**С.Б.СЕЙЛХАНОВ**

*старший преподаватель*

*Военно-инженерный институт*

*радиоэлектроники и связи г. Алматы, Республика Казахстан*

**ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА ГОСУДАРСТВА ЧЕРЕЗ СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ**

В настоящее время прослеживается устойчивая тенденция на повышение роли и значения социальных сетей, история которых началась в 1995 году с появлением американского портала Classmates.com. Любое общественно значимое событие сегодня обсуждается заинтересованными и активными пользователями в социальных сетях.

По прогнозам в 2017 г. число пользователей социальных сетей вырастет до 2,2 млрд (или 31% всего населения), расходы на рекламу в соц. сетях в 2015 г. составили более 15,3 млрд. долл. Сегодня социальные сети, помимо выполнения функций поддержки общения по различным интересам, обмена мнениями, получения информации их членами, организации и ведения бизнеса, всё чаще становятся объектами и средствами информационно-психологического воздействия и управления на различных уровнях (в рамках региона, страны, международного сообщества).

Сети, социальные медиа — это существенный инструмент деструктивного информационно-психологического влияния, в том числе — в целях манипулирования личностью, социальными группами и обществом в целом.

При этом отмечу, проблемы деструктивного использования Интернета и социальных сетей, как угрозы вмешательства во внутренние дела, актуальны, первую очередь, для государств с достаточным уровнем проникновения Интернета (по данным МСЭ к концу 2014 года Интернетом пользовались почти 3 миллиарда человек, или 42,3% населения планеты).

К сожалению, в настоящее время радикализация является динамичным расширяющимся процессом, проникающий во все социальные слои общества. И социальные сети используются в качестве главного инструмента распространения.

Отмечаемый всеми рост радикализации ведет к социализации экстремизма, что ложится в основу терроризма. Недавние террористические акты в Европе потребовали пересмотра и активизации противодействия распространению этих идей, и в первую очередь, через соцсети.

В 2014 году «Исламское государство» (ИГ) использовало по меньшей мере 46 тысяч аккаунтов в Twitter, сообщает The Wall Street Journal со ссылкой на исследование Brookings Institution. По последним исследованиям 2015 года Европарламента 90% всей террористической активности, включая пропаганду радикализма и экстремизма, ведется в Интернете с использованием социальных сетей.

Мировые лидеры, государственные деятели и руководители спецслужб имеют схожие позиции по проблеме распространения экстремистской идеологии через социальные сети. Еще в ноябре 2014 г. директор Центра правительственной связи Великобритании (GCHQ) Роберт Ханниган (Robert Hannigan) писал, что ведущие социальные сети стали удобным плацдармом для террористических организаций, что террористы «Исламского государства» использовали возможности Интернета для создания глобальной международной террористической сети, а мессенджеры и социальные сети используются экстремистами для пропаганды своих идей и вербовки новых членов.

В феврале 2015 г. министр национальной безопасности США Джей Джонсон (Jeh Johnson) в интервью СМИ отметил, что по сравнению с планированием и организацией терактов 11 сентября, современные террористические организации более эффективно используют Интернет, социальные сети и другие средства для провокации индивидуальных терактов.

В ходе Саммита по противодействию насильственному экстремизму (февраль 2015 г., Вашингтон) и Президент США Барак Обама (Barack Hussein Obama), и Генеральный секретарь ООН Пан Ги Мун (Ban Ki-moon), и Верховный представитель ЕС Федерики Могерини (Federica Mogherini) в своих выступлениях говорили о проблеме использования онлайн-СМИ и социальных сетей для распространяя идей экстремизма и терроризма, об идеологической обработке молодых людей и вербовке новых членов экстремистских и террористических групп, о распространении вируса страха.

По итогам Саммита (а в нем приняли представители органов государственной власти из более чем 60 стран мира, в том числе и директор ФСБ России А.В.Бортников) было озвучено совместное Заявление, в котором, как одно из направления деятельности, выделялось использование глобальных коммуникаций, в том числе и социальных медиа, чтобы противостоять агрессивным экстремистским сообщениям.

Напомню, что вчера на заседании нашего Форума Брюс Макконнелл (Bruce McConnell), рассказывая о приоритетах деятельности Института Восток-Запад, поставил проблему деструктивного контента на второе место.

В России также актуальна борьба с распространением идеологии радикализма и экстремизма в социальных сетях. 1 февраля 2014 года в России вступил в силу закон, позволяющий Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по запросу Генеральной Прокуратуры без суда блокировать интернет-ресурсы с призывами к экстремизму и массовым беспорядкам. Ограничение доступа к таким сайтам должно осуществляться незамедлительно. Процедура может быть инициирована на основании мониторинга интернета, а также уведомлений от органов власти, организаций и граждан.

В 2014 году в РФ по требованию прокуратуры заблокировали более 900 экстремистских сайтов. Президент Российской Федерации В.Путин в этом году минимум дважды обращал внимание на эти вопросы: 4 марта 2015 г. на расширенном заседании коллегии МВД Владимир Путин отметил попытки использовать так называемые «цветные технологии» — от организации незаконных уличных акций до открытой пропаганды вражды и ненависти в социальных сетях. Цель этих действий очевидна — спровоцировать гражданские конфликты, ударить по конституционным основам нашего государства, по суверенитету страны в конечном итоге. 26 марта 2015 г., выступая на заседании коллегии ФСБ Президент, среди иных вопросов обеспечения информационной безопасности, отметил, что в части противоправного контента было выявлено свыше 25 тысяч интернет-ресурсов с публикациями, нарушающими закон. Прекращена работа более полутора тысяч экстремистских сайтов. Президент поставил задачу продолжать очищать российское интернет-пространство от незаконных, преступных материалов, более активно использовать для этого современные технологии, участвовать в формировании системы международной информационной безопасности.

Владимир Путин отметил, что речь не идёт о том, чтобы ограничивать свободу в интернете, необходимо строго соблюдать российские и международные правовые нормы, и стандарты в данной сфере. Не препятствовать общению людей в сети и размещению там законной, допустимой и корректной информации. Как видим, все политики озвучивают общие взгляды на проблемы распространения экстремистской идеологии через глобальные коммуникации и социальные сети. Но пока никто не предложил, как выработать общие механизмы противостояния и борьбы с этим явлением.

Хочу напомнить, что проблема фильтрации контента в глобальном информационном пространстве рассматривалась в ходе работы 7-й (апрель 2013 г., Гармиш-Партенкирхен) конференции нашего Консорциума (МИКИБ). Обсуждение показало, что большинство экспертов не сомневается в необходимости фильтрации вредоносного контента — и ряд развитых государств уже применяет такую практику. Вопрос только в том, какие выбраны механизмы определения контента как вредоносного, и какие средства используют для его фильтрации.

Эксперты согласились в необходимости соблюдения баланса между правами и свободами Интернет-пользователей, и обеспечением безопасности в информационной среде. Каждое государство в рамках национального информационного пространства вправе решать какие механизмы использовать: «Отключать» или «не отключать» национальный сегмент Интернета от глобальных сетей, закрывать отдельные Интернет-ресурсы и аккаунты в социальных сетях, усиливать уголовную ответственность, принимать иные, возможно жесткие меры — это внутреннее дело каждого государства.

Так, 15 марта этого года Правительство Франции заблокировало 5 сайтов за пропаганду идей джихада. Эта мера вызвала неоднозначную реакцию: с одной стороны, Правительство обвинили в нелигитимности действий, в административном подходе; с другой стороны, прозвучала критика эффективности данного решения, т.к. эти ресурсы могут изменить свои адреса или разместиться за пределами Франции.

Это подтверждает мысль о том, что только на национальном уровне решение данных проблем невозможно. Распространение противоправного контента в социальных сетях служит не только преступным, экстремистским и террористическим целям. В ряде регионов и стран отрабатываются технологии использования глобальных сетей, социальных медиа и мобильной связи для проведения трансграничных информационно-психологических воздействий на общественное сознание, организации массовых волнений и государственных переворотов. Т.е. вмешательство во внутренние дела суверенных государств. Самый распространённый пример — события в Тунисе, Ливии и Египте.

На наш взгляд, порой в освещении в социальных сетях отдельных событий в Украине есть элементы вмешательство во внутренние дела этой страны и России. Сложность противодействия угрозам пропаганды экстремизма и вмешательства во внутренние дела суверенных государств через социальные медиа сохраняется и углубляется. Практика свидетельствует, что только национальных регулятивных, в том числе запретительных, правовых норм для решения этих задач недостаточно. Трансграничный характер информационного пространства требует согласованных действий государств, международного сообщества. Конечно, на единых принципах равноправия, взаимного учета интересов и с опорой на международное право и соответствующие Декларации ООН.

27 сентября 2014 года, выступая на пленарном заседании 69-й сессии Генеральной Ассамблеи ООН, министр иностранных дел России Сергей Лавров предложил принять декларацию о недопустимости вмешательства во внутренние дела суверенных государств, о непризнании госпереворотов как метода смены власти. На наш взгляд, это предложение приемлемо и к цифровому пространству, к социальным сетям.

9 января 2015 г. государствами-членами ШОС в качестве официального документа ООН были внесены «Правила поведения в области обеспечения международной информационной безопасности». В документе, среди прочих предложений международному сообществу, представлены следующие:  
• Не использовать ИКТ и информационные и коммуникационные сети для вмешательства во внутренние дела других государств и в целях подрыва их политической, экономической и социальной стабильности (п. 3 Правил поведения);  
• …сдерживать распространение информации террористического, сепаратистского или экстремистского характера, а также разжигающей ненависть на национальной, расовой или религиозной почве (п. 4 Правил поведения).

Современные информационные технологии все чаще используются в агрессивных целях. В сочетании с экстремистскими, националистическими, расистскими действиями они способны дестабилизировать обстановку и устранить от власти любое правительство как в самом развитом, так и в отсталом государстве.

Сегодня ни одна страна мира не может считать себя защищенной от трансграничных информационных угроз. Информационные технологии могут стать детонатором развязывания даже межгосударственного военного конфликта. Причем для создания конфликтной ситуации требуется гораздо меньше затрат чем классическая подготовка традиционной войны. При этом не нужно создавать крупных группировок войск, концентрировать в определенных районах авиацию, артиллерию, противовоздушную оборону, подтягивать логистические подразделения и так далее.

Информационные воздействия являются бескровными, не разрушают окружающую среду и могут реализовываться через вполне мирные средства — СМИ, «Интернет», средства телекоммуникаций, информатики, связи и др. Посредством дезинформационных вбросов, публикаций и распространения экстремистских заявлений, проведения расистских или ксенофобских флэшмобов, трансграничных компьютерных атак на критически важные для жизни и деятельности общества объекты и т.п. возможно «разогреть» ситуацию в любой стране до «социального взрыва».

Подобными действиями также можно поссорить несколько государств и довести их до состояния войны. На примерах цветных революций и конфликтов последнего десятилетия можно с уверенностью сказать, что такие технологии уже достаточно хорошо обкатаны. Вопрос: где, когда и против кого они будут применены в дальнейшем?

Еще один вопрос: какое государство сегодня с полной уверенностью сможет однозначно ответить — против него эти технологии применить не возможно, потому, что оно полностью защищено?

Ответ очевиден — таких государств не существует. Еще одним аспектом борьбы в информационной сфере является быстро совершенствующееся и распространяющееся информационное оружие.

Экспертами не раз уже отмечалось, что ущерб от его использования может приводить к техногенным катастрофам на критически важных объектах промышленности, экономики, энергетики и транспорта, к финансовому коллапсу и системному экономическому кризису.

С развитием информационных технологий будет расширяться линейка информационного оружия, а также увеличиваться перечень объектов, по которым возможно его применение. Ситуацию обостряет тот факт, что данное оружие может попасть в руки террористов и криминальных структур. В этом случае последствия его применения будут не предсказуемы.

Многие эксперты сходятся во мнении, что запретить разработку такого оружия, а главное проконтролировать его наличие у государств, а тем более террористов нельзя. Но выработать механизм его нераспространения возможно.

Сегодня многим государствам стало очевидным, что пора принять универсальные правила, которые будут способствовать предотвращению использования информационных технологий для развязывания войн и вооруженных конфликтов. Например, в январе этого года такую инициативу предприняла Шанхайская организация сотрудничества, внеся в ООН проект искомых правил поведения [1].

Государства, входящие в ШОС, предлагают принять членам мирового сообщества обязательства не использовать ИКТ в целях, противоречащих поддержанию международного мира и безопасности, укреплять доверие и воздерживаться от применения силы или угрозы силой в информационном пространстве. К сожалению, некоторые страны считают иначе. По их представлениям, для поддержания мира и безопасности в информационном пространстве нужно придерживаться стратегии устрашения.

Действительно, в годы «холодной войны» взаимная угроза ядерного возмездия позволила избежать развязывания крупномасштабной войны. Однако это еще не повод для того, чтобы только на основе устрашения пытаться предотвращать конфликты, которые, как полагают на Западе, могут возникнуть в результате применения информационного оружия [2]

Считаем, что такой подход несет серьезную угрозу международной безопасности, так как он основывается на создании и демонстрации мощного военного информационного потенциала. Этот шаг неизбежно приведет к гонке информационных вооружений, грубому нарушению принципа равной безопасности и общей дестабилизации военно-политической обстановки в мире. Кроме того, российские военные эксперты полагают, что сравнение нынешнего исторического периода с ситуацией начала «холодной войны» не корректно.

Оценивая высказывания главы американского киберкомандования М. Роджерса, что «обретение США ядерной мощи … позволило снизить конфронтацию и в итоге привело к переговорам по контролю над вооружениями» [3], считаем — все было с точностью наоборот. Именно создание ядерного потенциала СССР привело к балансу сил и позволило избежать катастрофы развязывания ядерной войны, а в конечном итоге вынудило США пойти на те самые переговоры.

Что касается современной ситуации, то хочу заострить ваше внимание на следующем. Сегодня нет «холодной войны». Поэтому такие заявления М.Роджерса, как «… наши противники полны решимости контролировать свои сегменты киберпространства, красть нашу интеллектуальную собственность и дезорганизовывать работу наших ведомств» и «…у нас мало надежды, что они будут вести себя ответственно в киберпространстве» вызывают недоумение.

Пока мы наблюдали обратную картину. По свидетельствам Э.Сноудэна, США в информационном пространстве шпионят не только за противниками, но и за союзниками, и за собственными гражданами. Поэтому нам не понятны мотивы, побуждающие Соединенные Штаты опираться не на силу права, а на право силы, основанное на реализации стратегии устрашения в информационном пространстве.

Теперь мне бы хотелось высказаться на данную тему в содержательном ключе. Скажу сразу, что мы отрицательно относимся к самой идее «информационного устрашения» и скептически к ее реализуемости.

Во-первых, в отличие от ядерного оружия при применении информационных технологий не существует явной угрозы взаимного гарантированного уничтожения. Следовательно, у политического руководства сторон конфликта не будет того страха развязывания «информационной войны», который эффективно мотивирует реальность ядерного возмездия.

Во-вторых, учитывая большое количество негосударственных акторов, действующих в информационном пространстве, представляется некорректным использовать аналогию с ядерным устрашением, которое, по сути, было реализовано двумя основными ядерными державами — СССР и США. Сейчас может оказаться недостаточно одному из двух государств, обладающих сопоставимыми информационными потенциалами, убедить другое не идти на эскалацию конфликта для того, чтобы предотвратить его перехода в горячую стадию.

В-третьих, образцы информационного оружия значительно легче разработать, произвести и передать кому-бы то ни было, чем технологии ядерного оружия. Поэтому достичь убедительного превосходства над соперниками чрезвычайно трудно.

В-четвертых, источник информационной атаки в компьютерных сетях сложно установить ввиду его анонимности и комплекса специальных мер, принимаемых для «запутывания» следов. Поэтому оперативно расследовать произошедший инцидент и достоверно собрать все необходимые доказательства для совершения легитимного «акта возмездия», который будет оправдан мировым сообществом, вряд ли получится.

В-пятых, мы полагаем, что в информационном пространстве будет весьма затруднительно обеспечить баланс военных информационных потенциалов на основе достоверного знания основных характеристик системы информационного вооружения сторон.

С одной стороны, публикация сведений о разработке новых систем вооружения немедленно приведет к разработке средств и способов противодействия им, т.е. к нарушению баланса. С другой стороны, любая неконтролируемая скрытая разработка таких систем также будет нарушать искомый баланс, и дестабилизировать военно-политическую обстановку.

Хочу заметить, что пока известен единственный исторический пример, демонстрирующий мощь информационного оружия. Это атака компьютерного вируса Stuxnet на иранские ядерные объекты в Натанзе и Бушере. Можно предположить, что она замышлялась как реинкарнация ядерных бомбардировок Хиросимы и Нагасаки. Однако в результате этой атаки мир не содрогнулся, а Иран не объявил о своей капитуляции и отказе от ядерных программ. Значит, потенциал информационных вооружений пока не сопоставим с мощью ядерного оружия, а ставка на его дальнейшее наращивание в принципе ошибочна.

Если государства возьмут курс на информационное устрашение, то это приведет лишь к новому витку гонки вооружений и милитаризации информационного пространства.

Единственной разумной альтернативой этому безумию является упомянутая мирная инициатива в области международной информационной безопасности, продвигаемая в ООН государствами ШОС. Она также направлена на предотвращение информационной агрессии. Однако в отличие от стратегии устрашения основывается не на страхе возмездия, а на добровольном принятии универсальных правил поведения государств в информационном пространстве, добросовестное выполнение которых обеспечит мир, стабильность и равную безопасность всем народам в глобальном информационном пространстве.

Мы выступаем за широкое международное сотрудничество в решении глобальной проблемы противодействия угрозе развязывания информационных войн, распространения информационного оружия. При этом основной целью развития сотрудничества, по моему мнению, является установление международного правового режима обеспечения международной информационной безопасности, регулирующего, в том числе, военную деятельность государств в мировом информационном пространстве на основе принципов и норм международного права. Мы выступаем за создание механизмов двустороннего и многостороннего сотрудничества по военным аспектам международной информационной безопасности.

**Литература:**

1. Информационное противоборство в моделях и задачах, Сергей Расторгуев, 2017 год.
2. СМИ пропаганда и информационные войны, Панарин И.Н., Поколение 2012
3. Международные отношения, Дипломатическая академия, //vpk-news.ru// обращение к источнику 20.12.2018 года