ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ЭЛЕМЕНТА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СОВРЕМЕННЫХ ГИБРИДНЫХ ВОЙН

О.Л. Узун, кандидат юридических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России.
С.Л. Узун, кандидат педагогических наук.
Министерство обороны Российской Федерации

Рассмотрены проблемы правового обеспечения информационной безопасности. Предложены меры по подготовке к информационному противодействию и укреплению национальной безопасности. Акцентировано внимание на создании национальной идеи как информационно-психологического «базиса безопасности» нации.

Ключевые слова: информационная безопасность, информация, национальная безопасность, государственная идеология, право

INFORMATION SECURITY AS THE ELEMENT OF NATIONAL SECURITY
IN THE CONDITIONS OF MODERN HYBRID WARS

O.L. Uzun, Saint-Petersburg university of State fire service of EMERCOM of Russia.
S.L. Uzun. Ministry of defendce of Russian Federation

Problems of ensuring information security are considered, measures for preparation for information counteraction and strengthening of national security are offered. The attention on creation of national idea as «basis of safety» of the nation is focused.

Keywords: information security, information, national security, state ideology, law

Современную ситуацию с правом можно охарактеризовать как средневековую – «Когда говорят пушки, право молчит». Нарушение основных принципов международного права, базовых конвенций по ведению войны и защите некомбатантов, двойные стандарты в признании прав одних народов на суверенитет (Косово) и отказ другим в построении самостоятельного государства (Новороссия) ознаменовали новый этап развития цивилизации.

За прошедшее столетие очень сильно изменилась и тактика ведения войн и средства ее ведения. Революционные изменения в информационных технологиях приравняли средства массовой информации (СМИ) к средствам ведения войны. Роль информационных технологий и СМИ многократно возросла – они сделались ключевым средством достижения военно-политических целей государств. Разрушительная мощь информационно-психологического воздействия в современных условиях настолько велика, что ставит под сомнение не только независимость побежденного государства, но и сам факт существования его народов как национальной общности [1].

Впервые новые информационные технологии как средства ведения боевых действий были использованы в ходе войны в Персидском заливе в 1991 г., а термин «информационная война» (ИВ) официально стал использоваться в Директиве Министра обороны США от 21 декабря 1992 г. Распространение спутникового телевидения и связи, увеличение скорости и объемов передачи данных привели к стиранию информационных границ и глобализации информационного пространства. Это в свою очередь, приводит к возникновению военных концепций, призванных обеспечить победу в изменившихся условиях, с качественно обновленным арсеналом сил и средств борьбы [1].

События последнего десятилетия при анализе военно-политических конфликтов позволяют утверждать, что перспективы цивилизаций во многом будут определяться тем,

насколько эффективно они готовы к противоборству в информационно-психологической сфере. Основная цель войны в данной области состоит в воздействии на общественное сознание таким образом, чтобы управлять людьми, заставить противоположную сторону действовать вопреки своим интересам или в более широком смысле – обеспечить себе возможность управлять поведением общественных масс. Особое значение при этом приобретает целенаправленное использование СМИ. Это объясняется тем, что в результате воздействия, направленного на ментальное пространство нации, происходит замещение традиционных базовых ценностей общества морально-психологическими установками агрессора.

Аналогичные процессы можно наблюдать и на Украине. Украинцы давно перестали считать себя неотъемлемой частью русского мира и добровольно участвуют в евроатлантических интеграционных процессах.

Саммит G20 в ноябре 2014 г. завершился очередными инвективами Б. Обамы, А. Меркель, Д. Кэмерона, С. Харпера, политиков стран Европы, чиновников Европейского союза (ЕС) и НАТО в адрес России на тему: «Вы должны убраться из Украины!» [2].

Насчет украинских властей говорить не приходится – о градусе враждебности в отношении России свидетельствуют жестокие карательные операции против пророссийского населения Донбасса и других территорий Юго-Востока Украины, провокация с малайзийским самолетом, вброс информации о готовившихся апокалиптического масштаба провокациях на Запорожской АЭС и Днепрогэсе, крайне безответственные, но не вызвавшие адекватных оценок американских и европейских политиков заявления Министра обороны Украины о разработке украинского ядерного оружия для войны с Россией, и применении Россией тактического ядерного оружия в Новороссии, заявления А. Яценюка о вторжении СССР в Украину и молчание мирового сообщества, и многое другое. Во второй половине сентября 2014 г. в украинское информационное пространство вброшен термин «российско-террористические войска» [3].

Накал страстей вокруг России отчасти объясняется эмоциями из-за провала крымской части американского проекта. Появившаяся в июле 2014 г. в испанском интернете публикация, раскрывает одну из важнейших целей февральского государственного переворота в Киеве – ликвидация автономии Крыма, удаление из Крыма российских военных объектов и развертывание на полуострове военной инфраструктуры США уже в 2014–2015 гг. Другие источники подтверждают адекватность этой информации [3].

Информационная война (ИВ) против России ведется уже давно, всеми доступными средствами среди всех возрастных, социальных и профессиональных групп. Утверждая, что никогда еще украинцы не были столь едины, как сейчас, П. Порошенко прав, но, к сожалению, это единство – на антироссийской основе. ИВ не следует воспринимать легко – внедренный в сознание большого процента населения страны агрессивный русофобский менталитет уже находит выход в практических действиях внутри и вне Украины.

Одним из примеров является накачка информационного пространства Украины с ноября 2013 г. путем, так называемой «политтехнологии декапитации» (обезглавливания), в отношении Президента Российской Федерации В.В. Путина – тотального, без всяких сдержек и приличий, клевету в СМИ на руководителя государства, объявленного враждебным. Антипутинская кампания ведется не только в украинских, но и в достаточно широких масштабах по всей Европе, в США и других странах. Ее смысл и задача – внедрять в массовое сознание мысль о том, что лидер России и сама страна – вне закона, против них будут справедливы в ближайшем или отдаленном будущем любые действия.

Продолжая линию «нерукопожатости» 17 ноября 2014 г. после Саммита G20 вышла статья об утрате доверия В.В. Путину со стороны Запада, озвученная германским канцлером А. Меркель [2]. Данная речь уже не имела скрытого подтекста и напрямую представляла образец прямой политической угрозы для Российской Федерации и ее Президента. Кроме того, А. Меркель поставила вопрос о пересмотре энергетических соглашений с Россией

в пользу США. Теперь помимо экономической войны, авторы считают возможным говорить и об открытой ИВ против России. После реализации второстепенных целей в последующем возможен переход к фазе «холодной войны» или открытому противостоянию, которое может проходить в форме «гибридной войны» или открытого военного противостояния со всеми вытекающими последствиями. Но сначала нужно создать образ врага и подготовить общественное мнение.

Указанные события показывают, что современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [4].

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Информационный ресурс занимает особое положение в совокупности ресурсов развития. Его объекты и объединяющая их инфраструктура имеют особые пространственно-временные характеристики, не ограничиваемые пределами национальных государств. Это заметно сказывается на общей оценке потенциала того или иного геополитического субъекта, вариантов воздействия на него извне, его способности к устойчивому развитию, восприимчивости к информационному трансферу, возможности к информационному противоборству.

Доктриной информационной безопасности Российской Федерации была обозначена проблема безопасности применительно к информационной сфере, где информационная безопасность рассматривается как неотъемлемая часть национальной безопасности страны. Документ имеет базовое значение для подготовки как общегосударственных, так и специализированных, отраслевых, ведомственных программ, реализуемых в информационной сфере в соответствии с полномочиями этих органов и организаций.

Более широкое определение дает А.В. Макеев. Под «информационной безопасностью» он понимает устойчивое состояние информационной сферы, сохраняющей, несмотря на неблагоприятные внешние и внутренние воздействия, свою целостность и способность к саморазвитию на основе осознания субъектами информационного взаимодействия своих ценностей, потребностей (жизненно важных интересов) и целей развития [5].

По мнению авторов, подготовка к обеспечению безопасности личности и общества начинается с институционализации «базиса безопасности». Под «базисом безопасности» они понимают целевую концепцию (идею) общественного устройства с определенным вектором социально-психологического, политического и экономического развития, обладающую устойчивостью к информационному противодействию и адаптационным потенциалом к глобальным изменениям.

Без формирования цели существования и направления развития общества, информационного пропагандирования заявленного «базиса безопасности» невозможны скоординированные и сплоченные усилия народа и власти в противодействии внутренним

и внешним угрозам, «общество представляется рыхлым и неустойчивым, скорее больным, чем здоровым». Кроме того, национальная идея будет иммунитетом для противодействия информационной накачке общества и отдельных его групп.

Сущность безопасности любой социальной системы заключается в ее способности сохранять свою идентичность и развиваться, в том числе в условиях конфликтов и неопределенности риска и реализации этой способности в реальных условиях. Из этого вытекает важный методологический вывод – вся система обеспечения безопасности (включая информационную) должна быть направлена, прежде всего, на обеспечение развития этих адаптивных способностей. Поэтому информационную безопасность необходимо рассматривать, во-первых, как безопасность объекта с использованием информационной сферы и, во-вторых, как безопасность собственно информационной сферы [6].

Одним из ключевых, по мнению авторов, внутренних источников угроз информационной безопасности России выделяется недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений и проводимой линии, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан. Отставание России от ведущих стран мира по уровню информатизации сказывается также негативно на жизни и деятельности общества [7]. В России информационное общество только формируется [8].

Геополитическая уязвимость России становится особенно тревожной в связи с реальной угрозой утраты контроля над своим информационным пространством. Авторы убеждены, что сегодня нельзя считать удовлетворительным проведение целенаправленной национальной информационной политики в Российской Федерации, сил и средств Государственной программы «Информационное общество (2011–2020)» явно недостаточно [9, 10]. Конфликт на Украине это подтвердил.

Военные доктрины развитых стран Запада постепенно трансформируются в направлении отказа от тотальной войны и переориентации военного искусства на стратегию «непрямых действий», «гибридной войны» в которых информационное противодействие, основанное на контроле и использовании информации и направленное для достижения информационного превосходства над противником играет особую роль.

Применение средств ИВ отражается не столько на ведении военных действий, сколько на иных, не боевых воздействиях: либо на сдерживании противника от активных боевых действий, либо на достижении победы «без единого выстрела» над умело деморализованным и дезинформированным противником. Этот аспект применения средств ИВ изучен, пока в наименьшей степени. В целом все формы ИВ сводятся к воздействию на инфраструктуру противника, его информационные системы и информационные ресурсы с целью искажения получаемой информации, лишения его возможности получения новой информации или физического уничтожения его информационных средств, а также защите собственных информационных систем и информационных ресурсов от аналогичных действий противника. В настоящее время в более чем 120 странах осуществляются работы по национальным программам ИВ, и здесь мы не должны отставать.

Сегодня для России, как никогда, остро стоит вопрос о выработке мер модернизации национально экономики, подготовки общества к новым вызовам глобальных перемен, преодоления состояния социальной дезинтеграции и стагнации на основе государственной идеи построения нового справедливого общества равных прав и возможностей. Только новая программа индустриализации и модернизации российского общества и государства, позволит встретить новые кризисы подготовленными и сплоченными.

Литература

1. Бобров А. Информационная война: от листовки до Твиттера // Зарубежное военное обозрение. 2013. № 1. С. 20–27.

2. Simon Shuster. Putin’s Loss of German Trust Seals the West’s Isolation of Russia. 2014. Nov. 17. URL: http://time.com/3590588/putin-merkel-germany-russia/ (дата обращения: 21.12.2014).

3. Виноградов И. Геополитика нового мирового порядка // URL:http://www.riss.ru/analitika/3758-geopolitika-novogo-mirovogo-poryadka#.VGxmW8ngVI1 (дата обращения: 22.12.2014).

4. Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации 9 сент. 2000 г. № Пр-1895) // Рос. газ. 2000. 28 сент. № 187.

5. Макеев А.В. Основы политики национальной безопасности: структурогенез и механизм реализации: автореф. ... канд. полит. наук. М.: Изд-во МГУ, 1999.

6. Стратегические факторы риска для России. М., 1996.

7. Першин А.А. Информационное взаимодействие государства и общества. URL:http://www.lawinrussia.ru/node/308148 (дата обращения: 22.12.2014).

8. Стратегия развития информационного общества в Российской Федерации (утв. Президентом Рос. Федерации 7 февр. 2008 г. № Пр-212) // Рос. газ. 2008. 16 фев. № 34.

9. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. (утв. Президентом Рос. Федерации В.В. Путиным 24 июля 2013 г., № Пр-1753).

10. О государственной программе Российской Федерации «Информационное общество (2011–2020 гг.): Распоряжение Правительства Рос. Федерации от 20 окт. 2010 г. № 1815 // Собр. законодательства Рос. Федерации. 2010. 15 нояб. № 46. Ст. 6026.