Антипова Татьяна Сергеевна,

студентка 2-го курса;

Зарипова Римма Солтановна,

канд. техн. наук, доцент,

ФГБОУ ВО «Казанский государственный энергетический университет»,

г. Казань. Республика Татарстан, Россия

УГРОЗЫ БЕЗОПАСНОСТИ ГОСУДАРСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

Статья посвящена рассмотрению информационного аспекта процесса глобализации с акцентом на информационное противостояние между различными субъектами в киберпространстве.

Ключевые слова: информационная безопасность, Интернет, информация, информационная война, кибервойна, национальная безопасность.

В XXI веке человек окружен информацией. Мы получаем новости из Интернета, из СМИ, из социальных сетей. Информационный поток становится всё больше, а времени для его оценки, проверки первоисточников – меньше, и человек бывает не в состоянии с ним справиться. Человеку не остаётся ничего, кроме как принять всё за правду. Именной этой слабостью пользуются многие страны мира, ведущие информационную войну, для эффективной внешней политики. Умелое использование информации позволяет не только влиять непосредственно на внутригосударственные процессы, но и формировать общественное мнение относительно тех или иных событий. Слабым звеном в этой системе являются люди, у которых отсутствует критическое мышление, люди со слабой гражданской позицией, люди, незнакомые с мировой и отечественной историей, люди с узким кругозором и молодые люди и подростки, личное мнение которых относительно мира ещё не сформировалось окончательно. Лакуны в сознании этих людей легко заполняются информацией из различных, порой недостоверных источников.

Разберём подробнее понятие *информационной войны.* Данное явление представляет собой воздействие на народные массы отдельного государства,

групп государств или всего мира путём распространения определённой информации или дезинформации. Синонимом этого термина можно считать выражение «психологическая война». Также понятие «информационной войны» частично включает в себя относительно новое понятие «кибервойны». Кибервойна подразумевает ведение войны с использованием компьютерных технологий и Интернета, а не физических способов. Два этих понятия отличает то, что информационная война направлена на формирование определённого общественного мнения, а кибервойна может включать в себя как и DDoS-атаки (нарушение работоспособности определённых сайтов), взлом частных аккаунтов и серверов и утечку конфиденциальных данных, так и воздействие на системы функционирования государства. Мир в полной мере осознал мощь информации ещё в прошлом столетии, в ожидании, когда холодная война между двумя державами-гигантами перерастёт в горячую.

Ведущий вектор развития современного мира – процесс глобализации – это процесс всевозрастающего воздействия на социальную действительность отдельных стран, различных факторов международного значения: экономических и политических связей, культурного и информационного обмена и т.п. Эта среда стала идеальной для распространения информации. В цифровом XXI веке информация является полноценным видом оружия, которое умело используется на межгосударственной арене для пропаганды, саботажа и влияния на массы. Новости СМИ и Интернета вращаются вокруг политики, разнося необходимую определённым лицам информацию с немыслимой скоростью.

Наша страна за свою историю не раз становилась целью информационного оружия. Например, в заявлении президента Грузии, которое активно форсировалось на Западе, относительно вооружённого конфликта в Южной Осетии. В качестве другого примера можно привести печальные события в Украине в 2013-2014 гг., а точнее то, что происходило в это время на новостных каналах, в печатных изданиях, в блогах и социальных сетях. Против России развернулась информационная война со стороны Украины, Европы и

Америки. Западные СМИ передавали не объективную реальность, а свою искажённую версию, выставляя каждое действие России в негативном свете. Согласно социальным опросам, за 2014 г. отношение стран мира к России резко ухудшилось. Позитивное отношение чаще всего высказывают жители азиатских стран, с которыми Россия является партнерами по БРИКС.

Другой угрозой информационного оружия является влияние на граждан страны. Следствием является снижение доверия граждан к власти, падение уровня патриотизма в стране, раздробленность народа. В РФ, как и в остальном мире, к проблеме противостояния стран в киберпространстве подходят с большой серьёзностью, признавая её угрозой национальной безопасности [1].

Последствия информационных войн и кибервойн может быть самым разнообразным, так как влияние оказывается на любую сферу общества. Умелое использование информационного оружия может не только сформировать отношение народных масс к какому-либо явлению, дискредитировать политических деятелей, оказать значительное влияние на экономику страны и прочее, но и переписать историю.

В настоящее время Россия нуждается в высококвалифицированных специалистах-программистах, математиках, специалистах в областях кибербезопасности и компьютерной криминалистики. Натан Майер Ротшильд однажды произнёс фразу, которая станет крылатой: «Кто владеет информацией, тот владеет миром». Английский банкир тогда не мог представить, насколько правдиво будет это утверждение через два столетия.

СПИСОК ЛИТЕРАТУРЫ

1. Бикмухаметов И.И. Кибертерроризм как угроза информационной безопасности / И.И. Бикмухаметов, Р.С. Зарипова // Аллея науки. – 2018. – Т.1. – №2(18). – С. 266-268.

2. Ромашкин В.А. Влияние информационных технологий на современное общество / В.А. Ромашкин, О.А. Пырнова, Р.С. Зарипова // Современные научные исследования и разработки. – 2018. – №9(26). – С. 341-344.