Секция «6. Экономическая и информационная безопасность: проблемы»

Политический аспект информационной безопасности.

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

Роль информационной безопасности в политике государства. 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.

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.

Вопросы отношений понятия информационной безопасности и государственной власти, включающие в себя изучение проблем информационной безопасности в сфере государственных органов и политической власти.

Обеспечение информационной безопасности государства в избирательных кампаниях и разработке федеральных целевых программ обеспечения информационной безопасности, разработка политических программ и нормативных документов, регулирующих информационную безопасность государства и совершенствование нормативно-правовой базы информационной сферы, организация функционирования систем обеспечения региональной безопасности и совершенствования существующих нормативных документов в области информационной безопасности, включая "Доктрину информационной безопасности Российской Федерации"и "Концепцию национальной безопасности Российской Федерации".

Сотрудничество федеральной и региональной властей по противодействию угрозам в информационной сфере.

Проблематика информационной безопасности регионов, включающая в себя влияние административно-территориального деления государства на информационную сферу, воздействие регионализации на национальную безопасность, специфику проявления

угроз информационного характера на региональном уровне и противодействие угрозам региональной информационной безопасности.

Развитие глобальных и внутригосударственных процессов, имеющих ярко выраженный информационный характер.

Экономическое и финансовое обеспечение информационной безопасности. Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются: разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации, разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики, принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России и т.д.

Внешнее влияние на информационную безопасность. Вмешательство во внутренние дела государства с целью поглощения информационных ресурсов, бессистемное распространение на территории государства глобальных электронных коммуникаций, проблематику использования информации как средства сохранения и приумножения власти.

Основные мероприятия по обеспечению информационной безопасности Российской Федерации в сфере внешней политики.

Разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса.

Разработка и реализация комплекса мер по усилению информационной безопасности и информационной инфраструктуры федеральных органов исполнительной власти.

Создание за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней и внутренней политике.

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности - неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информаци-

онной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются: деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем, вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств,нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности, привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Информационная политика США, направленная на обеспечение информационного превосходства путём навязывания информации, побуждающей высшее военно-политическое руководство других стран принимать выгодные для США решения.

Ключевыми элементами в деле достижения целей национальной информационной стратегии являются управление восприятием целевой аудитории и формирование её «общественного мнения» путем манипулирования информацией.

Наиболее важные аспекты информационной безопасности - это политическая обстановка в мире, наличие потенциальных внешних и внутренних угроз, состояние и уровень информационно-коммуникационного развития страны, внутриполитическая обстановка в государстве.

Некоторые аспекты информационной безопасности несут гуманитарное (духовное, нравственное), а в конечном результате – патриотическое начало, что является составной частью национальной безопасности любого государства.

В отчетах и докладах органов различных государств Китай, как правило, с большим отрывом занимает первое место в списке стран, осуществляющих хакерские атаки и акты кибершпионажа.

Основным документом, в котором подчеркивается значимая роль информационной безопасности в жизни китайского общества, является Всеобъемлющая концепция национальной безопасности Китая.

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

Войны четвёртого поколения - 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. В качестве бикфордова шнура могут быть задействованы самые разные факторы: религия, расовая неприязнь, имущественное неравенство и т.д.

Методики воздействия на аудиторию. Часть СМИ одновременно говорит об одном и том же событии, по сути, возможно, малозначимом, но выигрышном для сторонников той или иной общественной тенденции. Аудиторию подталкивают к определенному выводу, создаётся определенное общественное настроение, облегчающее проведение тех или иных уличных акций.

«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.

Открытая военная конфронтация с государствами, обладающими ядерным оружием, чрезвычайно опасна для всех участников конфликта. В настоящее время информационные технологии и их воздействие на человека по эффективности превзошли многие материальные ресурсы.

Обеспечение информационной безопасности гражданского общества. Роль средств массовой информации, которые могут быть использованы в целях манипуляции общественным мнением и проведения провокаций, в связи с чем политические науки сталкиваются с проблемой информационно-психологической безопасности личности.

Меры по предотвращению деструктивного воздействия на массовое сознание.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина 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.

Информационная безопасность – это сложное системное, многоуровневое явление, на состояние и перспективы развития которого оказывают непосредственное воздействие внешние и внутренние факторы.

Внедрение в ментальность граждан жестокости, идеи о допустимости применения насилия, «привыкание» к нему создают благоприятную почву для распространения в стране экстремизма и терроризма. Сформировавшаяся в настоящее время индустрия СМИ достаточно свободно пропагандирует культ насилия и жестокости.

Литература

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

2. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты, М.: Изд-во "РАГС 1998.

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

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

5. Доктрина информационной безопасности Российской Федерации.

Слова благодарности

Выражаю благодарность своему научному руководителю А. П. Кабаченко за помощь в написании работы.