УДК 351.751

© Владимир Викторович Калмыков
доцент, д-р экон. наук, профессор кафедры ГМУ,
Владимирский филиал РАНХиГС

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННЫМ СТРАТЕГИЯМ ИНФОРМАЦИОННЫХ ВОЙН В РАМКАХ НОВОЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *в данной статье рассматриваются вопросы реализации государственной политики обеспечения информационной безопасности в Российской Федерации, проводится анализ современных механизмов обеспечения информационной безопасности, определенных в Доктрине информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»).*

Abstract*: this article discusses the implementation of the state policy of information security in the Russian Federation, the analysis of modern mechanisms of information security defined in the information security Doctrine of the Russian Federation (decree of the President of the Russian Federation from 05.12.2016 No. 646 "About approval of the information security Doctrine of the Russian Federation").*

Ключевые слова: *государственная политика, информационная безопасность, информационные войны, доктрина, механизмы, новое качество управления, глобальное информационное пространство, информационная структура, импортозамещение, стратегия.*

Keywords: *public policy, information security, information warfare doctrine, mechanisms, new quality control, global information space, information structure, Import substitution, strategy.*

В рамках современной концепции «нового качества государственного управления в Российской Федерации» в отечественной научной дискуссии обсуждаются важные и актуальные вопросы. Спектр их достаточно широк. И один из актуальных вопросов дискуссии заключается в том, что новое качество государственного управления базируется на проведении эффективной государственной политики в сфере обеспечения информационной безопасности.

Актуальность темы, раскрытой в данной статье, заключается в необходимости исследования современных методов противодействия разрушительным стратегиям информационных войн, которые ведутся против Российского государства, деструктивно влияют на процессы социально-экономического развития страны, снижают эффективность государственного управления, дестабилизируют общество [1].

В настоящее время очевидным является то, что в мире идет открытая гибридная война, против России она ведется в течение длительного времени, а информационная война является ее важнейшим компонентом. Причем усиливающееся противоборство в глобальном информационном пространстве для некоторых стран является средством достижения определенных геополитических целей.

Развитие средств и технологий информационной войны, ориентированных на целевые группы населения, выдвигает задачу разработки эффективных средств противодействия технологиям манипулирования сознанием и развития методов государственного управления, направленных на защиту информационного пространства страны и безопасности ее граждан [2].

Необходимо отметить, что в Российском государстве идет формирование современной системы противодействия разрушительным информационным стратегиям, однако эффективность данной системы требует коренного изменения государственной политики обеспечения информационной безопасности Российской Федерации и её регионов.

5 декабря 2016 года подписан Указ Президента Российской Федерации об утверждении новой Доктрины информационной безопасности Российской Федерации [2].

Это документ стратегического планирования в сфере обеспечения национальной безопасности, в нем развиваются положения Стратегии национальной безопасности Российской Федерации [1] и других документов стратегического планирования в указанной сфере, в том числе и Военной доктрины [3].

Необходимость принятия новой Доктрины информационной безопасности определяется задачами повышения эффективности государственного управления, изменения его качества. Приоритеты российской государственной политики в сфере обеспечения информационной безопасности соответствуют мировым тенденциям развития информационных технологий. Выделим некоторые из них:

- возрастающее противоборство в глобальном информационном пространстве;
- усиление угроз безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;
- усиление угроз использования информационных и коммуникационных технологий в экстремистской деятельности и ее крайней форме - терроризме;
- формирование механизмов мпортозамещения современных IT-технологий в условиях санкционного давления на российскую экономику;
- снижение критической зависимости отечественной экономики от зарубежных технологий [2].

Необходимо отметить, что, несмотря на системную работу органов государственного управления в сфере предотвращения угроз национальной безопасности, многие проблемы в сфере информационной безопасности не решены.

Во-первых, несмотря на постоянный рост уровня развития отечественных информационных технологий, он недостаточен и пока не достиг уровня минимально достаточных показателей.

Во-вторых, все большую опасность приобретают угрозы компьютерных атак на объекты критической информационной инфраструктуры, в том числе и на объекты системы государственного и муниципального управления.

В-третьих, в условиях обостряющейся конкурентной борьбы и непростой геополитической обстановки наличие зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности становится недопустимым. И, следовательно, проблема импортозамещения информационных технологий становится одной из важнейших.

В последнее время, в рамках беспрецедентно раздуваемого скандала в американской прессе, связанного якобы с «вмешательством России в президентские выборы в США», широкой общественности стало известно множество фактов, подтверждающих наличие уязвимостей в программном и программно-аппаратном обеспечении, как за рубежом, так и в Российской Федерации, в том числе и в средствах защиты информации, которые используется органами государственного управления. Эти факты подтверждают, что использование современных технологий в информационных провокациях может нести реальную угрозу государственной и общественной безопасности страны. *Важнейшим направлением государственной политики в сфере обеспечения информационной безопасности является защита критической информационной*

инфраструктуры РФ, что связано с непрерывно возрастающим количеством угроз информационной безопасности критически важных объектов страны. Именно на необходимости обеспечения устойчивого и бесперебойного функционирования критической информационной инфраструктуры государства сделан акцент в новой *Доктрине информационной безопасности Российской Федерации* [2].

Не случайно в день подписания новой Доктрины на рассмотрение Государственной Думы был вынесен законопроект, вводящий уголовную ответственность до 10 лет лишения свободы за создание программ для кибератак на инфраструктуру Российской Федерации [6], а также законопроект о безопасности критической информационной инфраструктуры Российской Федерации [7].

В этих условиях разработка и применение отечественных информационных технологий, удовлетворяющих требованиям информационной безопасности, становятся одной из первостепенных задач, а ликвидация зависимости от иностранных информационных технологий провозглашается частью стратегии информационной безопасности Российской Федерации.

Среди новых задач государственной политики обеспечения информационной безопасности, возложенных на государственные органы, необходимо выделить меры государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности.

А в перспективе, по мнению экспертов, государство должно предложить эффективные меры поддержки компаний-интеграторов в сфере информационной безопасности.

Создание благоприятных условий для осуществления деятельности на территории Российской Федерации российских ИТ-компаний определено основным направлением развития экономической сферы системы информационной безопасности [2]. Эти меры позволят увеличить долю продукции отрасли информационных технологий в валовом внутреннем продукте и в структуре экспорта страны.

Актуальным направлением государственной политики является формирование системы управления информационной безопасностью РФ, которая, по нашему мнению, должна включать:

- укрепление вертикали управления информационной безопасностью;

- усиление взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам и др.

Сегодня в Российской Федерации созданы и начали работать новые институты обеспечения информационной безопасности. Особое внимание государство направляет на создание и организацию эффективной деятельности ГосСОПК (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак), организацию деятельности Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (*FinCERT), АПК «Безопасный город»* (аппаратно-программный комплекс), а также на создание системы распределенных ситуационных центров [5].

В соответствии с новой Доктриной информационной безопасности одним из аспектов защиты частной жизни также должно стать повышение защищенности информационных систем и других объектов информационной инфраструктуры, задействованных в обработке персональных данных граждан.

Многие годы Россия неизменно декларировала свою приверженность идеям международного сотрудничества в сфере информационной безопасности. К сожалению, данные идеи не были должным образом поддержаны другими государствами.

В этих условиях возрастает необходимость самостоятельно защищать национальные интересы в сфере информационных технологий и информационной безопасности и потребность в превентивных мерах. К таким мерам относится развитие национальной системы управления российским сегментом сети «Интернет».

И еще на одном аспекте данного вопроса необходимо остановиться - развитие кадрового потенциала.

По оценке Правительства Российской Федерации, для обеспечения информационной безопасности государства, общества и личности в настоящее время необходимо подготовить миллион специалистов высшей категории в сфере информационных технологий. Создание рабочих мест для выпускников образовательных учреждений, создание условий для их подготовки, развитие практики сотрудничества учебных заведений и профильных предприятий, в рамках которого создаются базовые кафедры от предприятий, формирование условий трудоустройства - это важнейшие инструменты формирования новой генерации современных управленцев, которые будут обеспечивать информационную безопасность страны в обозримом будущем.

Список литературы

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собр. законодательства Рос. Федерации. – 2016. – № 1, ч. II, ст. 212.

2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собр. законодательства Рос. Федерации. – 2016. – № 50, ст. 7074.

3. Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976) // Рос. газ. – 2014. – № 298.

4. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 1 декабря 2016 г. // Парламентская газета. – 2016. – № 45.

5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) [Электронный ресурс]. URL: http://www.tadviser.ru/index.php (дата обращения: 09.06.2017).

6. Замахина Т. Госдума рассмотрит законопроект об уголовной ответственности за кибератаки на Российскую Федерацию» // Рос. газ. – 2017. – 11 января.

7. Проект Федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации (ред., внесенная в ГД ФС РФ, текст по состоянию на 06.12.2016) [Электронный ресурс]. URL: http://asozd.duma.gov.ru/.