ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЕК ГЛОБАЛИЗАЦИИ

Крылова И. А.[*]

Статья посвящена проблеме обеспечения информационной безопасности в век глобализации, а также анализу информационных войн, которые являются частью современной информационной реальности. Выявлена специфика информационно-технической войны, кибервойн; информационно-психологической войны (и ее связь с «цветными революциями»); технологий «управляемого хаоса». Сделан вывод о необходимости выработки универсального международно-правового документа, касающегося возникновения новых угроз в сфере информационной безопасности. Показано, что в условиях дальнейшего ужесточения антироссийских санкций и потенциальной угрозы отключения Российской Федерации от Интернета необходимо создавать независимый Рунет, форсировать развитие отечественных информационных технологий, чтобы не быть зависимыми от Запада. Иначе говоря, совершенствовать систему обеспечения информационной безопасности России.

Ключевые слова: *век глобализации, информационное общество, информационно-техническая война, кибервойна, информационно-психологическая война, «цветная революция», «управляемый хаос», информационная безопасность, кибербезопасность, национальная безопасность.*

The article is devoted to the problem of ensuring information security in the age of globalization, as well as the analysis of information wars, which are the part of the modern information reality. The author defines peculiar features of information-technical warfare, cyber wars; information-psychological war (and its connection with 'color revolutions'); technology of 'controlled chaos'. The conclusion is made about the necessity to develop a universal international legal document touching the emerging threats in the field of information security. It is shown that in the situation of further tightening of anti-Russian sanctions and the potential threat of the Russian Federation being 'cut off' the Internet, it is necessary to create an independent Runet and speed up the development of domestic information technologies (to be independent from the West); in other words, to improve Russia's information security system.

Keywords: *age of globalization, information society, information-technical war, cyber war, information-psychological war, 'color revolution', 'controlled chaos', information security, cyber security, national security.*

В век глобализации на основе развертывания информационной и телекоммуникационной революции происходит формирование глобального (планетарного) информационного общества, то есть объединение человечества фактически

[*] Крылова Ирина Анатольевна – д. ф. н., ведущий научный сотрудник Института философии РАН. E-mail: tatyanawings@gmail.com.

в «сверхобщество» с более высоким уровнем социальной интеграции. Глобальная информатизация (электронные средства массовой коммуникации: радио, телевидение, Интернет), как и глобальная компьютеризация современного общества (когда все большее количество людей во всем мире включается в использование новых технологий, а массовое сознание «перемещается» в интернет-пространство), позволяет назвать XXI век информационным.

Приходится констатировать, однако, что современное глобальное информационное пространство представляет собой объект ожесточенной борьбы за информационное превосходство, политические, экономические и сырьевые преимущества, арену постоянного противоборства различных социальных структур. Причем в современных условиях наблюдается тенденция перехода от традиционных – силовых – методов борьбы государств при отстаивании своих национальных интересов к нетрадиционным, в частности информационным средствам воздействия на противника. «Традиционное вооружение и военная техника все более становятся фактором сдерживания, – подчеркивает В. К. Потехин, – реальным же оружием все больше выступают информация и информационные технологии – **информационное оружие**» [Потехин 1999: 69]. Фактически речь идет о новом феномене глобализации – **информационной войне**, которая становится, по существу, новой формой противостояния государств, одним из видов «нетрадиционных» войн нового поколения. Поэтому в условиях стремительного формирования глобального информационного пространства (а также киберпространства) огромное значение в обеспечении национальной безопасности всех стран приобретает информационная безопасность.

Информационные войны являются частью нынешней информационной реальности. В век глобализации они представляют собой эффективное средство достижения превосходства в различных сферах жизни современного общества: политической, экономической, научно-технической, военной, социальной, духовной. Информационная война – это противостояние борющихся сторон, которые оказывают агрессивное воздействие на информационную инфраструктуру друг друга с целью достижения преимущества и победы над противником. Различают информационно-техническую и информационно-психологическую войну.

Информационно-техническая война представляет собой противоборство государств в военной информационной сфере. По существу, это разновидность военных действий, в которых основным объектом является информация. Главная цель такой войны заключается в информационном воздействии, которое позволяет без традиционных военных действий добиться победы над противником. «На арену выдвигается новый тип вооружений, – подчеркивает В. К. Потехин, – средства РЭБ, СВЧ-генераторы, информационные вирусы, электронные ловушки, компьютерные “закладки”, программы двойного назначения, интеллектуальные программные системы, голосовые синтезаторы, искусственные изображения в атмосфере…» [Там же: 70]. Информационное воздействие может быть направлено не только на нарушение работы компьютерных центров и сетей связи, ликвидацию главных штабов противника и психологическое подавление его армии, но и на разрушение инфраструктуры систем жизнеобеспечения и жизнедеятельности общества, что приводит к полной дезорганизации управления государством и дезориентации населения побежденной страны.

Как известно, впервые новое средство информационного воздействия, а именно телевидение, было применено США на население всей страны в ходе войны во Вьетнаме. В конце XX – XXI в. широкое применение информационного оружия во многих военных конфликтах и войнах – в Гренаде, Панаме, Ираке, Югославии, Ливии, Сирии – показало, что разрушение не только военной, но и гражданской инфраструктуры заставляет побежденное государство в конечном счете прекратить военные действия и принять любые кабальные условия нападающей стороны. Это сделало очевидным тот факт, что информационно-техническая война представляет новую угрозу национальной безопасности суверенных государств в XXI в.

В настоящее время путем пролонгирования и ужесточения антироссийских санкций сознательно создаются условия для зависимости России в сфере новейших информационных технологий. При этом преследуется цель увеличения технологического отрыва стран первого мира, а также наращивания их возможностей для противодействия созданию в России конкурентоспособных информационных технологий. Поэтому в связи с возросшей угрозой применения информационного оружия против российской информационной инфраструктуры одной из первостепенных задач является обеспечение технологической независимости Российской Федерации, прежде всего в тех областях информатизации, телекоммуникации и связи, которые отвечают за национальную безопасность страны.

В век глобализации киберпространство также является ареной острейшего противоборства между различными государствами и коалициями стран. В условиях стремительного формирования глобального киберпространства большинством развитых стран мира создаются специальные кибервойска для ведения войн, основанных на использовании компьютерных сетей в военных целях. Речь идет фактически о **кибервойне**. Иначе говоря, о воздействии страны-агрессора на компьютерные сети другого государства, что делает последнее совершенно неспособным оказать сопротивление противнику.

В настоящее время кибератакам подвергается большинство стран мира, и ущерб от них в целом оценивается в 0,5 млрд долларов. Что касается России, то сайты президента РФ, Государственной Думы и Совета Федерации постоянно подвергаются кибернападениям (до 10 тысяч кибератак в день) [Капто 2013: 618]. Не являются исключением и США, которые до недавнего времени доминировали в киберпространстве. Причем угроза кибератак и кибервойн в мире только нарастает. Ныне вести масштабную кибервойну способны уже более 100 государств. В связи с нарастающей угрозой кибервойн возникает задача выработки международно-правового документа по кибербезопасности на уровне ООН. В век глобализации умение вести противоборство в киберпространстве в значительной степени обеспечивает информационную безопасность и суверенитет страны. «Уровень информационной безопасности государства, – подчеркивает А. А. Кокошин, – во многом зависит от степени развития национальной электронно-компонентной базы, от наличия в стране собственных решений в области программирования, от уровня развития криптографии, от системы организации информационного противоборства» [Кокошин 2014: 1096]. Поэтому во всех развитых странах придается такое огромное значение разработке новейших информационных технологий для отражения кибератак и предотвращения кибервойн,

а также подготовке высококвалифицированных специалистов в сфере обеспечения кибербезопасности.

Под **информационно-психологической войной** понимается информационное воздействие на сознание человека. Информационно-психологическое оружие направлено на «переформатирование» сознания людей (путем внедрения чуждых ценностей, традиций и культуры), а через него – на изменение существующей социально-политической системы. Диапазон информационно-психологического оружия чрезвычайно широк – от сокрытия важной информации и ее искажения до полной дезинформации населения. Опасность нового вида оружия заключается в том, что его воздействие приводит в конечном счете к кардинальной трансформации общественного сознания, влечет за собой социальный взрыв и свержение неугодного политического лидера или режима в стране-объекте. Таким образом, достижение победы над противником происходит без традиционных военных действий. Главным же является то, что страна-агрессор получает огромную выгоду в политической, экономической, финансовой, научно-технической, военной и других сферах побежденного государства, которое становится «страной-донором» и на долгое время попадает под внешнее управление. Именно так уничтожили СССР. В то время как Советский Союз наращивал оборонный потенциал для обеспечения национальной безопасности государства, Запад, преследуя свои геополитические цели, не применяя военную силу, победил советскую сверхдержаву, «взорвав» ее изнутри. В результате в России была разрушена промышленность, уничтожено сельское хозяйство, подорван научный и военный потенциал, что значительно ослабило национальную безопасность страны. Крах СССР наглядно показал, что информационно-психологическая война, в которой используются информация, информационные ресурсы и информационные технологии, представляет собой не менее разрушительное оружие, чем традиционное. Поэтому многие страны принимают жесткие меры для защиты своих духовных ценностей, традиций и культуры, а также национальных информационных ресурсов от чуждой информационной экспансии.

Что касается России, то в последние годы, особенно после воссоединения Крыма с Российской Федерацией, США и Евросоюз ведут против нашей страны агрессивную информационно-психологическую войну. Причем в своем информационном противоборстве с Россией эти страны, кроме собственных средств массовой информации, используют не только силы, которые они «проплачивают» внутри нашей страны (русофобские СМИ, несистемную оппозицию, другие организации), но также антироссийски настроенные политические элиты и СМИ ряда соседних и европейских государств (Украины, Грузии, Литвы, Латвии, Эстонии и Польши). Главной целью этой информационно-психологической войны для США и стран НАТО является свержение существующего «режима Путина» и ослабление российского государства. Поэтому западные СМИ пытаются не только испортить репутацию России за рубежом, представить нашу страну отсталой, тиранической и агрессивной, но также демонизировать президента Российской Федерации. При этом информационно-психологическое воздействие направлено на население как России, так и других государств. В этих условиях информационную контратаку против западной дезинформации успешно ведет отечественный стратегически наступательный канал *Russia Today*.

В век глобализации к новым формам ведения информационно-психологических войн относятся и так называемые консциентальные войны. Основным оружием таких войн является дезинформация населения, которая осуществляется через различные средства массовой информации, радио, телевидение и Интернет. «Под консциентальной войной, – пишет В. К. Потехин, – мы понимаем войну психологическую по форме, цивилизационную по содержанию и информационную по средствам, в которой объектом разрушения и преобразования являются ценностные установки народонаселения противника» [Потехин 1999: 66]. Исходя из того, что ценностные и целеполагающие установки человека тесно связаны с культурой народа, являющейся основой той или иной цивилизации, главной целью в консциентальной войне предстает уничтожение культуры противника, а значит, разрушение другой цивилизации. Сегодня угрозу информационной безопасности России представляет пропаганда образцов массовой культуры и ценностей, чуждых традиционным духовным и нравственным ценностям, принятым в нашем обществе. Представляется, что в век глобализации надежной защитой от манипулирования индивидуальным, групповым и массовым сознанием может стать общее повышение информационной культуры как необходимое условие существования социума в информационном обществе.

Надо сказать, что многочисленные **«цветные революции»**, происходящие ныне в тех или иных странах, также являются результатом современных информационно-психологических войн. В век глобализации США и странами НАТО все чаще инициируются протестные социальные движения в суверенных национальных государствах путем информационно-психологического воздействия на массовое сознание (с целью насаждения западной демократии и европейских ценностей) для свержения неугодных политических режимов и лидеров. «Проблема “цветных революций” значительно актуализировалась в контексте глобального финансово-экономического кризиса (который далеко не закончен), – считает А. С. Брычков, – что связано с борьбой за ограниченные ресурсы планеты и дает шансы выйти из него с наименьшими издержками тем государствам, которые поставят чужую ресурсную базу под свой контроль» [Брычков 2018: 118]. Подготовленные США и Западом «цветные революции» в ряде бывших советских республик (Украине, Грузии, Киргизии), направленные на «взрыв» государства изнутри, показали, что они являются мощным инструментом информационно-психологической войны, которая заставляет население стран-объектов совершать действия, в действительности противоречащие их убеждениям и потребностям.

Наиболее наглядным примером такого воздействия «мягкой силы» и информационно-психологической войны является Украина. Преследуя свои национальные интересы, США вложили в сферу «переформатирования» массового сознания украинцев всего 5 млрд долларов (по сравнению с Российской Федерацией, оказавшей за прошедшие годы экономическую помощь в размере более 200 млрд долларов), что привело в конечном счете к предательству национальных элит, свержению законной власти, гражданской войне, превращению братской страны во враждебную России, которая стремится ныне вступить в НАТО и Евросоюз. В свое время о необходимости полного выведения Украины из сферы влияния России писал еще З. Бжезинский в книге «Великая шахматная доска», так как был убежден, что без Украины невозможно восстановление мощи Российской импе-

рии, то есть территориального и государственного единства страны. Сейчас США и страны Евросоюза воплощают рекомендации З. Бжезинского по Украине на практике.

В настоящее время США предпринимают попытку инициировать «цветную революцию» в Венесуэле, чтобы свергнуть законного президента Николаса Мадуро. Вполне вероятно, что в случае провала «невоенного» сценария он будет дополнен традиционно военным вмешательством. Следует учитывать, что на Западе давно вынашивается идея подготовки «цветной революции» и в России. При этом не скрывается, что главной целью введения и ужесточения антироссийских санкций является ухудшение социально-экономической обстановки, снижение уровня жизни населения, провоцирование социального недовольства для смены политического руководства и дальнейшего распада нашей страны на «осколочные» государства.

Трансформация массового сознания и мировоззрения противника с использованием новейших информационных технологий положена и в основу **концепции «управляемого хаоса»**, направленной на сокращение численности населения на планете, а также разрушение национальных государств для постановки под контроль ТНК их ресурсов. В этом смысле чрезвычайный интерес представляет точка зрения В. Е. Лепского, который считает организацию «управляемого хаоса» в национальных экономиках и социальной сфере различных стран новой мировой информационно-психологической войной. «Технологии управляемого хаоса, – подчеркивает он, – это новый неконтролируемый в настоящее время международными организациями вид оружия массового поражения для установления мирового порядка в интересах стороны, его применяющей» [Лепский 2016: 104]. Целью технологий «управляемого хаоса» является разрушение экономик национальных государств путем захвата управления в конкретных странах-объектах и блокирования в них способности к инновационному развитию, которое в условиях глобальной конкуренции представляет главный фактор сохранения политического суверенитета. То есть, по существу, технологии «управляемого хаоса» ведут к новой форме неоколониализма, который превращает страны-объекты в придаток «избранных» государств. «Главной особенностью, отличающей неоколониализм от традиционного колониализма, – пишет А. А. Горелов, – является то, что управляют страной представители коренной нации, составляющие правящую элиту, но управляет она, как и при колониализме, в интересах метрополии» [Горелов 2013: 69]. В конечном счете такое управление приводит к утрате неоколониальными странами политического суверенитета, деградации экономики, демографической катастрофе, деморализации и деградации вооруженных сил, разрушению традиционных ценностей, традиций и культуры.

Технологии «управляемого хаоса» направлены на организацию «бессубъектности» развития в таких неоколониальных странах. Следует констатировать, что после разрушения СССР к России также были применены подобные технологии. В результате сформировалась бессубъектность развития, прежде всего инновационного (что наблюдается и поныне, несмотря на провозглашенный высшим политическим руководством страны курс на технологический прорыв), представляя реальную угрозу национальной безопасности Российской Федерации. Практика показала, что катастрофичность последствий использования технологий «управ-

ляемого хаоса» в ряде национальных государств сопоставима с применением оружия массового уничтожения. Отсюда следует, что такие технологии должны быть запрещены на уровне ООН, поскольку их применение нарушает международные нормы о невмешательстве во внутренние дела суверенных государств. Фактически речь идет о необходимости международно-правового регулирования в сфере использования технологий «управляемого хаоса», инициатором которого могла бы стать Российская Федерация.

В век глобализации от надежности обеспечения информационной безопасности зависит национальная безопасность суверенных государств. Причем в ходе научно-технического прогресса и информационной революции эта зависимость будет только возрастать. Следует отметить, что за последнее время в России был реализован широкий комплекс мер по совершенствованию системы обеспечения информационной безопасности. Однако известно, что в ряде стран не только ведется интенсивная разработка различных концепций информационных войн, но также создаются особые средства опасного воздействия на информационную инфраструктуру других государств, способные нарушить работу информационных и телекоммуникационных систем для получения свободного доступа к их информационным ресурсам. В частности, США продолжают разработку новых проектов воздействия на информационную инфраструктуру Российской Федерации, а также ведения информационно-технической войны, кибервойн, информационно-психологической войны, провоцирования «цветных революций», применения технологий «управляемого хаоса» против нашей страны. Поэтому в условиях дальнейшего ужесточения антироссийских санкций и потенциальной угрозы отключения России от Интернета необходимо создавать независимый Рунет, форсировать развитие отечественных информационных технологий, чтобы не быть зависимыми от Запада. Иначе говоря, совершенствовать систему информационной безопасности для обеспечения суверенитета России.

Литература

Брычков А. С. «Цветные революции» в России: возможность и действительность // Россия в условиях изменяющегося мира: философия осмысления и перспективы будущего. М. : Проспект, 2018. С. 115–122.

Горелов А. А. Глобальный неоколониализм: государство и инволюция // Глобальные тенденции развития мира: материалы Всероссийской научной конференции, 14 июня 2012 г. М. : Научный эксперт, 2013. С. 69–82.

Капто А. С. Кибервойна: генезис и доктринальные очертания // Вестник РАН. 2013. № 7. С. 616–625.

Кокошин А. А. Обеспечение реального суверенитета России в современном мире // Вестник РАН. 2014. Т. 84. № 12. С. 1090–1097.

Лепский В. Е. Технологии управления в информационных войнах (от классики к постнеклассике). М. : Когито-Центр, 2016.

Потехин В. К. Национальная безопасность: информационная компонента в современных войнах // Безопасность. 1999. № 5–6. С. 63–74.