УДК 122/129
DOI 10.23683/2227-8656.2019.2.8

ИНФОРМАЦИОННЫЕ УГРОЗЫ ВОЕННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ ПРОЦЕССОВ

INFORMATION THREATS TO MILITARY SECURITY OF RUSSIA IN TERMS OF MODERN GEOPOLITICAL PROCESSES

Медяник Игорь Анатольевич
Начальник факультета военного обучения,
Южно-Российский государственный
политехнический университет (НПИ)
имени М.И. Платова,
г. Новочеркасск, Россия,
e-mail: gmu-npi@yandex.ru

Igor A. Medyanik
Head of the Faculty
of Military Training,
South-Russian State
Polytechnic University,
Novocherkassk, Russia,
e-mail: gmu-npi@yandex.ru

Статья посвящена анализу информационных угроз военной безопасности России, обусловленных геополитическими процессами современного мира. Характеризуя возможности новых информационных технологий, автором отмечается, что в условиях информационной реальности современное геополитическое противоборство осуществляется уже не столько вооруженными способами, сколько посредством технологий «мягкой силы». Это определяет необходимость расширения системы военной безопасности России с учетом переноса геополитического противоборства из вооруженных форм в информационную сферу.

The article is devoted to the analysis of information threats to the military security of Russia, caused by the geopolitical processes of the modern world. Describing the capabilities of new information technologies, the author notes that in the conditions of informational reality, the modern geopolitical confrontation is carried out not so much by armed means, as by means of “soft power” technologies. This determines the need to expand the military security system of Russia, taking into account the transfer of geopolitical confrontation from the armed forms to the information sphere.

Ключевые слова: военная безопасность; информационная реальность; геополитическое противоборство; информационная война; киберпреступность; информационная безопасность; технологии «мягкой силы»; духовная безопасность.

Keywords: military security; information reality; geopolitical confrontation; information war; cybercrime; information security; "soft power" technologies; spiritual security.

Введение

В современном мире происходят кардинальные геополитические процессы, порождающие новые угрозы военной безопасности России. Специфика этих процессов заключается в разрушении биполярного мира; увеличении численности локальных вооруженных конфликтов, участниками которых являются как государства, так и негосударственные акторы; развитии финансовой, экономической, технологической взаимозависимости государств; снижении роли международных институтов обеспечения безопасности в современном мире. Политическая нестабильность глобального мира несет новые риски и угрозы для системы военной безопасности государств.

В условиях новой информационной реальности современное геополитическое противоборство осуществляется уже не столько вооруженными способами, сколько посредством технологий «мягкой силы» (soft power). Все это способно нанести существенный урон военной безопасности страны без очевидного вооруженного конфликта. Понимание этого заставляет пересматривать систему военной безопасности современных государств. Сегодня происходит перенос геополитического противоборства из вооруженных форм в информационную сферу, что определяет необходимость исследования информационных угроз военной безопасности России.

Специфика и риски новой информационной реальности

Стремительное развитие информационных технологий изменяет сегодня практически все сферы общественной жизни, в том числе и военную. Вследствие этого большое значение приобретает проблема появления новых информационных угроз и способов их предотвращения.

Развитие современных информационных технологий привело к формированию новой модели социальной реальности, получившей название «информационное общество». Современные исследователи рассматривают информационное общество как определенный этап эволюционного развития цивилизации, в котором огромную роль начинают играть информация и знания, становясь ключевыми факторами производства и экономического развития стран (Bell, 1973; Toffler, 1990).

Очевидно, что нынешний этап общественного развития характеризуется высоким статусом информации, которая из фактора воздействия на технологическое развитие общества стала по сути основой производства нового знания и ключевой детерминантой общественной эволюции (Полякова, 2013). В силу этого современная цивилизация становится технократической, что приводит к снижению гуманистической составляющей общественного развития.

Стремительный рост локальных конфликтов на этнорелигиозной основе, активизация экстремистских организаций, новый виток холодной войны – все это свидетельствует о расширении пространства рискогенности современной цивилизации (Самыгин, 2014; Бедрик, 2018). Информационные технологии в наращивании рисков и угроз безопасности современного человечества играют на современном этапе далеко не последнюю роль, поскольку в настоящее время пропаганда экстремизма, войны и других агрессивных явлений перенеслась в информационное пространство, преимущественно в сеть Интернет, и контролировать этот процесс практически невозможно. Порожденное самим обществом информационное пространство становится пространством рисков, в которое попадают все социальные сферы, социальные группы, индивиды, народы, государства.

Таким образом, современное информационное пространство становится источником угроз информационной безопасности, под которой ученые предлагают понимать «состояние защищённости данных, при котором обеспечиваются их конфиденциальность, доступность и целостность, а также… комплекс мер, связанных с достижением этого состояния» (Самыгин, 2015. С. 460).

Риски, возникшие в мире в результате развития информационных технологий, не могли не затронуть сферу военной безопасности России. Россия, которая также включена в интенсивный процесс формирования информационного общества, хотя и в меньшей степени, нежели другие экономически развитые страны, уже испытывает на себе негативное влияние информатизации, охватившей все социальные сферы, в том числе и военную.

Российские исследователи, анализируя динамику изменения в военных доктринах передовых стран, пришли к выводу, что во второй половины XX в. в борьбе с противником ставка начала делаться на минимизацию собственных потерь: объектом военного воздействия является личный состав армии противника, в то время как его территория должна сохраниться для дальнейшей экономической деятельности победителя. Наиболее эффективно поставленную задачу решала информационная война (Подвигайло, 2015). При минимальных экономи-

ческих затратах разрушительный эффект информационного воздействия, осуществляемый посредством СМИ и Интернета, вполне сопоставим с последствием применения оружия массового поражения, но без негативного влияния для окружающей среды. Тщательно отфильтрованная и определенным образом поданная информация проникает в сознание населения государства-противника, детерминируя выгодные организатору информационной войны общественные движения, провоцируя протесты, конфликты, политическую дестабилизацию и социальный хаос.

Впервые термин «информационная война» был использован американскими военными при описании операции «Буря в пустыне». Считается, что итоги войны в Персидском заливе во многом были определены глобальным и комплексным применением средств и сил информационно-психологического воздействия на иракское общество, что предопределило успех военной операции США.

Обобщив опыт последних военных операций, американские военные теоретики в 90-е гг. XX в. сформулировали понятие современной информационной войны, определив ее как «использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс» (Требин, 2005. С. 399).

Анализируя возможности современных информационных технологий в военном противоборстве, специалисты выделили следующие черты информационной войны: добывание разведывательной информации, дезинформация противника, психологическое воздействие, уничтожение информационных ресурсов врага, внедрение компьютерных вирусов в информационные системы. Такое понимание информационной войны позволяет говорить о появлении в современном мире новых способов нанесения ущерба противнику и достижения стратегических целей.

В условиях новых информационных технологий объектами информационной войны выступают «властные, управленческие, информационные системы, вооруженные силы, процессы принятия решений, сознание населения, общественное мнение, важная инфраструктура» (Манойло, 2012. С. 27). Таким образом, информационная война охватывает широкий спектр объектов воздействия, что более эффективно, чем только вооруженные способы борьбы.

Современные информационные угрозы военной безопасности России

Новые информационные технологии обладают реальными возможностями для создания угроз и нанесения ущерба национальной безопасности государств. Отечественные специалисты отмечают, что сегодня «основная озабоченность в сфере обеспечения информационной безопасности связана с возможностью применения информационно-коммуникационных технологий (ИКТ) в целях, несовместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами здесь видятся враждебное использование ИКТ на уровне государств против информационных инфраструктур в политических и военных целях, преступная и террористическая деятельность в киберпространстве» (Крутских, 2007. С. 28).

Практика показывает, что современные информационные угрозы подразделяются на информационно-технические и информационно-психологические.

Угрозы информационно-технического характера включают негативное воздействие на системы связи, радиоэлектронные средства, компьютерные сети и т. д. В этом случае система военной безопасности должна постоянно совершенствовать свой технологический потенциал защиты, способный противодействовать такого рода угрозам. В настоящее время через сеть Интернет можно нарушить работу информационных сетей практически любого государства. В частности, в США были проведены эксперименты под руководством Агентства информационной безопасности Министерства обороны, которые показали, что «степень уязвимости компьютерных систем и баз данных военного ведомства США достаточно высока. Проникнуть в мозговой центр Пентагона, оказывается, несложно, т.к. он имеет множество различных выходов в другие информационные системы как внутри государства, так и за его пределами» (Кучерявый, 2013. С. 91–92). В настоящее время роль сети Интернет в функционировании современных государств «настолько велика, что малейшее посягательство на ее неприкосновенность расценивается как жизненная угроза безопасности страны» (Ноговицын, 2004. С. 115).

В некоторых случаях угрозы информационно-технологического характера могут быть вызваны внешним политико-экономическим давлением на то или иное государство. Так, угрозой информационно-технологического характера является вытеснение российских компаний с мирового рынка информационных технологий, что существенно затрудняет технологическое развитие страны. Сегодня «доля России

на мировом рынке электронной техники и компонентов составляет не более 0,1–0,3 %, доля России на мировом рынке информационных услуг составляет приблизительно 0,2 %. Вклад ИКТ в экономический рост России заметно ниже (приблизительно в три раза!) соответствующих показателей развитых стран… при этом основная часть оборудования, его материальной базы и программных продуктов производятся за рубежом и там закупаются» (Кузнецов, 2013. С. 251).

Сложившаяся ситуация, особенно в условиях экономических санкций против России, является препятствием для дальнейшей информатизации страны и угрозой военной безопасности, поскольку возникают проблемы с приобретением компьютерных программ, способных эффективно противостоять гибридным войнам в информационном пространстве.

Очевидно, что угрозы в информационной сфере не ограничены исключительно информационно-технологическими аспектами, включая и информационно-психологический фактор, в частности воздействие на психику личного состава вооруженных сил, массовое сознание, на систему формирования общественного мнения и принятия решений. Как следствие, в научной литературе к информационным угрозам относят воздействия более широкого генеза: «действия стран, преступных и террористических групп с целью ущемления национальных интересов России, нарушения конституционного строя, подрыва идеологических устоев, подмены ценностей российского общества» (Лопатин, 2008. С. 51).

В исследованиях информационные угрозы на основе источников возникновения подразделяются на внутренние и внешние.

Внутренние угрозы связаны с киберпреступностью в сфере ИКТ, которая способна нанести урон экономической, финансовой и военной безопасности страны. Как отмечают специалисты, «в наши дни преступность в Интернете стала неотъемлемой частью социума, который пользуется виртуальным миром» (Крошилин, 2011. С. 49). Информационные данные в компьютерных системах постоянно подвергаются хакерским атакам. Сегодня отмечается «появление их новых форм – кибершпионаж, хищение информации у производителей SIM-карт, киберкражи у банков и т. д.» (Казарин, 2016. С. 61).

Внешние угрозы заключаются в навязывании посредством глобальных информационных сетей чуждых ценностных систем, прежде всего идеологии либерализма; искажении информации – вплоть до заведомо ложной – для психологического подавления сопротивления противника и пр. Так, разрушение советской системы ценностей привело к возникнове-

нию в общественном сознании духовного вакуума, который начал интенсивно заполнялся либеральными идеями, идущими с Запада, в том числе в форме массовой культуры.

К ключевым информационным угрозам духовной безопасности российского общества исследователи относят разрушение традиционных культурных институтов (семья, образование); распространение западной потребительской культуры; атомизацию и фрагментацию общества; девальвацию достижений советского периода; фальсификацию истории; криминализацию общества, снижение уровня образованности, воспитанности и духовности; рост социального неравенства и социальной поляризации (Павлова, 2013).

Духовный потенциал российского общества является одним из факторов обеспечения военной безопасности страны, так как духовное здоровье нации выступает основой эффективного функционирования политической, экономической, социальной сфер жизни страны.

Кроме того, военная безопасность страны опирается на морально-психологическое состояние личного состава (воинских коллективов), которое проявляется в таких явлениях, как патриотизм, моральный дух, воинская и офицерская честь и т. д. Эти моральные ценности формируются на основе уже сложившейся у граждан страны системы духовных ценностей. В условиях новой информационной реальности «уничтожение духовной самобытности и морального духа противника делает возможным достижение экономических, политических и иных целей без масштабного привлечения вооруженных сил и долгих дипломатических процедур» (Кочетков, 2015. С. 264). Все это свидетельствует о том, что сегодня происходит переход геополитического противоборства из вооруженных форм в информационную сферу.

Заключение

Анализ специфики информационных угроз военной безопасности России, обусловленных новым витком геополитического противоборства в мире, позволяет сделать вывод о том, что сегодня понятие силы не сводится исключительно к военной мощи страны. Более того, доктрины массированного возмездия, гибкого реагирования, ядерного сдерживания утрачивают свою актуальность.

Современное геополитическое противоборство осуществляется уже не столько вооруженными способами, сколько посредством технологий, получивших название «мягкой силы» (soft power). Распространение последних обусловлено развитием информационных средств, кардинально изменивших социальную реальность. Суть технологий «мягкой силы»

очень точно сформулировал Дж. Най. Под soft power профессор Гарвардского университета понимает «способность государства (союза, коалиции) достичь желаемых результатов в международных делах через убеждение (притяжение), а не подавление (навязывание, насилие, принуждение)» (Nye, 2004. P. 143). Однако «мягкая сила» используется не только для разрешения конфликтов путем дипломатии, убеждения, апелляции к международному праву, она также может быть направлена на разрушение институциональной среды неугодного государства, его культурной матрицы, разжигание межэтнической вражды, использование экономических санкций против страны и т. д. Все это способно нанести существенный урон военной безопасности страны без очевидного вооруженного конфликта. Понимание этого заставляет пересматривать систему военной безопасности современных государств, в том числе и России, поскольку сегодня происходит перенос межгосударственного противоборства из вооруженных форм в информационную сферу, что позволяет говорить об информационной войне как наиболее актуальном виде боевых действий.

Таким образом, сегодняшняя информационная реальность несет новые вызовы и угрозы военной безопасности государств, связанные с развитием технологий «мягкой силы», включающих распространение посредством глобальных коммуникационных сетей ценностей западной цивилизации, формирование имиджа современных государств в международной системе отношений, реализацию технологий управляемого хаоса и осуществление «цветных революций», целью которых является свержение неугодных США и их союзникам политических режимов в различных регионах мира.

Литература

Бедрик А.В., Зарбалиев В.З. Факторы распространения молодежного экстремизма на Юге России на современном этапе // Caucasian Science Bridge. 2018. 1(1). С. 38–50.

Казарин О.В., Скиба В.Ю., Шарянов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1 (3). С. 54–72.

Кочетков В.В. Культурное измерение гибридных войн // Вестник Московского университета. Серия 18 : Социология и политология. 2015. № 4. С. 263–267.

References

Bedrik, A.V., Zarbaliev, V.Z. (2018). Factors of the spread of youth extremism in the south of Russia at the present stage. *Caucasian Science Bridge*, 1(1), 38-50. (in Russian).

Kazarin, O.V., Skiba, V.Yu., Sharyapov, R.A. (2016). New types of threats to international information security. *Vestnik RGGU. Dokumentovedenie I arkhivovedenie. Informatika. Zashchita informatsii I informatsionnaya bezopasnost',* 1 (3), 54-72. (in Russian).

Kochetkov, V.V. (2015). Cultural Dimension of Hybrid Wars. *Vestnik Moskovskogo universiteta. Seriya 18: Sotsiologiya I politologiya,* 4, 263-267. (in Russian).

Крошилин С.В. Информационные войны на микро- и макроуровне и их влияние на экономическую безопасность // Национальные интересы: приоритеты и безопасность. 2011. № 7 (100). С. 73–77.

Крутских А. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 1. С. 28–37.

Кузнецов Ю.А., Маркова С.Е. Анализ качественных особенностей динамики развития российского рынка ИКТ. Структурный подход // Труды Нижегородского государственного техн. ун-та им. Р.Е. Алексеева. Экономика, инновации и менеджмент. 2013. № 3 (100). С. 242–252.

Кучерявый М. Глобальное информационное общество и проблемы безопасности // Власть. 2013. № 9. С. 91–92.

Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2008. № 2. С. 51–57.

Манойло А.В. Современные интерпретации термина «информационная война» // Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях) : сб. науч. ст. / под ред. Ю.Г. Чернышова. Барнаул: Изд-во Алт. ун-та, 2012. 244 с.

Ноговицын А.А., Барвиненко В.В., Мушков Ю.И. Методика оценки и пути обеспечения военной безопасности государства // Вестник Академии военных наук. 2004. № 1 (6). С. 112–116.

Павлова Т.А. Духовная безопасность российского общества как условие обеспечения социальной безопасности // Социология в современном мире: наука, образование, творчество. 2013. № 5. С. 202–205.

Подвигайло А.А., Целютина Т.В. Трансформация экономической и военно-технической доктрины современного общества как доминирующий фактор развития институтов гражданского общества // Власть. 2015. № 9. С. 27–33.

Полякова Г.В. Информация как общенаучная категория // Власть. 2013. № 9. С. 98–102.

Kroshilin, S.V. (2011). Information wars at the micro and macro levels and their impact on economic security. *Natsional'nye interesy: prioritety i bezopasnost'*, 7 (100), 73-77. (in Russian).

Krutskikh, A. (2007). To the political and legal basis of global information security. *Mezhdunarodnye protsessy*, 1, 28-37. (in Russian).

Kuznetsov, Yu.A., Markova S.E. (2013). Analysis of the qualitative features of the dynamics of the Russian ICT market. Structural approach. *Trudy Nizhegorodskogo gosudarstvennogo tekhn. un-ta im. R.E. Alekseeva. Ekonomika, innovatsii i menedzhment*, 3 (100), 242-252. (in Russian).

Kucheryavyy, M. (2013). Global Information Society and Security Issues. *Vlast'*, 9, 91-92. (in Russian).

Lopatin, Yu.N. (2008) Information security in Russia. Problems, search for solutions. *Gumanitarnye issledovaniya v Vostochnoy Sibiri i na Dal'nem Vostoke*, 2, 51-57. (in Russian).

Manoylo, A.V. (2012). Modern interpretations of the term “information war”. *Sovremennaya Rossiya i mir: al'ternativy razvitiya (Informatsionnye voyny v mezhdunarodnykh otnosheniyakh):* sb. nauch. st. Yu.G. Chernyshova (ed.). Barnaul: Izd-vo Alt. un-ta.

Nogovitsyn, A.A., Barvinenko, V.V., Mushkov, Yu.I. (2004). M Methods of assessment and ways to ensure the military security of the state. *Vestnik Akademii voennykh nauk*, 1 (6), 112-116. (in Russian).

Pavlova, T.A. (2013). The spiritual security of Russian society as a condition for ensuring social security. *Sotsiologiya v sovremennom mire: nauka, obrazovanie, tvorchestvo*, 5, 202-205. (in Russian).

Podvigaylo, A.A., Tselyutina, T.V. (2015). Transformation of the economic and military-technical doctrine of modern society as the dominant factor in the development of civil society institutions. *Vlast'*, 9, 27-33. (in Russian).

Polyakova, G.V. (2013). Information as a general scientific category. *Vlast'*, 9, 98-102. (in Russian).

Самыгин С.И., Верещагина А.В. Глобальные вызовы современности и безопасность цивилизации третьего тысячелетия // European Social Science Journal (Европейский журнал социальных наук). 2014. № 6, т. 2.

Самыгин С.И., Верещагина А.В., Кузнецова А.В. Обеспечение информационной безопасности военно-инженерных войск // Гуманитарные, социально-экономические и общественные науки. 2015. № 10. С. 459–462.

Требин М.П. Войны XXI века. M.z: АСТ; Мн. : Харвест, 2005. 399 с.

Bell D. The Coming of Post'Industrial Society: A Venture in Social Forecasting. Harmondsworth : Penguin, 1973. 507 p.

Nye J.S. Soft power: the means to success in world politics. N.Y. : Public Affairs, 2004. 192 p.

Toffler A. Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. N.Y. : Bantam, 1990. 613 p.

Samygin, S.I., Vereshchagina, A.V. (2014). Global Challenges of Modernity and the Security of a Third Millennium Civilization. *European Social Science Journal (Evropeyskiy zhurnal sotsial'nykh nauk)*, 6, 2. (in Russian).

Samygin, S.I., Vereshchagina, A.V., Kuznetsova, A.V. (2015). Ensuring the information security of military engineering troops. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki*, 10, 459-462. (in Russian).

Trebin, M.P. (2005). Wars of the XXI century. M.: AST; Mn.: Kharvest, 2005. 399 p.

Bell, D. (1973). The Coming of Post'Industrial Society: A Venture in Social Forecasting. Harmondsworth: Penguin, 507 p.

Nye, J.S. (2004). Soft power: the means to success in world politics. N.Y.: Public Affairs, 2004. 192 p.

Toffler, A. (1990). Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. N.Y.: Bantam, 1990. 613 p.

Поступила в редакцию ***11 февраля 2019 г.***