниками угроз интересам государства в информационной сфере являются неконтролируемое распространение информационно-психологического оружия и ведение информационных войн. Такого рода войны идут на разных уровнях - в корпорациях, регионах, государствах, мировом сообществе. Механизмы и процедуры их ведения почти одинаковы, используются одни и те же элементы: дефицит информации, неудовлетворенность ситуацией, генерирование идей и др. Применение информационно-психологического оружия обычно происходит в глобальных сетях гражданского назначения. Оно представляет собой совокупность средств, методов и технологий, обеспечивающих возможность воздействия на информационную сферу противника с целью разрушения его информационной инфраструктуры, системы управления, в целом, снижения уровня безопасности [12, с. 9]. И. Л. Морозов различает три вида информационно-психологического оружия относительно стратегии нападения: 1. Системы дистанционного искажения или уничтожения информации: компьютерные вирусы общего и специализированного назначения (программы, проникающие извне и разрушающие систему); логические бомбы, тайно внедряемые в компьютер на этапе заводской сборки, которые при активизации парализуют работу компьютера; 2. Системы хищения информации: электронные шпионы (программы, проникающие извне и производящие незаметный для пользователя сбор служебной и непосредственно личной информации); системы комплексного воздействия на психику пользователя: мультимидийные сайты в виде информационно-развлекательных или аналитических страниц с "горячей", "сенсационной" информацией [13].

Существует мнение, что повышение уровня "прозрачности" и доступности информации для всех участников политического процесса (например, в случае проведения президентских и парламентских выборов) облегчает общественный контроль за ним со стороны общественности. Однако И. Л. Морозов выделяет два блока угроз, ведущих к подрыву политических режимов: системные и периферийные угрозы. 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 (или транснациональной структуры), 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 террорис-

тических организаций до всевозможных хакерских групп. Неструктурируемость, диффузность и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной защиты от них [13].

И. А. Василенко, анализируя состав политических акторов, различает их на носителей власти и внесистемную оппозицию [14, с. 24 - 25]. Сетевые пользователи, составляющие внесистемную оппозицию, делятся им на две группы - легальное "самобытное сопротивление", которое находит себе опору в традиционных и нетрадиционных ценностях сообщества, и на нелегальные криминально-мафиозные сети. Основной силой легального и нелегального сопротивления является исключительно сетевая, децентрализованная форма организации и политических действий. Характерным примером такого сопротивления становится стремительно нарастающее движение антиглобалистов, которое строится на основе национальных и международных сетей, активно используется Интернет, и при этом сети не только обеспечивают организацию их деятельности, но и совместное использование информации.

Децентрализованный, неуловимый характер сетевых структур сопротивления антиглобалистов и других самобытных движений (экологисты, "зеленые", женские движения, различные молодежные субкультуры, представленные, в частности, в блогосфере) во многом затрудняет их восприятие и идентификацию со стороны государственного управления. "Новые гибкие сетевые структуры внесистемной оппозиции становятся сегодня главным козырем в борьбе с неповоротливыми институтами политической власти, которая в большинстве случаев имеет старую иерархическую организацию и только отдельные силовые подразделения в ней перестроены по сетевому принципу" [14, с. 24 - 25].

В итоге, на наш взгляд, можно выделить основные группы информационных угроз безопасности личности, общества, государства, обусловленных сетевыми коммуникациями.

- *Угрозы безопасности личности, связанные с расширением возможностей манипулирования сознанием человека, информационной перегрузкой, с ростом Интернет-зависимости и развитием форм психосоциальной депривации. К этой же группе отнесем угрозы использования во вред персональных данных (расширение возможностей скрытого сбора персональной информации).*

- *Информационные угрозы, связанные с расширением масштабов манипуляции общественным мнением, появлением возможностей эффективной организации деструктивных процессов в ценностных системах общества.*

- *Угрозы безопасности личности, общества, государства, связанные с работой сетевых структур отечественной и международной преступности и терроризма.*

- *Угрозы стабильности существующих политических режимов власти: системные и периферийные, также обусловленные сетевой логикой многих социальных процессов в обществе.*

Полагаем, *что* здесь приведен далеко не исчерпывающий список групп угроз. В доктрине Информационной безопасности РФ от 2000 года выделяются три основных группы методов обеспечения информационной безопасности: правовые, организационно-технологические и экономические [7]. На наш взгляд, отдельно необходимо говорить о формировании общих и профессиональных компетенций в области работы в сетевом коммуникативном пространстве, как о важнейшей группе методов обеспечения информационной безопасности. Под компетенциями мы понимаем знание сетевого коммуникативного пространства, его проблемных аспектов, а также навыки и умения работы в нем.

Сегодня человек все чаще связывает свою профессиональную деятельность, образование, досуг, пользование услугами с социальными сетями, с различными виртуальными сообществами, с сетевыми организационными структурами. С развитием сетевого коммуникативного пространства образуется разрыв между сетевым принципом организации и традиционной управленческой деятельностью. Территориальные организационные структуры начинают претерпевать серьезные реконструкции. Частично они становятся дисфункциональными. И. А. Василенко отмечает, что отдельные виды

политической деятельности не исчезают, а исчезает их прежнее структурное значение в поле социального, политического управления, оно переходит в новую логику информационного сетевого пространства [14]. В литературе (в работах М. Кастельса, У. Бека, Дж. Урри, В. Л. Иноземцева, Д. В. Иванова, И. А. Василенко и др.) часто встречается точка зрения, что власть в условиях информационного, сетевого общества перестает быть монополией государственных институтов и политических партий. Она распространяется по глобальным сетям богатства, информации и имиджей, которые циркулируют и видоизменяются, не привязанные к какому-либо одному географическому месту. М. Кастельс отмечал, что новая власть заключается в информационных кодах, в представительских имиджах. На их основе общество организует свои институты, а люди выстраивают свои действия и принимают решения [15]. Победитель на виртуальной политической сцене обладает реальной политической властью. Современное социальное пространство общества начинает формироваться по новым правилам и принципам политической игры, которые диктует специфика информационных, сетевых технологий. "Между тем, наше политическое зрение так привыкло к сакраментальным политическим организациям - к трем ветвям политической власти, к государственным структурам, к ярким знаменам и лозунгам политических партий, что мы испытываем вполне понятное чувство растерянности перед виртуальными формами политической борьбы, перед натиском информационной агрессии, перед стремительно расширяющимся миром символов" [14, с. 15].

Сравнительно недавно российское общество приступило к решению серьезнейшей задачи - построению основных демократических институтов: формирование многопартийной политической системы, системы демократических выборов, независимой судебной системы власти, гражданского общества и др. Мы сталкиваемся с парадоксом: с одной стороны в России начинают развиваться и набирать силу институты политической демократии, с другой же стороны, они, еще не сформировавшись в должной мере, уже перестают играть заметную роль в жизни общества. Развитие информационного сетевого пространства демонстрирует противоречивую тенденцию: чем современнее становится общество, тем большее значение в нем придается не институтам и социальным нормам, а самим действующим лицам и их имиджам, разворачивающимся в сетевом пространстве, причем на виртуальной политической сцене [14].

Современный мир столкнулся с удвоением социальной реальности - с появлением виртуальной реальности, где актор получает большую свободу, реализуя "актуальное виртуальное действие" [16]. Отсутствие компетенций в сфере определения и прогнозирования сетевых коммуникативных процессов ведет к обострению проблемы информационной безопасности. Виртуальная социальная реальность, структурируемая сетевыми коммуникациями, не знает ограничений, сформированных традиционными социальными нормами, это мир, лишенный социального порядка в традиционном его понимании. С другой стороны, это ускользающий мир, где интенсивность коммуникаций всякий раз возрастает, отдаляя возможности его адекватного осмысления. Названные два момента в особенностях социальной виртуальной реальности сетевого коммуникативного пространства уже закладывают проблематику безопасности общества и призывают к ответственности человеческий разум.

СПИСОК ЛИТЕРАТУРЫ

1. *Белинская Е. П.* Человек в информационном мире, http://psynet.carfax.ru/texts/bel3.htm.

2. *Тираспольский Л.* К вопросу жанра виртуальной конференции // Компьютера ONLINE http: // www.computerra.ru/offine/2000/362/4482

3. *Кузнецова Ю. М., Чудова Н. В.* Психология жителей Интернета. М.: Изд-во ЛКИ, 2008.

4. *Игнатьев В. И.* Системно-генетическая динамика социума. Новосибирск: Изд-во НГТУ, 2007.

5. *Романов О. В.* Философия Интернета (генезис и синтез фундаментальных идей). Самара: Перспектива, 2003.

6. *Пронина Е. Е.* Психология журналистского искусства. М.: Изд-во Моск. ун-та, 2002.

7. Доктрина информационной безопасности РФ.
http://www.rg.ru/oficial/doc/min_and_vedom/min_bezop/doctr.shtm

8. *Корытникова Н. В.* Интернет-зависимость и депривация в результате виртуальных взаимодействий // Социол. исслед. 2010. N 6.

9. *Черных А. И.* Социология массовых коммуникаций: учебное пособие. М.: Изд. дом ГУ-ВШЭ, 2008.

10. *Ревич Ю.* Реалии виртуальности. Нужен ли России специальный закон об Интернете? // ФСБ "за" и "против". 2009. N 2.

11. Интервью с первым заместителем председателя комитета по безопасности Государственной Думы РФ М. И. Гришанковым // ФСБ "за" и "против". 2009. N 2.

12. *Бухарин С. Н., Циганов В. В.* Методы и технологии информационных войн. М.: Академический проект, 2007.

13. *Морозов И. Л.* Информационная безопасность политической системы // Политические исследования. 2002. N 5. С. 134 - 144.

14. *Василенко И. А.* Политическая философия: Учебное пособие. М.: Гардарики, 2004.

15. *Кастельс М.* Информационная эпоха: экономика, общество и культура. М.: Изд-во ГУ-ВШЭ, 2000.

16. *Игнатьев В. И., Владимирова Т. В., Степанова А. Н.* Социальная система как информационное взаимодействие. Новосибирск: Изд-во НГТУ, 2009.

17. Национальный стандарт РФ "Защита информации. Основные термины и определения" (ГОСТ Р 50922 - 2006). http://www.e-nigma.ru/stat/gost4