УДК 355.23:004.056

«БЕСКОНТРОЛЬНЫЕ СОЦИАЛЬНЫЕ СЕТИ» КАК НОВЫЙ ИСТОЧНИК УГРОЗЫ БЕЗОПАСНОСТИ ГОСУДАРСТВА

А. В. Гаврилин
подполковник, преподаватель военной кафедры БрГТУ
Беларусь, Брест

В статье рассматриваются актуальные вопросы влияния социальных сетей и коммуникационных средств реального времени в деструктивных движениях, направленных на подрыв и свержение политической системы государства. Делается вывод, что для обеспечения информационной безопасности государства, предотвращения кибератак в сети Интернет возрастает потребность в подготовке квалифицированных специалистов в сфере IT, состоящих на государственной службе.

***Ключевые слова*:** национальная безопасность, информационная безопасность, информационная война, социальные сети, коммуникационные средства реального времени, «Soft Power», «Twitter-революция».

The article deals with topical issues of the influence of social networks and real-time communication tools in destructive movements aimed at undermining and overthrowing the political system of the state. It is concluded that in order to ensure the information security of the state, to prevent cyber-attacks on the Internet, there is an increasing need for the training of qualified specialists in the field of IT, who are in the public service.

***Key words*:** national security, information security, information warfare, social networks, real-time communications, Soft Power, Twitter revolution.

Развитие веб-технологий и их влияние на современное общество привело к изменению традиционных сфер коммуникаций, изменению способов и форм коммуникации в Интернете. Интернет и компьютерные сети пользуются спросом по всему миру. Финансовая сфера, СМИ, политика, общественные движения организованы вокруг сети Интернет. Темп роста всемирной сети высок и продолжает нарастать как за счёт увеличения количества пользователей глобальной сети Интернет, так и за счёт роста объёмов информации в самом Интернете, но наряду с положительными моментами появление сети Интернет принесло в нашу жизнь новую площадку для ведения войн.

Войны могут выигрываться на поле боя, а проигрываться в сознании людей. Информационные войны сопровождают всю историю человечества. Сначала они были религиозными и идеологическими, причём для борьбы с носителями чужих взглядов применялись все виды репрессий.

Впервые термин «информационная война» вошёл в широкое употребление в последней четверти XX века. Хотя о значении информации в военном деле было сказано ещё в V–VI вв. до н. э. древнекитайским философом и полководцем Сунь Цзы в «Трактате о военном искусстве»: «Подрывайте престиж руководства

противника и выставляйте его в нужный момент на позор общественности. Разжигайте ссоры и столкновения среди граждан враждебной вам страны. Сковывайте волю противника песнями и музыкой. Делайте всё возможное, чтобы обесценить традиции ваших врагов и подорвать их веру в своих богов. Будьте щедры на предложения и подарки для покупки информации и сообщников, вообще не экономьте на деньгах, это приносит прекрасные результаты».

Социальные сети, такие как Facebook, LiveJournal, «ВКонтакте», а также коммуникационные средства реального времени, такие как Twitter, Telegram, WhatsApp, стали одним из основных средств воздействия в политических событиях последних лет. Несмотря на технологические различия, их объединяет сетевая модель взаимодействия. Во всех недавних «цветных революциях» использовался подобный функционал. Социальные сети активно применялись во время протестных событий в Украине, Иране, Турции, Египте, России, Беларуси. Они являются эффективным способом трансляции настроений массам и входят в состав технологии «Soft Power».

Общая схема взаимодействия: через социальную сеть Facebook, LiveJournal путем создания развернутых аналитических статей, интервью, создается протестный дискурс, создаются информационные поводы, инициируются дискуссии, что приводит к формированию массового мнения и настроения. Люди, объединенные определённым настроением к некоторому событию, представляют собой основу формирования протестной группы, так как начинают формироваться схожие взгляды и настроения по отношению к нужному событию. Twitter используется для информационных вбросов с эффектом срочности и усиления информационного фона. Коммуникационные средства реального времени Telegram, WhatsApp используются для координации действий.

Twitter создан в 2006 году, за полгода количество пользователей достигло десятков миллионов по всему миру. Twitter основывается на принципе подписчиков для отображения новостных лент и структуре коротких публикаций пользователей – до 140 символов. Краткость – основа оперативности передачи публикаций и удобства восприятия информации с экранов мобильных устройств. В 2009 году при аварийной посадке самолета на Гудзон пост о событии с фотографией опередил сообщения официальных СМИ и новости сети Интернет.

Хороший пример использования Twitter – координация действий и мобилизация протестных групп перед молдавскими выборами. Сначала была проведена массовая рассылка сообщений и новостей в Facebook, далее через Twitter были созданы специальные хештеги для информирования участников. Под хештегами размещались основная информация, связанная с протестующими. Обновления в Twitter публиковались практически непрерывно, содержали в себе записи очевидцев, комментарии.

Через несколько месяцев события повторились в Иране. Информационным поводом для развития оппозиционных течений стало несогласие с результатами президентских выборов. Действующие власти предприняли попытку блокировать сегменты сети GSM, службу отправки SMS, мобильный интернет. Но действия запоздали – были организованы резервные ретрансляторы и Wi-Fi передатчики. Это позволило использовать Twitter как основной коммуникационный канал: почти ежесекундно публиковались сообщения о подготовке, перемещениях, происшествиях.

Революционные события и протестные процессы показали актуальность применения систем микро-публикаций, таких как Twitter. СМИ стали использовать определение «Twitter-революция», особенно актуальное после революции в Египте в 2011 году.

После этих событий и ряда других власти некоторых государств стали ограничивать использование социальных сетей, например, Китай или Южная Корея. Так, во время выборов сообщения Twitter с тематикой предвыборной кампании должны быть с пометкой агитации. Наиболее эффективные методы противодействия – это массовый вброс новостей, перекрывающий протестные ленты. Если отсутствует возможность ограничить передачу информации, то её можно перекрыть информационным шумом, вызвав информационный перегруз восприятия целевых групп. Также возможно модернизировать протестные сообщения, внедряя в информационные ленты различные комментарии и новые трактовки происходящего.

Процессам «ненасильственных переворотов» характерен коммуникативный характер, это революции нового организационно-информационного типа, «революции флешмоба». Социальные сети становятся информационной основной революций нового типа. Twitter выполняет подчас решающую роль в координации протестных сил, усиления информационного давления. Однако наибольший эффект применения Twitter достигается Facebook, YouTube, Livejournal, обладая при этом важнейшим отличием от них – практически неограниченной оперативностью. Использование Twitter, однако, в большой степени зависит от «подготовки почвы» для протестных действий или прочих коллективных акций. В целом же, очевидно: Twitter обладает гигантским потенциалом с точки зрения развития социального моделирования.

«Наиболее уязвимым местом современных сложных систем становятся процессы принятия решений. Именно поэтому информация как таковая постепенно начала менять свой статус», – считает доктор филологических наук, профессор, специалист в области коммуникативных технологий Г. Г. Почепцов [2]. Большинство «цивилизованных» государств мира щедро вкладываются в подготовку «специалистов», работающих воздействуя на наши чувства через социальные сети и другие источники информации глобальной сети. Таким образом, исход действующих и будущих войн начинает вершиться в IT-пространстве. Принимая во внимание потенциальные угрозы, исходящие от бесконтрольных социальных платформ в сети Интернет, «Концепция информационной безопасности Республики Беларусь» предусматривает осуществление мониторинга, анализа и оценки информационных ресурсов сети Интернет на предмет безопасности для государства, реализует «комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз» [3]. Особое внимание уделяется кадрам, способным своевременно обнаружить риски для государственных информационных систем, воспрепятствовать кибератакам и акциям деструктивного воздействия. В связи с этим возникает необходимость в подготовке квалифицированных специалистов в области информационных технологий, состоящих на государственной службе. Развитие современной системы образования должно пролегать в этой новой плоскости защиты государства и морально-нравственных ценностей общества.

Список источников и литературы

1. Хрущёва, Н. Информационные войны – от Сунь Цзы до «фабрики троллей» Н. Хрущёва, С. Распопова // журнал «Журналист». – 2021. – № 6. – 27 мая [Электронный ресурс]. – Режим доступа : https://jrnlst.ru/information-wars. – Дата доступа : 02.02.2023.

2. Почепцов, Г. Информационные войны: тенденции и пути развития Г. Почепцов // Библиотека «Пси-фактора» Psyfactor.org. 16+ [Электронный ресурс]. – Режим доступа : https://psyfactor.org/psyops/infowar7.htm . – Дата доступа : 02.02.2023.

3. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: // Pravo.by. Национальный центр правовой информации Республики Беларусь – Режим доступа : https://pravo.by/document/?guid=125–51&p0=P219s0001&p1=1. Дата доступа : 01.02.2023.