Секция «Государственное и муниципальное управление»

Роль информационной безопасности в политике государства.

Ведерникова Мария Игоревна
Студент
Московский государственный университет имени М.В. Ломоносова, Факультет политологии, Москва, Россия
E-mail: o.mishin2015@yandex.ru

Внимание к вопросам международной и национальной безопасности в новых условиях связано с информационными отношениями, обеспечением безопасности государственных информационных ресурсов, систем и средств коммуникации, а достоверность и целостность информации становится важным аспектом решения и преодоления многих глобальных и внутригосударственных проблем.

Необходимо отметить, что расширяется спектр субъектов политических отношений, чувствительных к вопросам информационной безопасности, который включает в себя государственную власть, национальную безопасность, политические структуры и объединения, средства массовой информации, социальные институты и другое [1].

При таких преимуществах информатизации, как оптимизация политических и экономических процессов, формирование более совершенных принципов взаимодействия власти и общества, существует и её обратная сторона, включающая в себя появление новых угроз, связанных с распространением и развитием информационных технологий, а также негативные и преступные последствия их использования, что определяет проблематику информационной безопасности в политике как особенно актуальную.

Защита информационной безопасности государства имеет прямое отношение к вопросам укрепления суверенитета и протекания внутригосударственных политических процессов[2].

«Арабская весна» как пример ведения информационной войны внутри страны и за её пределами.

Одним из основных видов оружия информационных войн на сегодняшний день являются социальные сети. Как известно, "Арабская весна"началась с информационных атак через социальные сети Facebook и Twitter. Социальные сети, имея огромное количество пользователей, стали мощным оружием. В XXI веке революция делается путем рассылки сообщений через интернет.

Открытое военное противостояние с государствами, обладающими ядерным оружием, чрезвычайно опасно для всех, без исключения, участников конфликта. В настоящее время информационные технологии и их воздействие на человека по эффективности превзошли многие материальные ресурсы.

Наиболее важные аспекты информационной безопасности - это политическая расстановка сил, наличие реальных и потенциальных внешних и внутренних угроз, уровень развития внутренних коммуникаций в стране, внутриполитическая обстановка в государстве, наличие или отсутствие диалога власти и общества.

Многие аспекты информационной безопасности содержат гуманитарное (духовное, нравственное), а зачастую – и патриотическое начало, которое является важнейшей частью национальной безопасности каждого государства[4].

Китай, как правило, с большим отрывом занимает первое место в списке стран, осуществляющих хакерские атаки на сайты правительственных организаций других государств и акты шпионажа в сети Интернет.

Электронные СМИ, по мнению Тауфика Окаша, египетского журналиста, являются сегодня главным полем битвы и одновременно основным оружием в войнах нового поколения. В эпоху информационных технологий, главные сражения идут на информационном поле.

Войны в современном мире - это войны, в которых используются определенные методики воздействия на общество с целью его раздробления на отдельные группы и последующего развития конфликтной ситуации между этими группами с помощью молниеносного распространения информации, выгодной противнику, в глобальной сети. Могут быть задействованы самые разные факторы, на основе которых разжигается вражда: религия, расовая неприязнь, имущественное неравенство.

Экономические методы, которые обеспечивают информационную безопасность, состоят из: подготовки программ по обеспечению информационной безопасности и нахождение источника финансирования данных программ, совершенствование системы финансирования работ, направленных на реализацию правовых, организационных и технических способов защиты важной информации, создание системы страхования информационных рисков физических лиц и бизнеса[3].

К правовым методам обеспечения информационной безопасности относится процесс разработки законодательной базы и правовых актов, определяющих отношения в информационной сфере, и официальных методических документов по вопросам обеспечения информационной безопасности.

Основными действиями, направленными на реализацию государственной политики обеспечения информационной безопасности, являются: разработка и принятие законодательных актов, направленных на регулирование отношений в информационном секторе, и, кроме того, разработка концепции правового обеспечения информационной безопасности государства, подготовка и внедрение механизмов повышения эффективности государственного контроля за деятельностью СМИ, в том числе, и электронных, осуществление целенаправленной государственной информационной политики, принятие и реализация программ на государственном уровне, направленных на повышение правовой культуры и компьютерной и грамотности населения, развитие единого информационного пространства страны.

Литература

1. С.И. Грачев, О.Н. Герасин, А.О. Колобов, М.И. Ливерко. Проблемные аспекты в информационной политике и информационной безопасности России // Вестник Нижегородского университета им. Н.И. Лобачевского, 2012, № 1 (1), с. 290–292.

2. Иншаков М.В. Человек и общество как информационные системы. Информационно-культурный подход к анализу информационной безопасности общества // Современные гуманитарные знания № 3, М., 2007.

3. А. В. Поляков. Проблематика информационной безопасности в политических научных направлениях // "Технологии техносферной безопасности". Выпуск № 3 (37) 2011.

4. Доктрина информационной безопасности Российской Федерации.

Слова благодарности

Выражаю благодарность своим научным руководителям.