**ИВАНЕНКО С.В**

*заместитель начальника кафедры защиты информации Военно-инженерного института радиоэлектроники и связи МО РК, города Алматы*

**ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА КАК ЭЛЕМЕНТ СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ**

В данной статье рассматривается новая роль информации в современном политическом процессе. Автор выявляет особенности и специфику информационного оружия, факторы распространения политического экстремизма в его информационной части, указывает на своеобразие развития информационного общества, приводит рекомендации по оптимизации государственной информационной политики.

***Ключевые слова:*** информация, безопасность, политика, экстремизм, государство.

Информация в настоящее время является одним из наиболее важных ресурсов в системе государственного управления. Невозможно переоценить значение информации и в бизнесе — обладание ею создает состояния ее владельцам, а недостаток информации или ее неправильная интерпретация разрушает крупные финансовые корпорации [1, с. 39]. Информация формирует систему союзов и блоков государств, способствует свержению правительств, влияет на политическую жизнь миллиардов людей во всем мире. Информационное оружие пытаются использовать в своих интересах как авторитарные, так и либеральные правительства, однако информационные потоки все же более способствуют демократизации политических систем. Как отмечает профессор И. Л. Морозов, авторитарному режиму бесперспективно выстраивать государственную информационную политику методом закрытия для своих граждан доступа к независимым источникам информации — при современных технических параметрах нашей цивилизации это просто невозможно [2, p. 620]. Огромное значение развитию информационной сферы уделяется сегодня на государственном уровне. С одной стороны, в современном информационном пространстве не представляется возможным принятие эффективных решений без системы анализа и оценки данных, изучения текущих тенденций, моделирования вариантов развития событий. С другой стороны, грамотная реализация государственной информационной политики обеспечивает поддержку принимаемым политическим и экономическим решениям, формирует общественное мнение по тем или иным вопросам, предотвращает и предупреждает развитие экстремистских движений.

Именно недооценка значения качественной информационной работы с населением, неспособность донести до сознания граждан цель и стратегию государственной политики, сыграли заметную роль в дестабилизации политической ситуации на Украине в 2013 году и привели к падению режима В. Януковича [3, с. 119–120]. Государственная информационная политика является неотъемлемой категорией внешней и внутренней политики страны. Успехи или неудачи информационной политики воздействуют на все сферы жизни общества и государства. На фоне всевозрастающей интенсивности развития информационной инфраструктуры и интеграции в мировое информационное пространство, с каждым днем эффективность функционирования политических и экономических институтов социума все больше зависит от качества информационной среды [4, c. 300].

Сегодня информационная инфраструктура, информационные ресурсы стали ареной межгосударственной борьбы за мировое лидерство, достижение противоборствующими странами определенных стратегических и тактических политических целей. Сложно представить возможность реализации государственных функций без четко отлаженной государственной информационной политики, в рамках которой заложены основы для решения таких задач, как формирование единого информационного пространства России и ее вхождение в мировое информационное пространство, обеспечение информационной безопасности личности, общества и государства, формирование демократически ориентированного массового сознания, становление отрасли информационных услуг, расширение правового поля регулирования общественных отношений, в том числе связанных с получением, распространением и использованием информации. В рамках обеспечения национальной безопасности России в нашей стране проводится государственная политика реализации комплекса мер по информационной безопасности, что определяет основные направления деятельности федеральных и региональных органов государственной власти, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере [5].

Важнейшей задачей государства в области информационной безопасности является обеспечение гарантий конституционных прав и свобод человека и гражданина на доступ к информации и обеспечение полноценных возможностей для деятельности в информационной сфере. В условиях развития информационного общества в нашей стране становится все более очевидным, что обеспечить информационную безопасность только путем деятельности органов государственной власти, правоохранительных структур, развития нормативно-правовой базы достаточно затруднительно, необходимо широкое сотрудничество с общественными движениями и группами, представляющими активную часть гражданского общества [6, с. 49–50]. По мнению российских специалистов в области информационной безопасности, практически любой программный продукт, предназначенный для обеспечения функционирования ЭВМ, в силу специфики своего производства имеет уязвимости, позволяющие осуществлять внешнее деструктивное воздействие. Развитие информационно-коммуникационных технологий несет не только новые возможности, но и огромное количество угроз, в первую очередь угроз информационной безопасности.

В условиях современного развития электронных коммуникаций и всевозрастающего потока данных, обеспечить защиту информации становится все сложнее. Вслед за развитием технологий, повышающих информационную и идеологическую уязвимость политических систем, государство и транснациональные структуры всеми доступными юридическими и аппаратно-программными методами стараются усилить контроль за этими технологиями. В итоге выстраивается своеобразная система управления сознанием и поведением как конкретного индивида, так и целых страт и наций. Компьютерные технологии открывают огромные возможности контроля над обществом. На данный момент нет средства, способного гарантированно обеспечить конфиденциальность общения в интернете. Интернет из свободной зоны общения сегодня превратился в средство воздействия на сознание пользователя со стороны политических и бизнес структур. Пользователь интернета психологически уверен в собственном свободном выборе информации и невозможности им манипулировать, в следствии чего значительно снижается порог рационально-критического восприятия. Именно интернет стал звеном, соединившим информационную и психологическую войны. В зарубежной политической науке популярна теория, согласно которой в современном мире, когда ядерное оружие обессмыслило открытые военные конфликты между великими державами, главной чертой геополитической борьбы станет перенос акцента в сферу информационного противоборства, а достижение «информационного господства» станет обязательным условием победы над противником. Более того, высказываются мнения, что в третьем тысячелетии лидерство в мире будет определяться не столько экономическим потенциалом государства, сколько его способностью контролировать информационные процессы, превращать информацию в оружие [7, c. 195–201].

Информационное оружие — это совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию, ограничивать или прекращать доступ к ней законных пользователей, нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства. Информационное оружие способно управляемо менять политическое сознание людей, заставляя их неадекватно воспринимать реальность, жить в мире иллюзий и совершать гибельные для себя поступки, приводящие к разрушению политических систем и государств [8, с. 58–72]. В статье российского политолога И. Л. Морозова выделяются нижеследующие виды информационно-психологического оружия (см. Табл. 1). Таблица 1 Виды информационного оружия по классификации И. Л. Морозова [9, c.140] Стратегия Системы дистанционного искажения или уничтожения информации. Системы хищения информации. Системы комплексного воздействия на психику пользователей. Вид оружия Компьютерные вирусы общего и специального назначения, адаптированные к работе в конкретных электронных компьютерных сетях по определенным протоколам (программы, проникающие извне и разрушающие систему) Логические бомбы — недокументированный аппаратный набор (микросхема, чип) тайно внедряемый в компьютер на этапе заводской сборки, который при активации парализует работы компьютера.

Электронные шпионы общего и специального назначения, адаптированные к работе в конкретных электронных компьютерных сетях по определенным протоколам (программы, проникающие извне и производящие незаметный для пользователя сбор служебной системой и непосредственно личной информации). Мультимедийные сайты в виде информационно-развлекательных или аналитических страниц с «горячей» и «сенсационной» и иной информацией, составленных с учетом особенностей восприятия человека и психологии виртуальных коммуникаций, что позволяет оказывать глубинное, иногда на уровне подсознания, воздействие на пользователя. Один из ведущих американских специалистов в области информационного противоборства, профессор университета Национальной обороны Мартин Либицки выделил семь основных форм информационного противоборства: борьба с системами управления, информационно-разведывательная, электронная, психологическая, хакерская, кибернетическая и экономическая (см. Табл. 2). Таблица 2 Классификация форм информационного противоборства М. Либицки Формы информационного противоборства Описание Борьба с системами управления Предусматривает их физическое уничтожение и отсечение командных структур противника. Такая борьба может достигаться непосредственным уничтожением управляющих структур и разрушением коммуникаций, связывающих системы управления с подчиненными подразделениями.

Информационно-разведывательные операции Предполагают оперативный сбор, обработку и доведение до конечного пользователя максимально полной информации о противнике в режиме реального или близком к реальному времени. Создание многоуровневой системы сбора данных позволяет получать максимально полную картину ситуации в районе боевых действий и облегчает распределение информации между пользователями. Электронная борьба Представляет собой снижение информационных возможностей противника. В соответствии с этим она подразделяется на радиоэлектронную (в частности, путем постановки активных и пассивных помех), которая считается главным направлением, криптографическую (искажение и ликвидация собственно информации) и борьбу с коммуникационными системами противника. Психологические операции Представляют собой комплекс мероприятий по распространению специально подготовленной информации для воздействия на эмоциональное состояние, мотивацию, аргументацию действий, принимаемые решения и поведение оппонентов в благоприятном для США и их союзников направлении. По своим масштабам они могут быть стратегическими, оперативными и тактическими и включают в себя четыре основных компонента: подрыв гражданского духа, деморализация вооруженных сил, дезориентация высшего политического и военного руководства и война культур.

Основным инструментарием ведения таких операций являются национальные и транснациональные средства массовой информации, а также глобальные информационно-коммуникационные сети, способные влиять на мировоззрение, политические взгляды, правосознание, менталитет, духовные идеалы и ценностные установки как отдельной личности, так и общества в целом. Хакерская борьба Представляет собой действия с применением программных средств (программно-математическое воздействие на информационно-коммуникационные сети), направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационно-коммуникационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компьютерных систем. Кибернетическая борьба Охватывает полный комплекс проблем и аспектов (организационные, доктринальные, стратегические, тактические, технические) ведения информационных операций и в настоящее время становится все более актуальной именно в военной сфере. При этом понятие кибернетической борьбы относится скорее к организационной форме информационного противоборства, чем собственно к борьбе с информационной инфраструктурой противника. Экономическая борьба Представляет собой комплекс методов и средств информационного воздействия в экономической сфере. На сегодняшний день абсолютным большинством экспертов признается тот факт, что владение эффективным информационным оружием и средствами защиты становится одним из главных условий обеспечения национальной безопасности государства. Информационные угрозы приобретают особое значение в условиях модификации идеологий — от рациональных доктрин к иррациональным религиозным идеологемам экстремистского характера. Как отмечает российский политолог: «Политический экстремизм теперь занимает весьма своеобразную нишу, он развивается как стихийный протест против глобализации со стороны социальных страт весьма различных по уровню культурного и экономического развития государств, объединенных общей чертой включенности правящих элит данных государств в мировую глобальную систему по ее правилам» [10, c. 149].

Подводя итог, выделим новые компоненты в системе государственной информационной политики, необходимые к широкому внедрению: формирование компетенции информационной безопасности как обязательного элемента подготовки государственных и муниципальных служащих в системе высшего образования и повышения квалификации введение в системе среднего школьного образования учебной дисциплины, позволяющей сформировать представление об основах феномена информационно-политической безопасности; расширение взаимодействия государственных институтов с гражданским обществом, социальными активистами;повышение прозрачности в работе государственных учреждений; ужесточение административного и уголовного наказания за правонарушения в информационной сфере.

**Литература:**

1. Бельских И. Е. Инновации и альтернативы в современной экономике // Экономика: теория и практика. 2015. № 1 (37). С. 39–43.
2. Morozov I. L. Information and political security of the democratic state — world experience and Russia // Life Science Journal. 2014. Т. 11. № 11. S. 620.
3. Матвиенко Е. А., Васильчук Е. О., Морозов И. Л. Особенности институционально-правового обеспечения противодействия экстремизму в Украине // Вестник Воронежского института МВД России. 2013. № 3. С. 117–122.
4. Бельских И. Е. Коммуникации в промышленном бизнесе: в поисках инновационной национальной стратегии / В сборнике: Информационная экономика: институциональные проблемы Материалы Девятых Друкеровских чтений. Под ред. Р. М. Нижегородцева. Москва, 2009. С. 299–307.
5. Справочно-правовая система «Гарант» — Режим доступа: http://www.garant.ru, свободный. — Загл. с экрана. Афанасьева О. В. «Электронное государство» в развитых странах: опыт институциональной трансформации // Мировая экономика и международные отношения. 2013. № 11. — С. 44–52.
6. Най Дж. Будущее власти. М.: АСТ, 2014.
7. Панарин И. Информационная война и геополитика. М.: Поколение, 2006.
8. Морозов И. Л. Информационная безопасность политической системы // Полис. Политические исследования. 2002. № 5. С. 134–145.
9. Морозов И. Л. Экстремистские политические идеологии в условиях глобализации — от концептуальной рациональности к религиозному экстремизму //
10. Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. 2009. № 1. С. 148–155.