проведение системного анализа показателей безопасности сетевых продуктов и систем с позиции их устойчивости и надежности в условиях различных сценариев террористических действий и на этой основе – совершенствование действующих стандартов безопасности.

УДК 34:004.77

П.Л. Боровик

ГЛОБАЛЬНАЯ СЕТЬ ИНТЕРНЕТ КАК ВАЖНЫЙ ИНСТРУМЕНТ ФОРМИРОВАНИЯ ОБЩЕСТВЕННОГО МНЕНИЯ

В настоящее время бурно развиваются новейшие информационно-коммуникационные технологии, активно применяемые в различных сферах человеческой деятельности. Информация, передаваемая с помощью современных средств коммуникации, не только превратилась в неисчерпаемый стратегический ресурс. При умелом использовании разнообразных форм, методов и приемов психологического воздействия на сознание и поведение людей она стала эффективным средством формирования общественного мнения и достижения геополитических целей. Эпоха мировой глобализации привела к созданию единого глобального информационного пространства всей планеты, в котором развернулось геостратегическое информационное противоборство между ведущими центрами силы, рассматриваемое большинством экспертов как неотъемлемый компонент современной войны.

Яркими примерами информационного противостояния являются современная ситуация вокруг Украины, Сирии, феномен «арабской весны», а также конфликт Израиля и Палестины, где информационная составляющая стала одним из наиболее важных элементов планирования и проведения военных операций. Противоборствующие стороны активно используют в своих интересах разнообразные коммуникативные средства целенаправленного психологического воздействия на массовое сознание посредством использования различных информационных ресурсов: печатных и электронных средств массовой информации, телевидения, радио, интернета, телефонных и иных коммуникационных сетей. Некоторые страны до сих продолжает сотрясать управляемый хаос в обществе, посеянный конструкторами сетевых политических технологий, который способствует развитию политическому кризису в их государствах.

Обращаясь с ежегодным Посланием к белорусскому народу и Национальному Собранию, президент Республики Беларусь А.Г. Лукашенко

отметил, что нашей стране не удастся остаться в стороне от этих глобальных процессов. «Следует по-новому взглянуть на существующую систему защиты своего информационного пространства. Она должна быть гибкой, отвечать всем требованиям времени. Первоочередная задача – оградить граждан от использования в отношении их манипуляционных технологий, не нарушив при этом конституционного права на получение информации», – отметил Глава государства [1].

Выступая во время оперативного сбора командного состава Вооруженных Сил Республики Беларусь, А.Г. Лукашенко справедливо обратил внимание на то, что в современных условиях противоборство на мировом информационном поле по своей интенсивности не уступает реальным боевым действиям, а ущерб, наносимый при этом, несоизмерим с потерями конфликтующих сторон в физическом пространстве, ведь борьба ведется за сознание людей. Не является исключением и информационное пространство Беларуси: неотъемлемой частью деструктивного воздействия на наше государство становится все нарастающая информационная экспансия. «Она является мощным оружием для достижения политического, экономического и военного превосходства в любом противостоянии», – подчеркнул Президент [2].

Это определяет ряд угроз, на которые наша страна должна реагировать адекватно интересам собственной безопасности.

Согласно Концепции национальной безопасности одной из основных угроз Республики Беларусь в информационной сфере является, с одной стороны, нарастание информационного противоборства между ведущими мировыми державами в информационном пространстве, а с другой – развитие технологий манипулирования информацией. Превращение глобальной сети Интернет в средство общемирового вещания, механизм распространения информации, среду для коммуникации в широком смысле этого слова является определяющим фактором, обусловливающим возрастание ее роли в качестве мощного средства манипулятивного воздействия на целевую аудиторию и формирования общественного мнения путем информационно-психологического воздействия.

Специфическим, актуализирующим обозначенную проблему обстоятельством является тот факт, что в современном обществе все более значимое место начинает занимать общение между людьми, опосредствованное различными интернет-ресурсами. Одним из наиболее значимых в коммуникативном плане ресурсов являются социальные сети, открывающие широкие возможности для взаимодействия, обмена комментариями и установления отношений с другими пользователями. Социальные сети способны не только концентрировать огромный объ-

ем информации, но и в результате массовых коммуникаций (общения) выявлять, группировать и консолидировать контингент определенного мнения и настроения. При этом социальные сети становятся не просто местом общения для самых разных слоев населения, но и мощным средством выражения активной позиции и формирования результативного общественного мнения. Существенное влияние на формирование общественного мнения оказывают также оценки, отзывы и комментарии пользователей интернет-ресурсов, признаваемых в виртуальном и реальном мире в качестве авторитетных, компетентных.

Вместе с тем, обладая колоссальным потенциалом информационного влияния на индивидуальное и массовое сознание, подобные электронные ресурсы «всемирной паутины» способны преподносить те или иные сведения либо факты в определенном контексте, создавая тем самым потенциальную угрозу манипулятивного воздействия на личность. Интернет-коммуникации становятся удобной площадкой для ведения информационной пропаганды и установления различными индивидами либо общественными группами доминирующего контроля за распространением информации. Опыт зарубежных стран показывает, что целенаправленное информационно-психологическое воздействие на граждан, реализуемое через социальные сети и иные интернет-ресурсы, потенциально способно создать атмосферу напряженности и политической нестабильности в обществе, спровоцировать социальные, национальные, религиозные конфликты, массовые беспорядки, привести к разрушительным последствиям для политического развития страны. Несмотря на очевидность данного факта, ответственность за манипулирование информацией и использование подложных либо искаженных фактов с целью получения конкретного конечного результата остается в определенной степени размытой.

Наиболее деструктивным видится информационное воздействие на молодых людей, у которых в силу социально-психологических и возрастных особенностей ценностные ориентации и смысловые установки еще неустойчивы либо не сформированы, вследствие чего их жизненные траектории под воздействием деструктивной пропаганды могут склониться в сторону асоциальных, антиобщественных действий.

В контексте обозначенной проблемы важным представляется рассмотрение некоторых наиболее распространенных технологий формирования общественного мнения путем манипулирования массовым сознанием с использованием ресурсов глобальной сети Интернет.

Существуют следующие приемы манипуляции сознанием людей: преподнесение нужной в данный момент, нередко грубо сфабрикованной информации; преднамеренное утаивание истинных, соответствующих действительности сведений; обеспечение информационной перегрузки, затрудняющей возможность объекту воздействия разобраться в сути дела; смешивание истинных фактов с предположениями, допущениями, гипотезами, слухами, что делает практически невозможным отличить правду от вымысла; оттягивание под различными предлогами обнародования важных сведений до момента, когда будет поздно что-то изменить, и т. д. При этом обман наверняка раскроется позже, но к тому моменту данное поведение будет восприниматься общественностью как нечто естественное, необходимое или вынужденное [3, с. 105–106]. Все эти приемы, как показывает практика, в той или иной степени применялись в конфликтах последних десятилетий.

Одним из основных механизмов манипулирования общественным мнением в социальных сетях является воздействие на пользователей через механизм большинства общественного мнения, когда сетевым участникам пытаются внушить, что продвигаемые среди них оценки происходящих тех или иных (как правило, политических) событий поддерживаются большинством граждан. В общем виде процесс подобного воздействия состоит из следующих этапов: подготовка информационной базы влияния; создание провокационной ситуации и контролируемого процесса ее обсуждения в социальной сети; попытка убеждения пользователей, что предъявляемые в ходе дискуссии мнения поддерживаются большинством представителей социальной сети; реализация управляемых воздействий.

Так, в процессе подготовки информационной базы влияния субъектами информационного воздействия закладываются сомнения в сложившихся устоях, освещается негативный опыт государственного управления, подрывается авторитет государственных средств массовой информации, формируется основа для создания лозунгов, которые будут использоваться в активной фазе информационного противоборства. Затем в ходе возникновения провокационной ситуации, поддерживаемой антиправительственными средствами массовой информации, в социальных сетях создается контролируемый процесс ее обсуждения. В активной фазе влияния со стороны большинства социальной сети осуществляется непосредственное воздействие на участников данной социальной сети с призывами к активным действиям и готовности поддержать их [4, с. 105]. Не последнюю роль в этом процессе играют вброс дезинформации, представление информации в выгодном для себя ключе и феномен сознательного преувеличения.

Информационное воздействие в Сети обычно реализуется в следующих формах словесных высказываний: а) утверждения о фактах и

событиях или констатация фактов и событий с использованием таких выражений, как «не вызывает сомнения», «естественно», «однозначно» и т. п.; б) мнения о фактах, событиях и лицах с использованием выражений типа: «с моей точки зрения», «не вызывает сомнения», «по моему мнению», «я считаю» и др.; в) оценка фактов, событий, лиц и их действий с использованием выражений, создающих отрицательную или положительную окраску: «ужасно», «отвратительно», «плохо», «мерзко», «отлично», «прекрасно» и т. д. К данному инструментарию также относятся: подтекст, намеки, ирония, фрагменты из популярных текстов, фильмов, выступлений и др. [5]. Все эти инструменты воздействия широко используются в языке средств массовой информации в процессе ведения информационных войн.

Для того чтобы государство и общество могли противостоять угрозам в информационной сфере, необходимо не только владеть методикой противодействия деструктивной идеологии в сети Интернет, но и активно использовать возможности информационно-коммуникационных технологий для ее нейтрализации и трансляции приоритетов государственной политики.

Мероприятия по нейтрализации деструктивного информационного воздействия на процесс формирования общественного мнения должны предусматривать следующие механизмы [6, с. 64–65]:

прогнозирование, что предполагает выявление угроз и оценку ущерба применения средств деструктивного информационного воздействия;

профилактика (упреждение) деструктивного информационного воздействия – предполагает осуществление ряда превентивных мероприятий по снижению восприимчивости и подверженности населения информационному воздействию. Главным инструментом этого процесса является систематическая, профессионально подготовленная контрпропаганда, разъяснение обществу истинных целей, способов, возможных последствий акций информационно-пропагандистского характера. Важнейшим аспектом такой информационной деятельности являются механизмы формирования общественного мнения путем размещения в средствах массовой информации и на популярных интернет-ресурсах информации упреждающего характера;

пресечение деструктивного информационного воздействия – достигается своевременным выявлением и предупреждением сил, средств, способов психологического воздействия (уничтожение материалов, блокирование сайтов, доказательное опровержением слухов и т. п.);

ликвидация последствий деструктивного информационного воздействия – предполагает анализ и оценку результатов, причин эффективности, наиболее слабых мест в системе информационного противоборства, организацию и проведение мероприятий по оптимизации всей системы противодействия распространению деструктивной идеологии.

Перечисленные механизмы должны планироваться и осуществляться непрерывно и комплексно с учетом особенностей деструктивного информационного воздействия, реального социально-политического и морально-психологического состояния общества и складывающейся обстановки. Проблема их регулирования многогранна, поскольку имеет технические, политические, нравственные, экономические, правовые и, конечно же, психологические аспекты.

Обобщая вышеизложенное, сформулируем следующие выводы:

1. Информационные ресурсы сети Интернет оказывают ключевое влияние на формирование общественного мнения. С одной стороны, электронные средства массовой информации и открытые источники в Глобальной сети предоставляют широкие возможности для осуществления комплекса мероприятий информационно-психологического характера с целью оказания влияния на формирование общественного мнения путем манипулирования последним. С другой стороны, Всемирная паутина привлекает внимание отдельных субъектов как арена информационного противоборства за расширение собственной электоральной базы в социуме. При этом самостоятельной формой информационного противоборства становится практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам.

2. Методы, на которых основывается информационное воздействие в интернете, направлены прежде всего на изменение оценки происходящего различными социальными группами и личностями, развитие «нужных» субъекту воздействия настроений и оценок и, в перспективе, обеспечение перехода на сторону субъекта информационного воздействия.

3. Мероприятия по нейтрализации деструктивного информационного воздействия на формирование общественного мнения должны основываться на механизмах его прогнозирования, профилактики (упреждения), пресечения и ликвидации последствий. Указанные механизмы следует планировать и проводить непрерывно и комплексно с учетом особенностей деструктивного информационного воздействия, реального социально-политического и морально-психологического состояния общества и складывающейся обстановки.

1. Обращение с Посланием к белорусскому народу и Национальному Собранию [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь. – Режим доступа: http://president.gov.by/. – Дата доступа: 01.02.2016.

2. Лукашенко: надежное обеспечение национальной безопасности по-прежнему является одним из основных условий благополучия любого государства [Электронный ресурс] // БелТА. Новости Беларуси. – Режим доступа: http://www.belta.by. – Дата доступа: 01.02.2016.

3. Манойло, А.В. Технологии несилового разрешения современных конфликтов / А.В. Манойло. – 2-е изд. – М. : Горячая Линия-Телеком, 2014. – 392 с.

4. Зверев, А.Л. Социальные сети как инструмент политического манипулирования (на примере организации массовых протестов в Гонконге 2014 г.) / А.Л. Зверев, А.П. Федоров // Вестн. Бурят. гос. ун-та. – 2015. – № 7. – С. 149–154.

5. Тихомиров, С.А. К вопросу о некоторых технологиях ведения «информационных войн» [Электронный ресурс] / С.А. Тихомиров // Психология человека. – Режим доступа: http://psibook.com. – Дата доступа: 01.02.2016.

6. Грачев, С.И. Проблемы и особенности использования информационно-пропагандистского фактора в системе антитерроризма / С.И. Грачев, А.И. Завьялов, А.В. Товашов // Вестн. Каз. юрид. ин-та МВД России. – 2014. – № 2 (16). – С. 62–65.

УДК 004.056

Т.О. Бочкарева

ПРОБЛЕМА ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ К ПРОВЕДЕНИЮ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ И ЕЕ РЕШЕНИЕ

Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации.

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном порядке. Деятельность

системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является ФСТЭК России в пределах ее компетенции, определяемой законодательными актами Российской Федерации.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации, составляющей государственную тайну, и предусматривает комплексную проверку защищаемого объекта информатизации в реальных условиях эксплуатации в целях оценки соответствия используемого комплекса мер и средств защиты информации требуемому уровню безопасности информации.

В ФКУ НИИИТ ФСИН России с 2006 г. и по настоящее время функционирует орган по аттестации объектов информатизации на соответствие требованиям по безопасности информации. Орган по аттестации является составной частью организационной структуры единой системы обязательной сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации и имеет аккредитацию ФСТЭК России.

За 9 лет существования данного органа было аттестовано более 200 объектов информатизации (объекты вычислительной техники и выделенные помещения). Специалисты органа по аттестации проводят свою работу в тесном взаимодействии с научными, производственными, режимно-секретными учреждениями (организациями, предприятиями), представителями органов ФСБ, ФСТЭК, МВД и ФСИН России.

За время работы сотрудники органа по аттестации приобрели большой практический опыт по созданию систем защиты информации в учреждениях и органах уголовно-исполнительной системы, выявлению угроз безопасности информации, определению технических каналов утечки информации, составляющей государственную тайну.

Практическая деятельность органа по аттестации показала, что в настоящее время основными проблемами в структурных подразделениях ФСИН России в рамках создания систем защиты информации, выполне-