УДК 32.019.51

Васильева Ю.Н.,
студент магистратуры, 2 курс
кафедра коммуникационных технологий
Московский государственный лингвистический университет
Россия, г. Москва

АНАЛИЗ СПЕЦИФИКИ ИСПОЛЬЗОВАНИЯ ИНСТРУМЕНТОВ ИНТЕРНЕТА В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Аннотация: *В статье проведен анализ специфики применения инструментов Интернета в информационном противоборстве (ИП) в международных отношениях. Автором рассмотрены основные инструменты Интернета в ИП, обозначены их преимущества и отличительные черты, приведены примеры их использования.*

Ключевые слова: *информационное противоборство, международные отношения, Интернет, социальные сети, блоги, мессенджеры.*

Abstract: *The article presents the analysis of the specific application of the Internet tools in the information warfare (IW) in international relations. The author considers the main Internet tools used in the IW, their advantages and characteristics are designated, examples of their use are given.*

Key words: *information warfare, international relations, internet, social networks, blogs, messengers.*

В современных реалиях Интернет представляет мощный набор инструментов, позволяющих воздействовать на общественное мнение и сознание в рамках деятельности информационного противоборства, в том числе и на международном уровне. Инструменты, которые предлагает Интернет,

позволяют осуществлять эффективную коммуникацию по всем направлениям жизнедеятельности современного общества.

Основными инструментами Интернета, которые могут быть использованы в информационном противоборстве, являются новостные ресурсы, социальные сети, блог-платформы, видеохостинги и мессенджеры. Рассмотрим специфику применения некоторых из них.

Особое место в информационном противоборстве в международных отношениях занимают социальные сети, функционирующие в Интернете. Особенности их информационно-психологического воздействия заключаются в том, что в виртуальных сообществах размещается информация, представляющая собой совокупность субъективных мнений лиц, являющихся своего рода «авторитетами мнений». Это позволяет сопоставить процесс распространения информации в социальных сетях с теорией «слуха». Социальные сети и блоги в настоящее время являются самым распространённым средством получения и передачи информации.

Пользователь социальных сетей получает легкий доступ к информации, а также возможность участвовать во взаимодействиях в социальных сетях. Социальные сети активно используют для влияния на общественное мнение, поскольку доступ к виртуальному миру человек может получить в любое время с помощью специальных гаджетов.

Есть много способов высказать свое мнение или оценку какого-то вопроса в социальных сетях:

- в виде текста в личной переписке с другим пользователем (можно не только высказаться, но и узнать мнение другого);
- в форме сообщения и комментариев;
- в форме обсуждения поднимаемого вопроса;
- в виде опроса (мнение выражается в форме голосования по какому-либо вопросу);
- в форме оценки, оценки кого-то или чего-то по балльной шкале, в зависимости от рода социальной сети (например: Facebook, Vkontakte, Одноклассники).

В качестве примера применения социальных сетей как основного инструмента в борьбе за превосходство в информационном пространстве рассмотрим ведение военной операции Израиля «Литой свинец» в секторе Газа, сопровождавшейся информационной поддержкой соответствующих государственных структур, которые должны выполнять подобную работу по долгу службы. В то же время были активно задействованы неофициальные методы распространения информации со стороны государственных структур. К информационной войне были подключены социальные сети, которые показали свою эффективность.

В ходе выше упомянутой операции социальные сети всех видов с самого начала стали орудием для ведения информационной войны со стороны Израиля. Основная работа велась в направлении подавления пропаганды противника, привлечения внимания к позиции Израиля и т.д. В то же время сетевые средства использовались и для проведения психологических операций внутри страны. Так была запущена акция «Пошли солдату улыбку» – была открыта возможность для всех граждан посылать солдатам Израиля, воюющим на передовой, свои приветствия.

Кроме того, для Израиля основным направлением в ведении информационной войны, естественно, стал внешний вектор. Сразу с началом эскалации арабо-израильского конфликта в Интернете резко повысилась активность блогеров – сторонников Израиля. Операция Израильской армии «Литой свинец» началась 27 октября. Уже 29 октября произраильские блогеры открыли на самой посещаемой русскоязычной площадке блогов Livejournal.com сообщество «gaza2009». Главная задача сообщества была поддержка и консолидация в сети всех, кто поддерживает Израиль в военное время. Через сообщество велось информирование об акциях в поддержку Израиля. Кроме данного сообщества, которое выделяется целевой работой, а также, вовлеченностью в него известных журналистов и политиков, были задействованы также социальные сети, которые были призваны работать уже не на конкретные задачи, а на массовое распространение нужной информации.

На наш взгляд рассмотренный пример показывает, что через блоги агентами активно реализовывается влияние на привычные стереотипы и модели поведения людей. Созданные условия, таким образом, являются обоснованием легитимности действий для внедренной агентуры. В результате, можно повлиять на качество принимаемого законопроекта, помешать или способствовать его рассмотрению, побудить общественность поддержать проект, а агентам влияния притворить его в жизнь.

Перенос настроений в реальный мир происходит в результате информационного воздействия на мотивационную основу личностей, с изначально сформированными взглядами, близкими для реализации тех или иных намерений, которые ожидает от них воздействующая сторона. А также в результате информационного воздействия на группы населения и конкретных лиц с неустойчивыми взглядами, трансформация которых позволяет поставить людей в требуемые рамки социального поведения. Создавая информационную обстановку и провоцируя общественность на активные действия, можно вынуждать военно-политическое руководство иностранных государств к ответным мерам. Препятствуя принятию грамотных решений с целью принуждения к совершению ошибочных действий, можно формировать впечатление у вышестоящего руководства или общественности об отсутствии компетенции лиц, несущих ответственность за эти решения. Это может спровоцировать отстранение или ограничение полномочий отдельных руководителей. Такими провокациями можно добиться сковывания инициативы руководства различного уровня или формирования общественного мнения и настроения, препятствующего работе органов государственной власти.

Таким образом можно говорить о том, что блоги, как и социальные сети, являются эффективным инструментом информационного противоборства в Интернете. Они дают возможность любому человеку общаться со всем миром напрямую, передавая и получая информацию меньше, чем за секунду, минуя какие бы то ни было границы. Система «друзей» (friends) позволяет распространять информацию тысячам адресатов в короткий промежуток

времени. Именно поэтому ведущие спецслужбы мира стали использовать блогинг в информационном противоборстве, в том числе и на международном уровне. В каждой стране имеются площадки для ведения блогов. Они есть во многих крупных городах и корпорациях. Наиболее востребованными в Интернет-среде являются следующие сервисы: Livejournal.com; Blogger.com; WordPress.com; Tumblr.com.

Выбор площадки зависит от предпочтений целевой аудитории, а также посещаемости конкретного Интернет-ресурса. На каждой площадке работает одно отделение – в сфере политики, экономики, промышленности. В рамках информационного противоборства одной темой занимаются два-три блогера-разведчика, каждый из которых ведет три-четыре вымышленных персонажа с разными характерами, живущих в разных местах, возможно, даже разноязычных. Причем, если три выдуманных иностранными блогерами персонажа, скажем, ругают Россию, один должен нелепо и глупо ее хвалить. В конце дискуссии такого персонажа разубеждают «фактами». Складывается впечатление реального общения, в котором участвуют тысячи человек, и блогеры подводят их к нужным выводам.

Следующим инструментом в информационном противоборстве в Интернете является видеохостинг. Видеохостинг – это веб-сервис, позволяющий загружать и просматривать видео в браузере, например, через специальный проигрыватель. При этом большинство подобных сервисов не предоставляют видео, следуя таким образом принципу «контент генерирует пользователь» (user-generated content). Видеохостинг стал набирать популярность вместе с распространением широкополосного доступа в Интернет и развитием (удешевлением) жёстких дисков, на которых стало возможно долговременно хранить огромные объёмы информации.

Большое количество сайтов видеохостинга тематически не ограничивают своё наполнение. Однако некоторые видеохостинги занимают специализированные секторы, предлагая тематические порталы. Отличительной чертой видеохостингов среди инструментов Интернета являются правовые

аспекты: в то время как на некоторых интернет-сайтах проводится жёсткий контроль закачанных видеофайлов, на многих видеохостингах контроль за качеством и содержанием выкладываемой информации отсутствует. Аудитория видеохостингов насчитывает более 1 млрд человек из разных стран мира. Ежедневно в них загружаются видеофайлы продолжительностью свыше 80 тысяч часов. Все файлы размещаются по соответствующим тематикам. Эмоциональное воздействие «живой картинки» намного выше, чем у обычного текстового материала. Поэтому видеохостинги, особенно занимающий ведущие позиции YouTube, активно используются в пропагандистской деятельности [3].

Еще одним инструментом Интернета, который может быть использован в информационном противоборстве, являются новостные ресурсы.

В Интернете новостные ресурсы представлены:

- интернет-изданиями ведущих газет и журналов (более 30 тысяч);
- новостными порталами (специфицируются только на оперативном выпуске новостей, более 1000 в различных странах мира);
- информационно-аналитическими ресурсами (военно-политическая, военная, военно-техническая аналитика, более 800 на основных языках);
- пропагандистскими порталами (размещенные материалы направлены против отдельных стран, группировок для их дестабилизации);
- экстремистскими сайтами (распространяют материалы, призывающие к насилию, ведению подрывной деятельности) [2].

У каждого из этих ресурсов имеются свои традиционные пользователи, которые регулярно знакомятся с их материалами. В последнее время отмечается более активное использование интернет-источников для получения свежей информации по политическим и общественно-политическим вопросам по сравнению с традиционными медиа-источниками. Это объясняется ростом количества владельцев мобильных устройств, подключенных к Интернету. Мобильные телефоны последних моделей позволяют получать любые новости в реальном масштабе времени [1].

Следующим инструментом Интернета, который можно использовать в целях информационного противоборства являются мессенджеры. Специфика их использования заключается в том, что они представляют из себя системы обмена мгновенными сообщениями в интернете, в том числе голосовыми и видео.

Компания «Вымпелком» (бренд «Билайн»), которая использовала данные большинства российских мобильных операторов, составила рейтинг популярности мессенджеров. Выяснилось, что самым популярным среди наших соотечественников стал мессенджер WhatsApp (его используют свыше 68%). На втором месте рейтинга расположился Viber (45% пользователей), а на третьем – Skype (17,9% пользователей), Telegram используют 7,5%. При этом указанные мессенджеры позиционируются как безопасные и защищенные, однако на практике все далеко не так просто. И причин тому несколько. Первая из них – значительная часть подобных приложений напрямую принадлежит корпорациям, которые хотят собрать как можно больше данных о пользователях.

Еще одна проблема – почти все самые популярные инструменты коммуникации сегодня – это закрытые продукты. Их исходный код никому недоступен, кроме правообладателя, следовательно, он недоступен для аудита независимыми исследователями информационной безопасности. Это, в частности, приводит к тому, что такие продукты могут раскрывать важные данные даже вопреки желанию разработчиков, например, вследствие программной ошибки. Злоумышленники могут найти уязвимость и атаковать пользователей, и пока об этом не станет известно самим разработчикам, они не смогут закрыть брешь. Кроме того, традиционная модель мессенджеров предполагает централизацию, что также не очень хорошо с точки зрения безопасности. Приведем пример: Telegram – один из самых защищенных мессенджеров. Этот инструмент централизован, что означает, помимо прочего, что доступ к нему может быть перекрыт властями — такие попытки уже случались не в одной стране. В итоге для конечных пользователей доступ к защищенному инструменту коммуникации затрудняется или становится невозможным, что заставляет их переключаться на менее безопасные альтернативы. В итоге общий уровень защищенности коммуникаций снижается.

Таким образом, проведя анализ специфики основных инструментов Интернета, которые могут быть использованы в противоборстве, мы пришли к выводу о том, что формирование информационной обстановки в сети Интернет происходит путем естественного отражения действительности в ходе непосредственного общения между участниками каких-либо событий и распространением ими информации через социальные сети на различные аудитории, так и формированием информационных ситуаций через спланированные акции подготовленными специалистами. Раскрутка информационных ситуаций до критической степени, позволяющей спровоцировать общественность на активные действия (к массовым протестам), осуществляется путем воздействия на циркулирующую в Интернете информацию, распространением слухов, подготовкой подтверждающих или опровергающих сведений, которые необходимы для того, чтобы в достаточной степени убедить общественность в правдивости тех или иных событий, сформировать требуемые настроения, взгляды, убеждения.

СПИСОК ЛИТЕРАТУРЫ

1. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств. – СПб.: СПб ГИКиТ, 2016.

2. Лапшин В.А. Формирование системы международной информационной безопасности: подходы и инициативы России // Научные проблемы национальной безопасности Российской Федерации. 2017. № 5. С. 177-179.

3. Польских Л.О. применении глобальной компьютерной сети Интернет в интересах информационного противоборства // Пси-фактор. [Электронный ресурс]. Режим доступа: http://psyfactor.org/lib/psywar40.htm (дата обращения 28.11.2018)