УДК 339.727.22/24:338.47

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Н.А. Сейдакматов

Анализируются современные проблемы обеспечения национальной безопасности Кыргызской Республики, имеющие комплексный, многогранный характер.

Ключевые слова: национальная безопасность; информационная безопасность; нормативно-правовая база; информационно-техническая инфраструктура; кибертерроризм.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на стояние политической, экономической, оборонной и других составляющих безопасности Кыргызской Республики и существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

К основным компонентам национальной безопасности относятся военная, экономическая, социальная, экологическая, информационная безопасность. Сама национальная безопасность представляет собой геополитический аспект безопасности вообще, охватывающий весь комплекс вопросов физического выживания государства, защиты и сохранения его суверенитета и территориальной целостности. В той мере, в какой задачи обеспечения национальной безопасности являются производными от национальных интересов, концепции национальной безопасности также связаны с теоретическим обобщением данных интересов [1, с. 37–48].

В настоящее время проблема информационной безопасности стоит еще более остро, поскольку

ку значительно возросла роль накопления, обработки и распространения информации, в частности в принятии стратегических решений, увеличилось количество субъектов информационных отношений и потребителей информации. Информация играет все большую роль в процессе жизнедеятельности человека. Об этом свидетельствует хотя бы тот факт, что средства массовой информации часто называют четвертой ветвью власти.

Важным результатом распространения информационных и коммуникационных технологий и проникновения их во все сферы общественной жизни является создание правовых, организационных и технологических условий для развития демократии за счет реального обеспечения прав граждан на свободный поиск, получение, передачу, производство и распространение информации.

Вместе с тем недостаточное развитие информационных и коммуникационных технологий в нашей республике усугубляется целым рядом факторов, создающих препятствия для широкого внедрения и эффективного использования этих технологий в экономике. К числу таких негативных факторов относятся:

- несовершенная нормативная правовая база, разрабатывавшаяся без учета возможностей современных информационных и коммуникационных технологий;
- недостаточное развитие информационных и коммуникационных технологий в области государственного управления, неготовность органов государственной власти к применению эффективных технологий управления и организации взаимодействия с гражданами и хозяйствующими субъектами;
- отсутствие целостной информационной инфраструктуры и эффективной информационной поддержки рынков товаров и услуг, в том числе в сфере электронной торговли;
- недостаточный уровень подготовки кадров в области создания и использования информационных и коммуникационных технологий.

Изменения, происходящие в информационной сфере, с одной стороны, обусловливают переход к единым стандартам, с другой – характеризуются возведением новых барьеров, связанных с обеспечением безопасности личности, общества и государства в целом.

Информационная безопасность общества и государства определяется степенью их защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы страны информационным воздействиям на уровне как внедрения, так и извлечения информации [2].

Информационная безопасность личности характеризуется защищенностью психики и сознания от опасных информационных воздействий: манипулирования, дезинформирования, побуждения к самоубийству, оскорблений и т. п.

Опасные информационные воздействия обычно разделяют на два вида. Первый связан с утратой ценной информации и либо снижает эффективность собственной деятельности, либо повышает эффективность деятельности противника, конкурента. Если объектом такого воздействия является сознание людей, то речь идет о разглашении государственных тайн, вербовке агентов, специальных мерах и средствах для подслушивания, использовании детекторов лжи, медикаментозных, химических и других воздействиях на психику человека. Безопасность от информационного воздействия данного вида обеспечивают органы цензуры, контрразведки и другие субъекты информационной безопасности. Если же источником информации служат технические системы, то речь идет уже о технической разведке или шпионаже (перехват телефонных разговоров, радиограмм, сигналов других систем коммуникации), проникновении в компьютерные сети, банки данных [2].

Второй вид информационного воздействия связан с внедрением негативной информации, что может не только привести к опасным ошибочным решениям, но и заставить действовать во вред, даже подвести общество к катастрофе. Информационная безопасность этого вида должны обеспечивать специальные структуры информационно-технической борьбы. Они нейтрализуют акции дезинформации, пресекают манипулирование общественным мнением, ликвидируют последствия компьютерных атак.

Развитие и внедрение в различные сферы жизни общества новых информационных технологий, как и любых других научно-технических достижений, не только обеспечивает комфортность, но и нередко несет опасность.

Выделим наиболее существенные группы информационно-технических опасностей, обусловленных достижениями научно-технического прогресса в условиях глобализации. Первая группа связана с бурным развитием нового класса информационного оружия, которое способно эффективно воздействовать на психику и сознание людей и на инфомационно-техническую инфраструктуру общества. В относительно мирных условиях информационно-психологические технологии могут применяться в качестве специальных механизмов

управления кризисами и провоцирования жестокости на территории противника. Вторая группа информационно-технических опасностей для личности, общества и государства – это новый класс социальных преступлений, основанных на использовании современных информационных технологий (махинаций с электронными деньгами, компьютерное хулиганство и др.). Вопрос обеспечения информационной безопасности как одной из важных составляющих национальной безопасности государства особенно остро встает в контексте появления транснациональной, трансграничной компьютерной преступности и кибертерроризма. Третья группа информационных опасностей – использование новых информационных технологий в политических целях.

Информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. А информационная сфера (среда) – это сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации. В научной литературе в составе информационной сферы общества выделяют субъектов, общественные отношения, информационную инфраструктуру общества и информацию [3].

К основным принципам обеспечения информационной безопасности можно отнести: принцип соблюдения Конституции и законодательства Кыргызской Республики, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности КР.

Национальная безопасность неразрывно связана с деятельностью государства. Только оно, опираясь на свой аппарат, может властными органами, деятельность которых поставлена в жесткие рамки и подкрепляется соответствующими правовыми актами, обеспечить покой граждан, создать благоприятные условия для их жизни и деятельности. Никакие другие социальные силы не смогут выполнить этой задачи. Обеспечение собственной безопасности, а также безопасности своих граждан является одной из основных задач, но не функцией любого государства. Успешное развитие и само существование нашей республики как суверенного государства невозможно без обеспечения ее национальной безопасности. Право не может и не должно оставаться в стороне от решений проблем безопасности государства. Более того, в этом ему должна принадлежать ведущая роль.

Таким образом, по мере развития информатизации и глобализации роль информационной безопасности личности, общества и государства увеличивается, и ее обеспечение должно занять подобающее место в политике государства. Информация стала одним из факторов, способных привести к крупномасштабным авариям, военным конфликтам и дезорганизации государственного управления. И чем выше уровень интеллектуализации и информатизации общества, тем надежнее его информационная безопасность. Поэтому нашей республике необходимо уделять своей национальной безопасности особое внимание, поскольку она является основой определения важнейших направлений и принципов государственной политики страны, жизненноважных интересов личности, общества и государства.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

На основе национальных интересов Кыргызской Республики в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности [3]. К объектам информационной безопасности относятся:

- права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности;
- информационные ресурсы, вне зависимости от форм хранения, содержащие информацию, составляющую государственную тайну и ограниченный доступ, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;
- система формирования, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных;
- информационные технологии, регламенты процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;
- информационная инфраструктура, включающая центры обработки и анализа информации,

каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации.

К субъектам информационной безопасности относятся законодательная, исполнительная и судебная ветви власти Кыргызской Республики, все физические и юридические лица, способные к созданию информации и формированию информационных ресурсов, располагающие возможностями по их распространению и хранению, а также обеспечивающие их защиту.

За последние годы в Кыргызской Республике реализован комплекс мер по совершенствованию обеспечения информационной безопасности.

Начато формирование нормативной правовой базы обеспечения информационной безопасности.

Действуют Законы Кыргызской Республики "О защите государственных секретов Кыргызской Республики", "Об информатизации", "О гарантиях и свободе доступа к информации", "О Национальном архивном фонде", "Об электронной цифровой подписи", "О средствах массовой информации", "Об электрической и почтовой связи", "О правовой охране программ для электронных вычислительных машин и баз данных", "Об основах технического регулирования в Кыргызской Республике", "О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики" и ряд других; развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Вместе с тем состояние информационной безопасности Кыргызской Республики не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение [3].

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Нет четкости при проведении государственной политики в области формирования национального информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства КР в мировое информационное пространство, что создает условия для вытеснения национальных информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры КР. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании.

В Кыргызстане реализация основных прав и свобод личности в информационном поле, а также деятельность государства и других субъектов правовых взаимоотношений в сфере формирования, сохранения и рационального использования информационных ресурсов осуществляется в рамках Конституции Кыргызской Республики, ряда других законов.

Однако несовершенство нормативно-правовой базы находит свое отражение в существующем понятии "безопасная правовая информация" и вытекающих из него разноплановых интересов личности, общества и государства.

В основе безопасности правовой информации находится свобода информации и запретительный принцип права (все, что не запрещено законом, разрешено).

Гармоничное применение запретительного принципа права остается достаточно проблематичным из-за отсутствия в законодательстве Кыргызской Республики четких юридических формулировок понятия информационной безопасности, а также классификации видов информации и их соотносимости с вышеназванным принципом права.

Особое место в системе правовых информационных взаимоотношений играют средства массовой информации. Именно они в своей основе формируют общественное сознание и влияют на состояние нравственного здоровья людей. В эпоху информационной революции их роль для обеспечения информационной безопасности республики становится ключевой.

Средства массовой информации, как и силовые структуры, не могут быть самостоятельными

политическими факторами и находиться вне контроля общества и закона. Они должны функционировать в рамках установленного правового поля, исключающего их использование в ущерб интересам личности, общества и государства.

Анализ состояния информационной безопасности Кыргызской Республики дает основание сделать вывод о том, что способность личности, социальных групп, общества и государства иметь достаточные информационные ресурсы обеспечивать их защиту не отвечает современным требованиям.

Отсутствует единый подход к классификации угроз интересам личности, общества, государства в информационной сфере, не отработан понятийный аппарат, не разработана методология оценки уровня угроз и последствий их реализации.

Таким образом, можно смело утверждать, что информационная составляющая национальной безопасности республики, создаваемая и выстраиваемая уже на протяжении многих лет, принесет положительные результаты лишь в том случае, если доступ к информации и ее использование будут упорядочены прежде всего законодательным образом, а сама информация перестанет быть способом массового эпатажа аудитории, станет средством и условием формирования массового сознания граждан, интегрирования общественных сил на основе общенациональных интересов.

Информационная составляющая национальной безопасности должна быть вплетена в "ткань" всей социально-экономической системы общества, должны быть проанализированы все значимые факторы и вскрыты основные причинно-следственные связи. Поэтому и законодательное, и технологическое, и социально-экономическое обеспечение должно работать в рамках единого целого.

Литература

1. *Крутских А.* О международной информационной безопасности / А. Крутских, А. Федоров // Международная жизнь. 2000. № 2.
2. *Мамонов В.В.* Понятие и место национальной безопасности в системе конституционного строя / В.В. Мамонов // Российское право. М., 2003. № 6.
3. *Темирбаев А.А.* Информационная безопасность Кыргызской Республики / А.А. Темирбаев, Р.Н. Сагынбаев. Бишкек, 2007.