Секция «Международная безопасность»

Деятельность России в сфере обеспечения международной информационной безопасности в начале XXI века

Касацкий Лев Константинович

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Москва, Россия

E-mail: levalhimik111@gmail.com

Концепция международной информационной безопасности предполагает наличие состояния защищенности мировой информационной системы от совокупности трех угроз: террористической, преступной и военно-политической, включающей в себя информационные войны между государствами.

Основным нормативно-правовым актов в РФ в данной сфере являются «Основы государственной политики в области международной информационной безопасности до 2020 года». В рамках данного документа список международных информационных угроз был расширен. В частности, были добавлены угрозы нарушения государственного суверенитета посредством использования ИКТ, дестабилизация общественного порядка и разжигание межэтнической или межнациональной вражды.

В качестве основных причин активного участия России в формировании концепции международной информационной безопасности можно выделить следующие:

· Создание правовых и организационных основ сотрудничества государств в области обеспечения международной информационной безопасности.

· Обеспечение безопасности государственного суверенитета, подрываемого при помощи «информационного оружия», что, в целом, явило собой реакцию РФ на события, развернувшиеся в странах Ближнего Востока в рамках т.н. «арабской весны».

· Противодействие консолидации международного терроризма и планированию и подготовке террористических актов, а также недопущение деструктивного воздействия на элементы критической информационной инфраструктуры.

· Недопущение нарушения социальной целостности государств и «расшатывания» общественного порядка посредством разжигания межнациональной или межэтнической розни или вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию.

· Оптимизация борьбы с правонарушениями в информационном пространстве на базе оптимального международного сотрудничества в данной сфере.

На основании проведенного сравнительного анализа политики международной информационной безопасности, проводимой Россией, США и странами Европейского Союза, можно сделать вывод о том, что в зависимости от различных структурно-политических факторов различных стран во главу угла ставятся различные цели. Так, приоритетом России в рамках международного сотрудничества в сфере информационной безопасности является обеспечение абсолютной «демилитаризации» глобального информационного пространства, в то время как основным направлением деятельности США и ЕС в данной области является противодействие международному кибертерроризму и киберпреступности.

Наиболее исторически значимым документом ООН в сфере обеспечения международной информационной безопасности является резолюция Генеральной Ассамблеи от 20 ноября 2000 г. «Роль науки и техники в контексте международной безопасности и разоруже-

ния», в которой, утверждается приоритет мирного, гражданского использования достижений науки и техники в сфере информационных технологий перед реализацией военного потенциала ИКТ.

На заседании Группы правительственных экспертов ООН по международной информационной безопасности 22-26 июня 2015 года было дополнительно закреплено суверенное право государств самостоятельно распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности (МИБ).

Для того, чтобы достичь заявленных целей и скоординировать усилия стран по борьбе с киберпреступностью, Международная конференция представителей государственных и коммерческих структур стран «Большой Восьмерки» по вопросам безопасности и доверия в киберпространстве. Деятельность этой конференции осуществляется в рамках регулярно проводимых встреч, где экспертами и политиками вырабатываются конкретные меры по трем основным направлениям:

· защита электронной торговли, критической инфраструктуры и повышение доверия в киберпространстве путем оценки угроз и предотвращения преступлений;

· улучшение способности обнаружения и идентификации преступников, использующих информационные технологии;

· совершенствование партнерских отношений между государственными структурами, частным сектором, пользователями в целях обеспечения безопасности и доверия в киберпространстве.

Таким образом, Конференция наметила важнейшие шаги по обеспечению безопасности информационного общества, в ее недрах родились значимые рекомендации государственному сектору, бизнесу и частным лицам о правилах безопасной и эффективной работы в киберпространстве.

Источники и литература

1) Беляев Е.А. Информационная безопасность как глобальная проблема / Международная конференция «Глобальные проблемы как источник чрезвычайных ситуаций». Доклады и выступления / Под ред. Ю.Л. Воробьева М.: УРСС, 2000

2) Белянцев А.Е. Глобализация информационного пространства: новые вызовы международной безопасности // Международные отношения в XXI веке: новые действующие лица, институты и процессы: Материалы международной научной конференции РАМИ, МГИМО (У) МИД РФ, ИСИ ННГУ. М.: МГИМО (У) МИД РФ, 2001.

3) Торопцев Е. Л., Репин А. В. Информационная безопасность и стандарт CobiT // Молодой ученый. — 2014. — №8. — С. 112-115.

4) Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. N ПР-1895

5) Министерство иностранных дел РФ «Об итогах заключительного заседания Группы правительственных экспертов ООН по международной информационной безопасности» 30.06.15, Режим доступа: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1525144

6) Окинавская Хартия Глобального Информационного Общества. Режим доступа: http://www.g8kyushuokinawa.go.jp/e/documents/it1.html.

7) Проект Доктрины информационной безопасности РФ 2015г. Режим доступа: http://infosystems.ru/assets/files/files/doktrina_IB.pdf