БОРЩЕНКО Виктор Владимирович – *преподаватель факультета профессионального образования и довузовской подготовки Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (199178, Россия, г. Санкт-Петербург, В.О., Средний пр-кт, 57/43; boss-victor@yandex.ru)*

ОСОБЕННОСТИ МЕХАНИЗМА ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПОЛИТИЧЕСКИМ УГРОЗАМ В ИНТЕРНЕТЕ

Аннотация. *В статье рассматриваются организационные, технические и правовые особенности построения механизма противодействия информационно-политическим угрозам в интернет-пространстве, связанные с определением и разработкой цели и задач механизма; субъектов и объектов противодействия; информационно-политических угроз, их источников и сферы применения; принципов эффективного функционирования механизма; алгоритма противодействия; мониторинга информационного пространства; критериев риска; ресурсов, мер и инструментов противодействия.*
Ключевые слова: *механизм противодействия, информационно-политические угрозы, Интернет, элементы механизма противодействия, принципы противодействия*

Введение

Под механизмом противодействия угрозам различного типа в общем виде обычно понимают структурно взаимосвязанную систему организационных, правовых, экономических и других мер, направленных на устранение ущерба какой-либо системе и профилактику его появления, осуществляемых органами внутренней безопасности. Он может включать в себя такие структурные элементы, как цель и задачи; субъекты; объекты воздействия; угрозы и источники угроз; принципы эффективного функционирования механизма; сферы угроз возникновения негативных явлений; алгоритм противодействия негативным явлениям в совокупности процедур и структурных элементов; мониторинг негативных явлений и координация противодействия; критерии риска негативных явлений; ресурсы, меры и инструменты противодействия[1]. Применение общей схемы механизма противодействия в конкретных областях практической деятельности предполагает адаптацию выполнения его основных мероприятий к характеру угроз, особенностям сферы их существования, особенностям объектов воздействия и т.п. [Епифанов, Симон 2013].

Основная часть

Основные элементы механизма противодействия информационно-политическим угрозам в Интернете, входящие в его общую схему, могут быть охарактеризованы следующим образом.

Основной целью противодействия информационно-политическим угрозам является создание благоприятной информационной обстановки для функционирования политической структуры страны в условиях возрастающих манипуляционных возможностей Интернета и других средств электронной коммуникации путем формирования и всестороннего обеспечения функционирования системы предупреждения, минимизации, локализации и ликвидации этих угроз, исходя из актуальных и перспективных потребностей обеспечения безопасности личности, общества и государства.

[1] Структура и ключевые элементы механизма противодействия теневым экономическим явлениям. Доступ: https://cyberpedia.su/5x796f.html (проверено 12.04.2018).

Исходя из поставленной цели, к числу основных задач противодействия информационно-политическим угрозам следует отнести:

– прогнозирование, выявление и оценку источников и характера информационно-политических угроз, основных субъектов информационно-политического воздействия, информационно-критических элементов политической системы, функционирование информационного компонента которых приводит к потере государственного или политического управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок;

– сбор информации об используемых и перспективных информационных технологиях органов информационного противодействия применительно к политической сфере деятельности объекта воздействия;

– защиту элементов политической структуры России, а также индивидуального, группового и массового сознания ее населения от применения противостоящей стороной информационно-политических средств и методов воздействия;

– защиту информационной инфраструктуры России в целом и информационной инфраструктуры политической системы России от применения противостоящей стороной информационно-технических средств и методов воздействия;

– создание и разработку стратегии проведения контринформационных операций в информационно-политической сфере в различных условиях внутриполитической и внешнеполитической обстановки;

– разработку нормативно-правовой базы информационно-политической безопасности, проведение специальных операций в информационной, в т.ч. информационно-политической, сферах, применение информационного оружия и методов информационной войны [Борщенко, Косов 2017].

Решение этих задач на начальном этапе предполагает формирование перечня субъектов информационно-политических угроз. В связи с тем, что политическая деятельность представляет совокупность сознательных, целенаправленных, волевых действий социальных субъектов по реализации своих политических интересов, направленных в первую очередь на завоевание власти или осуществление влияния на нее [Круглова 2009], к числу субъектов информационно-политических угроз следует отнести представителей государства, государственных органов и органов местного самоуправления, политических партий и общественных объединений, иных институтов, а также членов гражданского общества. Все перечисленные субъекты способны эффективно решать свои задачи, ведя активную деятельность в информационном пространстве. Многие современные политики все чаще обращают внимание на свое присутствие в различных социальных сетях и интернет-ресурсах: *Instagram, YouTube* и блогах. Так, например, официальные аккаунты в *Instagram* имеют Д. Медведев, М. Захарова, Р. Кадыров, С. Аксенов, А. Меркель, С. Берлускони и многие другие[1]. 68% глав государств и правительств из 193 стран – членов ООН имеют свои собственные аккаунты в соцсетях[2].

Объектами рассматриваемого механизма противодействия являются информационно-политические угрозы, под которыми предлагается понимать потен-

[1] Политики в Instagram. Доступ: http://actualcomment.ru/politiki-v-instagram-1802081913.html (проверено 15.04.2018).

[2] Политики в социальных сетях: досье. Доступ: http://tass.ru/info/1442493 (проверено 15.04.2018).

циальную возможность (явно или неявно выраженную) нанесения ущерба интересам граждан, государства и постиндустриального общества в целом в политической сфере при помощи информации, циркулирующей в элементах политической структуры – политических, государственных организациях, институтах и учреждениях, а также в едином информационном пространстве.

Источниками информационно-политических угроз являются внешние и внутренние субъекты (государственные, военные, политические, общественные и т.п. организации и отдельные представители иностранных государств), действия которых могут привести к нарушению политической безопасности. К внешним источникам таких угроз следует отнести, например:

– правительство США, планирующее распространить «войну идей» на популярные интернет-сайты, блоги и чаты в русскоязычном сегменте Интернета[1];

– Совет управляющих по вопросам вещания США (*Broadcasting Board of Governors, BBG*, бывшая *USIA*) – орган управления гражданской внешнеполитической пропагандой США, отвечающий за продвижение американских ценностей и контролирующий организации, вещающие на 61 языке в более чем 125 странах, в т.ч. «Голос Америки», «Радио Свободная Европа/Радио Свобода»; «Белые каски» (Сирийская гражданская оборона – организация по защите и спасению мирных жителей), которые особо и не скрывают, что являются фабрикой фейков[2], и др.;

– З. Бжезинского, занимавшего крайне жесткую позицию в отношении Советского Союза и сохранявшего глубокий скептицизм в отношении целей и намерений России, даже когда призывал США интегрировать ее в систему Запада[3];

– Д. Сороса, делающего ставку на НКО в регионах, чтобы ввести в России хаос изнутри[4], и др.

К основным принципам эффективного функционирования механизма противодействия информационно-политическим угрозам следует отнести:

1) принцип оперативности вскрытия мероприятий технологии информационно-политического воздействия, заключающийся в добывании информационных признаков этих мероприятий в сроки, допустимые для принятия эффективных мер противодействия. В основе принципа лежит предвидение возможности применения различных технологий информационно-политического манипулирования. Примером игнорирования этого принципа является беспрепятственный допуск проникновения в социальные сети пранкеровской информации о числе жертв при пожаре в торговом центре «Зимняя вишня» в Кемерове, усилившей массовые волнения в городе[5];

2) принцип упреждающего характера действий, сущность которого заключается в прогнозном обосновании применения той или иной технологии информационно-политического манипулирования, оперативном принятии мер по публичному разоблачению манипуляционных действий и предупреждению о возможных последствиях. Ярким примером эффективного использования этого принципа является своевременное получение достоверной информации о под-

---

[1] Джеймс Глассман: приносит ли война идей результаты. Доступ: https://ria.ru/society/20081031/154201253.html (проверено 15.04.2018).

[2] «Белые каски» даже не заботятся о достоверности: очередной вброс фабрики фейковых новостей. Доступ: https://www.vesti.ru/doc.html?id=3005126&tid=95994 (проверено 15.04.2018).

[3] Бжезинский о России: анализ, выводы и рекомендации. Доступ: https://inosmi.ru/politic/20170609/239543871.html (проверено 15.04.2018).

[4] Какое будущее уготовил для России Джордж Сорос. Доступ: http://kolokolrussia.ru/pyataya-kolonna/kakoe-buduschee-ugotovil-dlya-rossii-djordj-soros#hcq=SBlxUOq (проверено 15.04.2018).

[5] Фейк о 300 жертвах пожара в Кемерово запустил украинский пранкер. Доступ: https://ruposters.ru/news/27-03-2018/zapustil-ukrainskii-pranker (проверено 15.04.2018).

готовке боевиками инсценировки применения правительственными войсками химического оружия против мирного населения в начале 2018 г., готовящейся в Сирии со стороны боевиков провокации с применением химического оружия, открытое заявление об этом начальника Генерального штаба ВС РФ генерала армии В. Герасимова 14 марта 2018 г. на селекторном совещании Вооруженных сил Российской Федерации и предупреждение о том, что «в случае возникновения угрозы жизни нашим военнослужащим Вооруженные силы Российской Федерации примут ответные меры воздействия»[1];

– принцип активности противодействия, заключающийся в настойчивом стремлении выявить в информационном пространстве (в т.ч. и в Интернете) манипулированную информацию путем проявления разумной инициативы, смелости и решительности действий, основанных на правильном понимании информационно-политических угроз и реальных условий информационно-политической обстановки;

– принцип непрерывности противодействия информационно-политическим угрозам, заключающийся в постоянном выявлении манипулированной информации. Современные интернет-технологии позволяют в автоматическом режиме выявлять информационные признаки такой информации. Для этого должны быть разработаны дескрипторы, отражающие сущность текущих и перспективных политических процессов, а также возможные варианты модификации политической информации, циркулирующей в информационно-критических элементах политической структуры;

– принцип объединения усилий государственных органов информационного противоборства, систем внутренней безопасности элементов политической структуры и непосредственно участников политического процесса предполагает их согласованные действия на основе четкого размежевания их компетенции.

Основной сферой информационно-политических угроз является информационное обеспечение действий в области политики, политической жизни общества в пределах распространения непосредственного влияния политиков и политических организаций, воздействия политических идей. В настоящее время эта сфера существенно расширена за счет потенциальных возможностей Интернета по созданию и тиражированию политической информации в рамках персонального контента (блоги, чаты, форумы, сайты) и рассылке ее политическим сторонникам, в адрес политических партий и органов государственной власти; участию в блогах, чатах, форумах и телеконференциях политических партий, некоммерческих организаций (в части политических вопросов), представителей государственной власти, политических лидеров, депутатов; участию в таких политических мероприятиях, как интернет-голосования, референдумы, социологические опросы; выработке политических программ, законодательных инициатив, проектов политических решений и др.; по проведению виртуальных съездов партий и других политических мероприятий; организации своих сторонников для участия в реальных политических действиях (митинги протеста или их поддержка, подача петиций, забастовки, политические акции и т.п.).

Общий алгоритм противодействия информационно-политическим угрозам в Интернете может быть представлен следующей последовательностью действий. На первом этапе должны быть разработаны операционно-временные и информационно-признаковые модели информационно-политических угроз.

[1] Глава российского Генерального штаба Валерий Герасимов дал оценку ситуации в Сирии. Доступ: http://xn----ctbsbaa3aibxhck.ru-an.info/ (проверено 15.04.2018).

Важнейшим элементом этих моделей является априорный словарь информационных признаков, свидетельствующих о модификации (в широком понимании – манипуляции, подмены, хищения и т.п.) информации. На следующем этапе в каждом информационном контенте, появляющемся в Интернете и относящемся к какому-либо направлению политической деятельности, выявляются фрагменты информации, характеризующие сущность политических процессов. Далее эти признаки сравниваются с признаками, находящимися в априорном словаре. При выявлении информационных признаков, соответствующих фактам манипулирования, делается вывод о проведении мероприятия информационно-политического воздействия и формируется прогноз об использовании каких-либо манипуляционных технологий. Это позволяет, во-первых, принять меры по противодействию информационно-политическому воздействию на промежуточных этапах реализации технологий; во-вторых, получить представление о вариантах дальнейших действий манипуляторов и тем самым выработать общую стратегию противодействия соответствующей информационно-политической угрозе.

Важнейшим элементом в реализации предложенного алгоритма является мониторинг информационного пространства с целью выявления информационных признаков информационно-политических угроз. Этот мониторинг должен осуществляться с соблюдением действующего информационного законодательства по доступу к открытой информации, а также в рамках полномочий, представляемых силовым структурам (ФСТЭК, ФСБ, МВД и др.). В качестве основных источников информации могут быть использованы электронные СМИ, поисковые информационные массивы русскоязычных и особенно иноязычных текстов, информация с интернет-сайтов и почтовых серверов (в т.ч. *Instant Messenger*), корпоративные базы данных и электронные архивы документов, а также информация на материальных (нецифровых) носителях и информация, полученная путем опроса экспертов, массового опроса согласно определенным критериям и иные всевозможные источники неструктурированной информации.

Применение любой технологии информационно-политического воздействия на политическую структуру страны порождает определенные риски для информационно-политической и, в целом, национальной безопасности страны. При идентификации такой технологии необходимо проанализировать причины, источники и факторы риска, вскрыть специфику взглядов на ведение информационной войны со стороны как внешних, так и внутренних интересантов, оценить степень информационно-политической угрозы и эффективность различных методов противодействия ей.

Для реализации механизма противодействия информационно-политическим угрозам потребуются определенные ресурсы, меры и инструменты противодействия, и особенно правовые: нормативные правовые предписания, регламентирующие приемы, способы противодействия коррупционным отношениям и юридические технологии, сопряженные с эффективным правовым инструментарием, юридической техникой, толкованием права и формами правореализационной практики, способствующие снижению негативных явлений и порождающих их причин. Необходимость совершенствования правового обеспечения механизма противодействия информационно-политическим угрозам связана с тем, что в настоящее время вопросы свободы слова, непосредственно связанные с распространением информации в Интернете, постоянно являются предметом политических дискуссий. Это и анонимность в Интернете, и закрытость мессенджеров, и ряд других вопросов.

Заключение

Таким образом, рассмотренные особенности механизма противодействия информационно-политическим угрозам предполагают решение ряда новых проблем технического, организационного и правового характера. К основным из них относятся:

– разработка аппаратно-программных средств, обеспечивающих оперативный мониторинг значительных объемов информации, циркулирующей в интернет-пространстве;

– формирование специальных информационных контуров в действующих информационных системах элементов политической структуры, нацеленных на вскрытие информационно-политических угроз;

– совершенствование информационного законодательства России.

Список литературы

Борщенко В.В., Косов Ю.В. 2017. Информационные аспекты теории политической безопасности. – *Управленческое консультирование*. № 12. С. 33-43.

Круглова Г.А. 2009. *Политология:* учебное пособие для студентов высших учебных заведений. Минск: Асар. 304 с.

BORSHCHENKO Victor Vladimirovich, *Lecturer at the Faculty of Vocational Education and Pre-university Tutorial, North-Western Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration (RANEPA) (57/43 Sredniy Ave, V.O., St. Petersburg, Russia, 199178; boss-victor@yandex.ru)*

FEATURES OF THE MECHANISM OF COUNTERING INFORMATION AND POLITICAL THREATS IN THE INTERNET

Abstract. *The article deals with the organizational, technical and legal features of the mechanism of counteraction to information and political threats in the Internet space. They are associated with the definition and development of the purpose and objectives of the mechanism; subjects and objects of counteraction; information and political threats, their sources and scope; principles of effective functioning of the mechanism; counteraction algorithm; monitoring information space; risk criteria; resources, measures and tools of counteraction.*

Keywords: *mechanism of counteraction, information and political threats, Internet, elements of counteraction mechanism, principles of counteraction*