
СОЦИОЛОГИЯ

УДК 004.056

ББК 32.973

А 50

Алиева М.Ф.,

*кандидат социологических наук, зам. декана физического факультета
Адыгейского государственного университета, Майкоп, тел. (8772)59-37-36*

Информационная безопасность как элемент информационной культуры (Рецензирована)

Аннотация: Статья посвящена определению влияния информационной безопасности на информационную культуру и развитие современного общества. Информационная безопасность общества в целом и его структурных частей обусловлена, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими и всеохватывающими.

Ключевые слова: информационная безопасность, информационные взаимодействия, информационное пространство, ценностные ориентации личности, технический прогресс, социально-культурологический аспект, информационно-коммуникативные процессы, информационные и телекоммуникационные системы.

M.F. Aliyeva,

*Candidate of Sociology, Deputy Dean of Faculty of Physics, Adyghe State
University, Maikop, ph.: +7(8772)59-37-36*

Information security as an element of information culture

Abstract: The paper deals with the definition of influence of information security on information culture and development of modern society. Information security of society as a whole and its structural parts is caused, first of all, by quickly growing technological capabilities of modern information systems which, by their influence on policy, economic life, spiritual and ideological sphere and moods of people, have become now decisive and comprehensive.

Keywords: information security, information exchanges, information space, value orientations of the personality, technical progress, social and culturological aspect, information and communicative processes, information and telecommunication systems.

Начало третьего тысячелетия ознаменовано рождением общества нового типа — информационного, в котором основным стратегическим ресурсом становится информация. Влияние, которое оказывают информационные процессы на все сферы жизни общества, актуализирует важнейшие вопросы социального бытия, в том числе вопросы информационных взаимодей-

ствий, включая борьбу за информационное пространство и противодействие различного рода информационным угрозам. В связи с этим не может не меняться ситуация в отношении исследования ценностной ориентации личности, ее информационного обоснования и информационной безопасности.

Роль информационной сферы, которая представляет собой совокупность

информации, информационной инфраструктуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также систем регулирования возникающих при этом общественных отношений, значительно возросла на современном этапе развития общества. Являясь важным фактором жизни общества, информационная сфера оказывает существенное влияние на состояние политической, оборонной и экономической составляющих безопасности России. От обеспечения информационной безопасности существенно зависит национальная безопасность России, и эта зависимость будет значительно возрастать в ходе технического прогресса и проникновения информационных технологий во все сферы деятельности современного общества.

В связи с этим информационная безопасность становится важнейшим базовым элементом всей системы безопасности российского государства. Обусловлено это, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими и всеохватывающими.

Проведенный нами анализ исследованности проблемы информационной безопасности показал, что, несмотря на огромный интерес к проблеме, ее изучение имеет преимущественно технико-прикладной характер и ориентировано на решение конкретных научно-технических задач. Лишь в немногих работах актуализируется социально-культурологический аспект проблемы информационной безопасности духовной сферы, обеспечения целостности, достоверности и доступности культурно-исторической информации, постоянное изменение текущей ситуации, отсутствие эффективных методик решения возникающих вопросов применительно к конкретным задачам сферы инфор-

мационной культуры, требует системного подхода. Информационная безопасность в контексте культурной жизни общества лишь начинает исследоваться, и целые области знания, связанные с функционированием различных социальных институтов, остаются мало изученными.

Исследованию социологических аспектов информатизации, социологическому анализу общества, обращенному к роли информационных процессов, посвящены работы Т.Н.Ананьевой, С.В.Балабая, Л.А.Василенко, М.Е.Васильева, Т.П.Вороной, Н.Д.Данилиной, О.Н.Дудко, Т.В.Ершовой, В.И.Иванова, Л.В.Климовой, И.В.Куприянова, С.В.Ляшко, А.Масловым, И.С.Мелюхина, Ю.А.Нисневича, В.В.Печенкина, С.В.Рабовского, Г.П.Смоляна, Д.С.Черешкина, И.В.Юшкиной и др.

Научное осмысление различных аспектов информационной безопасности активно проводилось отечественными учеными А.В.Возжениковым, Ю.Ф.Нуждиным, Е.Н.Пасхиным, Е.Е.Перчук, А.И.Поздняковым, Г.Г.Почепцовым, А.А.Прохожевым, С.П.Расторгуевым, А.А.Стрельцовым, Г.Л.Смоляным, Д.С.Черешкиным, А.С.Шийко, В.Н.Цыгичко и другими.

Итак, степень научной разработанности проблемы свидетельствует о том, что сегодня информационная безопасность занимает одно из центральных мест в научных изысканиях. Вместе с тем анализ работ показывает, что информационная безопасность как объект социологии культуры, хотя и находится в поле зрения ученых, однако информационно-коммуникативные процессы, происходящие в современном российском обществе, в качестве объекта комплексного социологического исследования представлены недостаточно.

Следует отметить, что разнообразие подходов к понятию информации в значительной степени определяется спецификой сфер, в которых данное понятие используется. Различия в способах передачи информации, видах информационных угроз и формах

представления готовых информационных продуктов диктует различные взгляды на исследование ключевых аспектов информационной безопасности. Соответственно этому специфика сферы культуры требует своего, особого подхода к изучению данной проблемы.

Опираясь на труды классиков философии, культурологии, социологии, а также новейшие исследования в области естественнонаучных дисциплин, мы берем за основу своего исследования атрибутивную концепцию информации, в которой последняя рассматривается как атрибут материи, ее всеобщее и существенное свойство. В данном контексте, информация представляет собой меру определенности, организованности, упорядоченности, сложности и разнообразия. Как следствие информация связывается с другим всеобщим свойством материи — отражением, т. е. информацию можно трактовать как содержание отражательного процесса, или как инвариантную часть отражения, которая может быть определена и передана от одной системы другой. В этой связи основная задача по обеспечению информационной безопасности в сфере культуры заключается в сохранении механизмов социальных взаимодействий, стабилизации функционирования социокультурных систем [1].

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной.

Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия и т. п.

Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа ком-

понентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной системы можно разбить на следующие группы:

— аппаратные средства — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);

— программное обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

— данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

— персонал — обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в автоматизированной системе является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:

— для представления информации — машинные носители информации в виде внешних устройств компьютерных систем, оперативной памяти, файлов и т. д.;

— объектам системы — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;

— субъектам системы — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается

обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы [2].

Основными компонентами информационной безопасности в области культуры являются: достоверность и полнота информации; обеспечение документирования историко-культурного процесса; сохранность информации, рассматриваемой не только как сохранность материальных носителей культурно-исторической информации, но и как бережное отношение к эмоционально-образной составляющей культурного наследия; качество и эффективность культурно-исторической информации, определяющие ведущую роль достоверного культурного наследия и культурных ценностей в регуляции массового сознания; обеспечение соответствия объектов культурного наследия и их атрибуции с целью недопустимости его — культурного наследия — искажения в коммерческих и других целях; сохранение историко-культурного контекста представляемой различными учреждениями культуры и образования информации и недопустимости его искажения в целях продвижения идеологии отдельных социальных групп; обмен и сотрудничество между учреждениями культуры, образования, СМИ в целях более полного и достоверного представления достоверного культурно-исторического наследия.

Информация на всех этапах исторического развития человечества являлась объектом борьбы. Сегодня правомерно утверждать: чем большими информационными возможностями обладает государство, тем вернее оно добивается стратегических геополитических преимуществ. Отсюда становится понятным, почему многие государства рассматривают информацию как стратегический ресурс.

Серьезную опасность представляют собой стремление ряда государств к доминированию в мировом информационном пространстве, разработка рядом государств концепции инфор-

мационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получении несанкционированного доступа к ним. Реалией наступившего информационного века является информационная война, а не противостояние армий, погибающих на полях генеральных сражений. Война в зоне Персидского залива может быть определена как первая полномасштабная война нового этапа в функционировании вооруженных сил в условиях создания глобального мирового информационного пространства.

Влияние информационных технологий, кроме военных операций наглядно демонстрируют события в экономической и финансовой сферах. Искусственное создание экономических кризисов можно смело приравнять к стратегическим информационным операциям. Таким образом, информационное противоборство меняет представление о том, что такое супердержава. Ядерное оружие как фактор стабильности и доминирования после Карибского кризиса 1962 года отходит на второй план, ему на смену приходит оружие информационное, которое позволяет реально управлять политикой государств.

Более того, в начале XXI века особенно обостряется опасная тенденция — появление и распространение глобального экстремизма, как действующей силы в международных отношениях. Главная особенность заключается в том, что террористы используют в международной политике технологии «стравливания» государств, для достижения своих целей, особенно таких крупных конгломератов, как США и Россия. Достаточно заметно данная тенденция проявилась со второй половины 90-х годов на примере ожесточившегося информационно-геополитического противоборства США и ряда стран

Западной Европы с Россией и ее союзниками. Для осуществления этого использовалась информация и, следовательно, информационное оружие.

Под таким мощным натиском этого сверхточного информационного оружия мировое сообщество дробится, раскалывается на части, искажается самовосприятие и восприятие других народов, теряется самоидентичность народов, порождается агрессия невероятных масштабов, усиливаются сепаратистские настроения. Поскольку современная идеология информационной войны базируется на символическом восприятии мира, система управления этими трудно обратимыми процессами упрощается [3].

В теоретико-методологическом отношении мы основываемся на принципах историзма и достоверности, на концепциях развития культуры, личности и общества, важнейшими принципами которой являются: принцип объективности в интерпретации рассматриваемого материала, принцип системности и конкретности рассмотрения фактов, требующих от исследователя анализировать любое общественное явление в процессе развития, учитывая при этом национально-региональную специфику, во всем многообразии его генетических и причинных взаимосвязей. В работе использован также комплексный системный анализ исследуемой проблематики, что помогает установить полиаспектность понимания проблемы и множественность способов ее решения.

Проблема защиты информации от несанкционированного доступа, изменения или повреждения исследуется человеком с древнейших времен. Были разработаны необходимые технологии, учреждены специальные службы и сформированы соответствующие подразделения. Все это отчасти остается актуальным и сегодня. Однако всеобщая компьютеризация, охватившая практически все сферы общественной деятельности привела к тому, что: все большие массивы информации хранятся на машинных носителях и обрабатываются по электронной технологии, интенсивно идет процесс слияния

традиционных и автоматизированных технологий обработки информации; информация становится более доступной, а скорость ее распространения более высокой.

Если раньше защите подлежали преимущественно государственные и военные секреты, то сейчас, наряду с ними, защите подлежат тайны коммерческие, промышленные, банковские и некоторые другие; защищать надо авторское право и право собственности на информацию; возникает необходимость защиты конфиденциальной и персональной информации и т.п. Все это настоятельно требует существенного изменения взгляда, во-первых, на проблемы безопасности информации и качества совершенствования способов, методов и средств ее обеспечения. Во-вторых, на вопросы информационной культуры современного человека. Компьютер является инструментом для работы, учебы, досуга и коммуникации почти для каждого члена современного общества, причем большинство из них не имеют профессиональных знаний по вопросам защиты информации.

Проблемы информационной безопасности можно разделить на три больших группы:

1. Проблемы гуманитарного характера — проблемы информационной безопасности, возникающие в связи с бесконтрольным использованием и распространением персональных данных граждан, вторжениями в частную жизнь, клеветой и кражами личности.

2. Проблемы экономического и юридического характера — проблемы информационной безопасности, возникающие в результате утечки, искажения и потери коммерческой и финансовой информации, краж брендов и интеллектуальной собственности, раскрытия информации о материальном положении граждан, промышленного шпионажа и распространения материалов, наносящих ущерб репутации компаний.

3. Проблемы политического характера — проблемы информационной безопасности, возникающие из-за информационных войн, кибервойн

и электронной разведки в интересах политических групп, компрометации государственной тайны, атак на информационные системы важных оборонных, транспортных и промышленных объектов, неполного информирования и дезинформации руководителей крупных учреждений.

Описываемых проблем можно избежать, если рассматривать вопросы информационной безопасности не только при обучении соответствующих специалистов, но и включать в перечень системообразующих компонентов понятия «информационная культура» элементов информационной безопасности, которыми, по нашему мнению, сегодня должен владеть не только специалист в области защиты информации, но и каждый, пользователь компьютера.

По нашему мнению, решение проблемы обеспечения информационной безопасности личности, должно носить комплексный системный характер и осуществляться на разных уровнях.

Первый уровень — нормативный. На данном уровне органы государ-

ственной власти должны создать непротиворечивую нормативную базу, учитывающую все аспекты проблемы информационной безопасности.

Второй уровень — институциональный, включает в себя согласованную деятельность различных социальных институтов, связанных с воспитанием и социализацией, по обеспечению информационной безопасности личности.

Третий уровень — личностный. Этот уровень связан, прежде всего, с самовоспитанием, самообразованием, формированием высокого уровня информационной культуры личности как части общей культуры человека. На данном уровне происходит формирование необходимых личностных качеств для обеспечения информационной самозащиты личности.

Итак, информационная политика тесно связана с проблемами обеспечения безопасности личности, а также социума в целом. Особенно ярко это проявляется в России, где информационные системы имеют тесную связь с властными структурами.

Примечания:

1. Хитарова И.Ю. Духовная жизнь общества как объект информационной безопасности // Этносоциум и межнациональная культура. 2008. №6. Р.37-47.

2. Основные понятия защиты информации и информационной безопасности. [Электронный ресурс]. URL: <http://ypn.ru/102/introduction-to-information-protection-and-information-security/> (дата обращения 28.11.12).

3. Астахова Л.В. Сущность понятия «Культура информационной безопасности» и ее формирование у студентов вуза / Л.В.Астахова // Экономика. Информатика. Безопасность. Сборник научных трудов Международной научно-практической конференции, 2007 / Науч. ред. В.А.Киселева, Л.В.Астахова. — Челябинск, Изд-во ЮУрГУ. — 2007. — С. 93-99.

References:

1. Khitárova I.Yu. Spiritual life of society as object of information security // Ethnosociety and international culture. 2008. No. 6. P. 37-47.

2. The main concepts of information protection and information security. URL: <http://ypn.ru/102/introduction-to-information-protection-and-information-security/> (date of the address 28.11.12).

3. Astakhova L.V. The essence of the concept “Culture of Information Security” and its formation at students of higher education institution / L.V.Astakhova // Economy. Informatics. Security. Proc. Intern. Sci. and Practical Conf., 2007 / Sci. Eds. V.A.Kiseleva, L.V.Astakhova. — Chelyabinsk, YuUrGU Publishing house. 2007. P. 93 — 99.