УДК 338.23

Букова Анастасия Владимировна

бакалавр экономики
бухгалтерский учёт, анализ и аудит
Финансовый университет при
Правительстве Российской Федерации
Челябинский филиал
Россия, Челябинск

nenss@mail.ru

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Аннотация

В исследовании выявлены основные закономерности и методы функционирования информационной безопасности, определена концепция, цели и основные объекты, раскрыты содержание, функции и условия укрепления информационной безопасности современного российского гражданского общества, вычленены сущность, и дана классификация информационных рисков, опасностей и угроз, определены их источники, глобальный характер и социальная составляющая. Сформулированные в работе выводы имеют непосредственное значение для рационализации государственной информационной политики, повышения ее предметности.

Ключевые слова:

информационная безопасность, информатизация общества, социальные процессы

Anastasia V. Bukova

Bachelor of Economics
accounting, analysis and audit
Financial University at the Government
of the Russian Federation
Chelyabinsk branch
Russia, Chelyabinsk

nenss@mail.ru

INFORMATION COMPONENT OF THE NATIONAL SECURITY OF RUSSIA

Abstract

The study identified the main patterns and methods of operation of information security, defined the concept, objectives and main objects disclosed the content, functions and terms of strengthening information security of modern Russian civil society, fleshed out the essence, and the classification of information risks, dangers and threats identified their sources, global and social component. Formulated in the findings have direct relevance to the rationalization of the state information policy, increasing its objectivity.

Keywords:

information security, information society, social processes

Современное информационное общество может быть представлено как специфическое социальное пространство, включающее системные и проблемные семантические зоны, которые в совокупности определяют условия функционирования общества, проблематику и перспективность его развития в эпоху научно-технического прогресса. Информационная безопасность институтов и субъектов общества основана на эффективном обеспечении составных частей информационной безопасности, нуждающихся в управлении процессами их формирования и поддержания на основе социологической парадигмы.

Современное понимание проблематики информационной безопасности социума почти не учитывает социологических подходов, социальные аспекты функционирования общества в условиях динамичных информационных процессов,

проблемы социальной адаптации, социальных последствий воздействия на него информационных процессов изучаются и исследуются, но, в то же время, практически не увязываются с феноменом информационной безопасности, которая до сих пор традиционно относится в плане изучения и исследований к области информатики, кибернетики и т.д. В то же время социальная система демонстрирует тенденции, выходящие за пределы технических решений, и нуждается как в макро-социологическом исследовании социального управления безопасностью информационной среды, так и в анализе микроуровня социальных отношений и обмена и передачи знаний.

Информационная безопасность: понятие, сущность, содержание

Информация (от лат «informatio» – разъяснение, изложение, ознакомление) объективна, существует вне зависимости от познавательных возможностей познающего субъекта и является одним из фундаментальных свойств материального мира.

Понятие информационной безопасности следует рассматривать как видовое по отношению безопасности в целом, и именно исходя из общих определений безопасности, под информационной безопасностью следует понимать такое состояние информационного пространства страны, при котором его основным характеристикам: целостности, доступности и конфиденциальности, – ничего не угрожает или обеспечена достаточно надежная защиты от угрозы, то есть информационное пространство находится в состоянии защищенности.

Информационную безопасность, следует понимать, как феномен, связный с функционированием и развитием государства. Для этого существует два веских основания. Во-первых, не имея физических границ, информационное пространство, тесно связано с имеющим четкие границы социально-политическим пространством и является отражением социальных и политических проблем и процессов в поле информации. Во-вторых, основными потребителями, реципиентами социально и политически значимой информации являются граждане, связанные с определенным социально-политической реальностью, границы которой определяются государством.

Информатизация общества, развитие гражданского общества и демократизация в единстве и взаимосвязи образовали цивилизацию нового гражданского типа. Демократия особенно остро испытывает потребность в

информационной безопасности, но только в гражданской цивилизации эта потребность может быть в полной мере обеспечена, поскольку субъектами, разделяющими взаимный интерес в целостности и доступности информационного пространства, и обладающими достаточными ресурсами для его реализации, могут являться только демократическое государство и гражданское общество.

Двуукладность цивилизационного развития России приводит к тому, что национальные интересы российского общества в сфере информационной безопасности также имеют два полюса. Государственные институты (и это подтверждается всеми доктринами и нормативными актами в данной сфере) отстаивают и охраняют концепцию информационной безопасности, в которой главным объектом охраны является национальная идентичность. На основе этих интересов формируются нормы, регулирующие функционирование информационного пространства, а также деятельность основных акторов, определяющих его содержание: в первую очередь, средств массовой информации. На противоположном полюсе – концепция национальных интересов, в основе которой лежат потребности общественного развития в направлении становления гражданской информационной цивилизации. Ее отстаивают институты гражданского общества, оппозиционные партии, независимые СМИ.

Российскому обществу еще требуется пройти длительный путь к тому, чтобы национальные интересы в информационной сфере представляли собой действительно «сбалансированную совокупность социальных интересов личности, общества и государства, реализуемых в информационной сфере», включая как интересы в сохранении национальной идентичности, так и интересы в развитии гражданского типа цивилизационных отношений.

Внешние угрозы в структуре информационной безопасности России

Внешние угрозы информационной безопасности России рождаются в контексте следующих геополитических тенденций:

- формирование единого глобального информационного пространства западных стран и США и оттеснение информационного пространства России к глобальной периферии, превращение России в глобальную информационную провинцию;

- уплотнение информационной взаимозависимости государств, прежде всего, формирование Интернет-инфраструктуры вокруг государств НАТО (США и

Великобритания производят более 90 % мировой высокотехнологичной продукции, поэтому их приоритет неоспорим);

- расширение стратегического военно-информационного пространства НАТО (за счет информационного пространства стран Восточной Европы, Балтии, Молдовы, Украины), его приближение к географическим границам России и проникновение в ее информационные границы;

- вторжение информационных акторов США в информационное пространство России, причем как по техническим, так и по идеологическим каналам;

- стирание граней между состояниями войны и мира, распространение стратегий и тактик информационных (нелетальных) войн, главные участники которых (например, США), рассматриваю Россию в качестве потенциального противника;

- геополитическая перегруппировка сил в информационном пространстве за счет информационного прогресса США, Западной Европы, Японии, Китая, утрата Россией геостратегического преимущества в информационной сфере;

- утрата Россией многих традиционно надежных геополитических союзников;

- информатизация мирового терроризма и экстремизма;

- «обострение международной конкуренции за обладание технологическими и информационными ресурсами, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики»;

- формирование негативного образа России и имиджа российской политической элиты иностранными СМИ и др.

Методология и результаты

В контексте темы исследования предлагаются следующие технологии:

1. Социальные технологии корпоративной культуры.

Решение проблемы информационной безопасности организации как общественной структуры должно осуществляться на основе внедрения надлежащей корпоративной культуры, локализующей и профилактирующей инсайдерские информационные угрозы. Этому способствуют тенденции и технологии управления, связанные с усилением влияния корпоративной культуры и иных корпоративных факторов.

Субъекты: организации (корпорации), как профессионально-устойчивые социальные группы общества.

Методы: социологический мониторинг, исторический метод, метод экспертных оценок.

Проблемы внедрения: недооценка руководством и коллективом многих организаций значимости корпоративной культуры как элемента формирования информационной безопасности субъекта и управления организацией в целом.

Пути преодоления. Внедрение элементов корпоративной культуры, сопоставление, оценка результативности на основе соц. опросов в коллективе.

2. Социальные технологии информационной культуры.

Суть технологии состоит в социализации предупреждения асоциального поведения личности и морально-нравственной деградации общества, преодоление отчуждения человека от общественных отношений, формирование условий для максимально полной и свободной саморегуляции в обществе.

Субъекты: общество, его социальные институты, социальные группы, средства массовой коммуникации, государство, как стимулирующий и поддерживающий фактор.

Методы: социологический мониторинг, контент-анализ средств массовой коммуникации, исторический метод, сравнительный метод,

Проблемы внедрения: коммерциализация средств массовой коммуникации, ставящая на второй план онтологические ценности общества, атараксия гражданских и государственных институтов от данной проблемы.

Пути преодоления указанных проблем. Активно внедрять присущие российскому обществу традиционные морально-нравственные и духовные ценности, при этом резко критикуя вредное, навязываемое в сознание общества современными информационными продуктами. Социальные технологии информационной культуры должны создаваться на положительных примерах нашей истории, нашей повседневности, включая такие понятия как патриотизм, социальная ответственность, единение российского социума как уникального геополитического образования.

Рассмотренные в работе вопросы подводят к выводу о том, что современные технологии, призванные содействовать процессам формирования информационной безопасности общества и управлению ими с учетом тенденций развития общества,

все более приобретают выраженное социальное содержание и способны решить актуальные вопросы защиты общества в информационной сфере, как крупной научной проблемы, имеющей важное социально-культурное значение.

На основе рассмотренных теоретических положений по информационной безопасности общества и анализа результатов собственного эмпирического социологического исследования был разработан ряд социальных технологий, способствующих оптимизации управления процессами формирования информационной безопасности социума.

Социальные процессы, управление ими, равно как и социальные технологии, во многом отражающие и детерминирующие эффективность управления, присутствуют практически во всех процессах социальной динамики: индивидуального взаимодействия, группового и межгруппового взаимодействия. В широком смысле этого понятия именно социальные технологии представляют собой особый вид социальной теории, которая после осмысления вопросов о качественной и количественной определенности изучаемого общественного явления ставит и обосновывает вопрос о том, как, каким образом и в какой последовательности возможны специфические операции с результатами познавательной деятельности.

Список использованной литературы

1. Доктрина информационной безопасности Российской Федерации // Независимая газета. – 2000. – 19 сент.

2. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов. – М. : МЦНМО, 2002. – 296 с. – С. 69.