Т.1. - 8 б.

4. Абылай хан / Құраст. С. Дәуіт. - Алматы: Жазушы, 1993. - 35 б.

5. Тұрсынов Е.Д. Қазақ ауыз әдебиетін жасаушылардың байырғы өкілдері. - Алматы: Жазушы, 1976. - 158-159 бб.

6. Туретт-Туржи К. Консалтинг / Пер. с франц. под ред. Л.Л. Никитиной. – СПб.: «Нева», 2004. - С. 7.

7. Макивелли Н. Государь. – М., 2006. – 176 с.

8. Беляков Е.Н., Устинкин С.В. Политический консалтинг. – Н. Новгород, 2003. – С. 27.

9. Березкина О.П. Политический консалтинг. – М.: Академия, 2008. – С. 4.

* * *

В данной статье исследуется история возникновения политического консалтинга.

* * *

In given article the history of occurrence of political consulting is investigated.

Б. Исабаев

ОСНОВНЫЕ ПРИНЦИПЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

Информационные потоки пронизывают все сферы жизни человечества и играют все нарастающую роль в условиях глобализации мирового сообщества. Развитие и распространение информационно-коммуникационных технологий, их проникновение практически во все сферы жизнедеятельности, с одной стороны, являются важным фактором мировой интеграции, социального развития и экономического роста, с другой стороны, являясь сильнейшим катализатором информационного обмена, эти технологии несут в себе также множество как явных, так и скрытых угроз: «угроза со стороны СМИ для общественного благополучия, морального здоровья, национальной безопасности, становится в третьем тысячелетии одним из основных вызовов, возникших перед мировым сообществом» [1].

Необычайную значимость в связи с этим приобретают вопросы обеспечения информационной безопасности. Существует мнение, что информационная безопасность в современном постиндустриальном мире, где основным товаром является информация, и именно та или другая информация влияет на принятие государством тактических и стратегических решений, является основой национальной безопасности.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Актуализация проблемы защиты информационного пространства и его влияния на информационную безопасность непосредственно связана с существующими реальными и потенциальными угрозами и вызовами безопасности государства, уровень и масштабы которых в последнее десятилетие существенно возросли и приобрели весьма опасный характер. Исходя из того, что информационная безопасность на рубеже третьего тысячелетия выходит на первое место в системе национальной безопасности, формирование и проведение единой государственной политики в этой сфере приобретает приоритетное значение.

Государство занимает особое место, как среди субъектов государственной информационной политики, так и среди субъектов обеспечения информационной безопасности, поскольку оно обладает уникальными средствами и силами противодействия угрозам в данной сфере. Свою деятельность государство осуществляет совместно с индивидами и обществом, но при этом влияние государства на обеспечение безопасности является определяющим.

Все органы государства в той или иной мере участвуют в деятельности по обеспечению информационной безопасности. Однако их компетенция и предметы ведения в данной сфере деятельности различны, в зависимости от целей и задач, стоящих перед этими органами.

Учитывая, что информационные системы и информационные ресурсы создаются и используются всеми органами государства, в системе обеспечения информационной безопасности особую роль играют те органы государства, которые выполняют руководящие и координирующие роли, от оптимального определения компетенции которых в существенной степени зависит информационная безопасность страны.

Общая структура государственной системы

обеспечения информационной безопасности включает четыре основные властные подсистемы, образующие ветви власти, различающиеся функциями в области обеспечения информационной безопасности и соответственно компетенцией: президент, законодательная, исполнительная и судебная власти. При этом основная тяжесть реализации государственной политики в области обеспечения информационной безопасности ложится на органы исполнительной власти, осуществляющие на основе законодательства административно-государственное управление.

Особенность реализации функции обеспечения информационной безопасности заключается в том, что каждый орган государства осуществляет свою деятельность на базе использования информационной инфраструктуры общества, производит и потребляет информационные ресурсы, имеет определенные отношения с гражданами как представитель собственника государственных информационных ресурсов, должен предпринимать определенные действия по обеспечению сохранности ресурсов и безопасности функционирования информационных и телекоммуникационных систем, сетей связи, систем автоматизации управления.

Фактором, определяющим в целом государственную информационную политику, является существование в информационной сфере источников угроз интересам государства, по мнению ряда авторов, наиболее опасные из которых — неконтролируемое распространение «информационного оружия» и развертывание гонки вооружений в этой области, попытки реализации концепций ведения «информационных войн».

В последнее время военные ведомства разных стран ведут интенсивные разработки в области информационных (информационно-психологических) войн. Сам термин «информационная война» появился в середине 80-х гг. XX в. в работах американских военных теоретиков и начал широко применяться после проведения операции «Буря в пустыне» в 1991 г. В настоящее время в армии США, например, есть специальные информационные войска. В армейском уставе США информационная война определяется так: «Действия, предпринятые для достижения информационного превосходства в интересах национальной стратегии и осуществляемые путем влияния на информационные системы противника при одновременной защите собственной информации и своих информационных сетей» [2].

Многими политическими аналитиками и социальными теоретиками глобальный мир сегодня рассматривается не иначе, как состояние войны цивилизаций, культур, наций, религий, ценностей. Считается, что войны XXI в. будут по преимуществу информационными войнами. Более того, некоторые исследователи считают, что в настоящее время уже идет «третья мировая информационно-психологическая война». А основным средством ведения такой войны являются средства массовой информации.

Границы войны и мира, ценностей и технологий, кооперации и противостояния радикально изменены информационно-коммуникативной революцией. Важнейшими компонентами вооруженных сил становятся информационно-коммуникативные системы, назначение которых – обеспечивать проникновение в сознание потенциального противника за счет размещения в контексте локальных культур определенных ценностных ориентаций и поведенческих моделей.

Информационная война обладает для развязывающей ее стороны целым рядом преимуществ по сравнению с обычной войной, в частности:

- война ведется в «белых перчатках». Агрессора, как правило, невозможно обвинить в применении вооруженных сил;
- эта война практически не регламентирована международным гуманитарным правом;
- ведение информационной войны стоит, как правило, дешевле, чем ведение обычной войны;
- эффект зачастую достигается гораздо больший, чем с помощью обычного оружия;
- развязывание информационной войны гораздо менее опасно для страны-агрессора, чем развязывание традиционной войны.

Отсутствие видимых разрушений, характерных для войн обычных, можно признать главной опасностью информационной войны. Население даже не ощущает, что подвергается воздействию. В результате общество не приводит в действие имеющиеся в его распоряжении защитные механизмы. Применение технологий информационной войны может вызвать нарушение социально-экономических процессов и, в конце концов, привести к гибели государства. При этом народ оказывается деморализованным и неспособным к сопротивлению [3].

В январе 1995 года влиятельной корпорации «РЭНД» было поручено в рамках мероприятий, осуществляемых министерством обороны США, выполнить ряд исследовательских работ в области ведения информационной войны. По мнению специалистов корпорации «РЭНД»,

применение информационного оружия предусматривает решение следующих задач:

- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;
- манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции и даже гражданской войны;
- снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование забастовок, массовых беспорядков и других акций экономического протеста;
- затруднение принятия органами управления важных решений;
- подрыв международного авторитета государства, его сотрудничества с другими странами;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

Приемы ведения информационной и сетевой войны могут применять разного рода террористические, подрывные и экстремистские организации, государства, не способные вести традиционные военные действия против стран, неизмеримо превосходящих их в технологическом уровне развития, наркокартели, преступные транснациональные синдикаты и даже международные финансовые спекулянты и харизматические авантюристы.

В этих условиях само понятие нейтралитета в современном мире становится проблематичным. Угрозы безопасности государства, общества и индивида в эпоху информационно-коммуникативной революции носят по сути всеобъемлющий и перманентный характер. Таким образом, формирование системы эффективной защиты национального информационного пространства становится важнейшей частью обеспечения национальной безопасности Республики Казахстан.

Государство должно иметь гибкую, адаптивную, мобильную и эффективную систему защиты собственного информационного пространства от деморализующих пропагандистских акций и информационно-психологических вторжений, способную быстро реагировать на возникающие угрозы и новые условия деятельности.

Для этого необходимо:

- обеспечить надежную защиту «закрытой» информации от несанкционированного (противоправного) доступа и опубликования;
- организовать постоянный контроль над ситуацией в тех сферах, где могут возникнуть угрозы информационной безопасности;
- вести мониторинг возможностей существующих систем обеспечения информационной безопасности по отражению реальных и потенциальных угроз;
- согласование разрабатываемой нормативно-правовой базы развития информационного пространства и обеспечения информационной безопасности, в первую очередь, в аспектах интегрирования Казахстана в международные телекоммуникационные сети;
- создание собственных технических средств обеспечения информационной безопасности, закупка зарубежных программных, технических и телекоммуникационных средств защиты информации и их использование в стратегически важных областях;
- объединение усилия широкой общественности, профессионалов, ученых и представителей органов власти, делового мира для решения исключительно важной в настоящее время для Республики Казахстан задачи – надежной защиты ее информационных ресурсов.

Вопросам обеспечения информационной безопасности Республики Казахстан посвящается ст. 22 Закона Республики Казахстан «О национальной безопасности Республики Казахстан», в которой записано, что в республике создается и укрепляется национальная система защиты информации, в том числе государственных информационных ресурсов. Обязанностью государственных органов, организаций независимо от форм собственности, должностных лиц и граждан является принятие всех необходимых мер по недопущению:

– информационной зависимости Казахстана;

– информационной экспансии и блокады со стороны других государств;

– информационной изоляции Президента, Парламента, Правительства и сил обеспечения национальной безопасности Республики Казахстан.

Вышеуказанным Законом не допускается

принятие каких бы то ни было решений и совершение действий, противоречащих национальным интересам формирования и бесперебойного функционирования информационного пространства Республики Казахстан и вхождения нашей страны в мировую систему связи и информации. В этой связи пунктом 5 ст. 22 Закона о национальной безопасности запрещается:

– распространение на территории Республики Казахстан печатной продукции, теле – и радиопередач зарубежных СМИ, содержание которых подрывает национальную безопасность;

– разглашение служебной и иной информации, связанной с интересами государства;

– иностранным физическим и юридическим лицам, а также лицам без гражданства, прямо и (или) косвенно владеть, пользоваться, распоряжаться и (или) управлять более 20% пакета акций (долей, паев) юридического лица – представителя СМИ в Республики Казахстан или осуществляющего деятельность в этой сфере.

Уполномоченным государственным органом по представлению Генерального Прокурора Республики Казахстан, согласно пункту 6 ст. 22 вышеуказанного Закона, приостанавливается деятельность СМИ, подрывающих национальную безопасность.

В связи с вышеизложенным важно отметить, что в соответствии со ст. 17 Закона Республики Казахстан «О государственных секретах» не подлежат засекречиванию сведения о состоянии демографии, образования, культуры, о фактах нарушения прав и свобод граждан; о фактах нарушения законности государственными органами и организациями, их должностными лицами, о массовых репрессиях по политическим, социальным и другим мотивам, в том числе находящимся в архивах, за исключением сведений в области разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, относимых к государственным секретам Республики Казахстан.

Как и всякая политика, политика в области информационной безопасности основывается на определенных принципах:

1) соблюдение Конституции и законодательства РК, а также общепризнанных принципов и норм международного права;

2) открытость в реализации функций республиканских органов государственной власти, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РК;

3) правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;

4) приоритетное развитие отечественных современных информационных и телекоммуникационных технологий.

Интересы человека и гражданина в информационной сфере заключаются в реализации их прав на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов граждан в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении Казахстан.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры Республики Казахстан, для реализации прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности Казахстан, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества [4].

Таким образом, целью информационной безопасности Республики Казахстан является защита национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов граждан, общества и государства.

---

1. Чемякин Ю.В. Политические коммуникации и информационная безопасность общества. Учебное пособие. – Екатеринбург, 2008. – С. 6.

2. См.: Онучко М.Ю. Информационная война: теория и практика// СМИ в системе политических институтов: теория и практика: Материалы международной научно-теоретической конференции. - Астана: ЕНУ им. Л.Н.Гумилева, 2010. – С. 179-182.; Чемякин Ю.В. Политические коммуникации и информационная безопасность общества. Учебное пособие. – Екатеринбург, 2008. – С. 25.

3. Стрельцов А. А. Актуальные проблемы обеспечения информационной безопасности // Информационно-аналитический журнал «Факт». 2003. № 11 // http://www.fact.ru/www/arhiv11s7.htm.

4. См.: Уранхаев Н.Т. Внедрение новых информационных технологий и развитие коммуникационного обеспечения в контексте обеспечения национальной безопасности Казахстана// Саяси институттар жүйесіндегі БАҚ: теория және практика: Халықаралық ғылыми-теориялық