УДК 327.88
DOI

ВОЗМОЖНОСТИ ДЕМОКРАТИЧЕСКИХ ГОСУДАРСТВ ПО РЕАГИРОВАНИЮ И ПРОТИВОДЕЙСТВИЮ ГИБРИДНЫМ УГРОЗАМ

CAPABILITIES OF DEMOCRATIC STATES TO RESPOND AND COUNTER HYBRID THREATS

П.В. Попов
P.V. Popov

Балтийский государственный технический университет «Военмех» им. Д.Ф. Устинова,
Россия, 190005, г. Санкт-Петербург, ул. 1-я Красноармейская, 1

Baltic State Technical University «Voenmeh» of D.F. Ustinov,
1, 1ya Krasnoarmeyskaya St, Saint-Petersburg, 190005, Russia

E-mail: pa052vel@rambler.ru

Аннотация
Гибридные угрозы стали одним из современных вызовов национальной безопасности любого государства. Они отражают значительные изменения в характере международной безопасности. Некоторые концепции гибридной войны включают обширные невоенные инструменты. В статье рассматриваются возможности иностранных демократических государств по реагированию и противодействию гибридным угрозам с точки зрения иностранных специалистов. Проведен анализ созданных в ряде европейских государств основных структур, отвечающих за противодействие гибридным угрозам. Рассмотрены правовые акты Европейского союза, объединяющие имеющийся опыт и вырабатывающие новые механизмы и передовые практики. Сделан вывод по ряду общих черт по подготовке, реагированию и противодействию гибридным угрозам ведущих иностранных государств.

Abstract
Modern technologies, changing the familiar picture of the world and the perception of reality, lead to cardinal changes in all spheres of society. New forms and methods of warfare appear which led to the emergence of hybrid wars. Hybrid threats have become one of the modern challenges to the national security of any state. They reflect significant changes in the nature of international security. Some hybrid warfare concepts include extensive non-military tools. Within the framework of hybrid threats, the adversary can simultaneously use combinations of conventional and irregular methods of warfare, along with political, military, economic, social and informational means. The article discusses the capabilities of foreign democratic states in responding to and countering hybrid threats from the point of view of foreign experts. The analysis of the main structures created in several European countries responsible for countering hybrid threats has been carried out. The legal acts of the European Union uniting the existing experience and developing new mechanisms and best practices for preparing, responding to and counteracting the hybrid threats of leading foreign countries are considered, the conclusion on a number of general features is made.

Ключевые слова: гибридные войны, гибридные угрозы, кибербезопасность, кибератаки, Европейский союз.
Keywords: hybrid wars, hybrid threats, cyber security, cyber-attacks, European Union.

Открытые общества по своей природе уязвимы, однако крайне важно, чтобы они оставались открытыми. Всемирная сеть Интернет всё чаще становится ареной противостояния государств и открывает новые возможности для гибридных угроз. Вместе с тем

она также необходима для открытой глобальной торговли. Так, демократии могут быть достаточно инертными и громоздкими, но всё же они являются частью системы, которая является основой современных государств. При этом необходимо соблюдать баланс между защитой свободы слова граждан и безопасностью государства от гибридных угроз.

Тем не менее это не значит, что возможности демократии вести гибридные войны ограничены. Демократиям не чужды информационные операции, тайные операции и использование агентов влияния. Тем не менее они сталкиваются с тремя проблемами при реагировании на гибридные угрозы [Sahin, 2016].

Во-первых, поскольку гибридные угрозы затрагивают как всё правительство, так и общество в целом, им будет сложнее, чем автократическим противникам, быстро координировать принятие решений на разных уровнях власти. Так, по мнению научного сотрудника Центра возникающих угроз и возможностей при командовании по развитию боевых действий морской пехоты США подполковника Ф. Хоффмана [Hoffman, 2009], необходимо реагировать и адаптироваться быстрее, чем противник завтрашнего дня. При этом как проявлять гибкость на всех уровнях принятия управленческих решений, так и развивать необходимый комплекс оборудования [Hoffman, 2009, p.36]

Во-вторых, связанные с этим сдержки и противовесы, бюрократия и отдельные институты демократического общества усложняют сами операции гибридной войны.

В-третьих, гибридный конфликт бросает вызов важным этическим принципам. По словам одного аналитика, «демократии [не] могут вести гибридную войну всеобъемлющим и организованным образом, как это могут делать их автократические и негосударственные противники. Если бы они это сделали, они бы скомпрометировали саму суть того, что они стремятся защитить» [Sahin, 2016].

Деятельность государств и региональных структур по противодействию гибридным угрозам

Европейский союз

В апреле 2016 г. ЕС выпустил «Совместную рамочную договорённость по противодействию гибридным угрозам – ответ Европейского союза» [Joint Framework on countering hybrid threats…, 2016], в которой были сформулированы 22 практических предложения по повышению устойчивости ЕС и государств-членов, а также партнёров к гибридным угрозам. Отмечалось, что постоянное изменение как определения, так и характера гибридных угроз требует гибкости для реагирования, чтобы охватить сочетание силовой и диверсионной деятельности, обычных и нетрадиционных методов (т. е. дипломатических, военных, экономических, технологических), которые могут быть использованы скоординированным образом государственными или негосударственными акторами для достижения конкретных целей, оставаясь при этом ниже порога официального объявления войны. При этом противником будут использоваться выявленные им уязвимости цели, а также создаваться неопределённость, препятствующая процессам принятия решений.

Хотя повышение устойчивости государств-членов имеет решающее значение, так как большинство национальных уязвимостей зависят от конкретной страны, ЕС надеется эффективно реагировать на общие угрозы, направленные на трансграничные сети инфраструктуры. В ходе первого мероприятия государствам-членам было предложено выявить ключевые факторы уязвимости. Другие меры включали повышение уровня защиты и устойчивости критической инфраструктуры, координацию действий в киберпространстве, нацеленность на финансирование защиты от гибридных угроз и усиление координации с НАТО. В рамках Совместной договорённости выдвигалось предложение о создании Координирующего подразделения (EU Hybrid Fusion Cell) для выработки единого подхода к анализу гибридных угроз.

19 июля 2017 г. Европейская комиссия выпустила обновлённую информацию о шагах, предпринятых для реализации «Совместной рамочной договорённости 2016 года по

противодействию гибридным угрозам» [Security and defence…, 2017]. Сотрудничество с государствами, не являющимися членами, расширилось после запуска в Молдове пилотного исследования риска с целью выявления ключевых факторов уязвимости и оказания целевой помощи в этих областях. ЕС также принял «План ЕС» для противодействия гибридным угрозам [Joint Staff Working Document…, 2016]. В документе подробно описывается процедура реагирования ЕС на гибридную угрозу, в котором Координирующее подразделение ЕС играет критически важную роль для первоначального выявления угрозы до возникновения полного кризиса.

Великобритания

В Великобритании для реагирования на гибридные угрозы государственные структуры объединяются под эгидой кризисного центра. Его ядро – COBR (COBRA, The Cabinet Office Briefing Rooms «A», комната «A» заседаний кабинета министров). Будучи чрезвычайным советом, COBR собирается для обсуждения приоритетных вопросов, национальных или региональных кризисов, угрожающих безопасности страны, решение которых требует координации действий нескольких ведомств в правительстве.

В июне 2016 г. Комитет по обороне Палаты общин опубликовал доклад, посвящённый угрозе России и её последствиям для политики безопасности. В докладе акцентируется внимание на всём спектре задач, стоящих перед российскими военными и не конвенциональными возможностями. Основным подразделением как по работе с угрозами, создаваемыми враждебной дезинформацией и пропагандой, так и собственно их проведением в Министерстве обороны Великобритании является 77-я Бригада. Подразделение, созданное в сентябре 2014 г. и преобразованное в июле 2015 г., ставит своей целью «бросить вызов трудностям современной войны, с использованием как нелегальных действий, так и легальных невоенных рычагов в качестве средств для реагирования на действия противоборствующих сил и противников». Великобритания также призывает НАТО увеличить ресурсы и полностью разработать стратегию эффективного противодействия российской пропаганде и дезинформации [Russia: Implications…, 2016, p. 36–37].

В октябре 2016 г. в Британии был создан Национальный центр кибербезопасности (National Cyber Security Centre, NCSC), объединяющий отдельные структуры правительства, занимающиеся вопросами кибербезопасности [2017 Annual Review, 2017]. NCSC анализирует вопросы кибербезопасности, реагирует на инциденты в области кибербезопасности, использует отраслевой и академический опыт для развития возможностей кибербезопасности, а также снижает риски для Великобритании, защищая сети государственного и частного секторов. Создание центральной организации для борьбы с угрозами кибербезопасности позволяет NCSC решать задачи защиты наших критически важных сервисов от кибератак, управления крупными инцидентами и улучшения базовой безопасности Интернета в Великобритании посредством технологического совершенствования и консультирования граждан и организаций [About the NCSC, 2017].

В декабре 2017 г. Британский комитет по разведке и безопасности опубликовал свой ежегодный отчёт за 2016–2017 гг. [Annual report 2016–2017…, 2018]. В докладе рассматривались угрозы национальной безопасности, с которыми сталкивалась страна, от терроризма в Северной Ирландии до кибербезопасности. Хотя в нём явно не упоминаются гибридная война, нетрадиционные возможности, асимметричные подходы или война нового поколения, но рассматриваются конкретные уязвимости и инструменты, связанные с гибридной угрозой, особенно в киберсфере. Киберугроза является значительной и разнообразной, нацеленной на «все слои общества ... от государственных сетей до компаний и частных лиц» [Annual report 2016–2017…, 2018, p. 29].

Изучив кибероперацию по «вмешательству» в президентские выборы в США 2016 г., комитетом был сделан вывод о том, что «Государственные акторы обладают высокой способностью осуществлять передовые кибератаки, однако использование этих ме-

тодов исторически было ограничено дипломатическими и геополитическими последствиями, которые последуют в случае обнаружения такой деятельности. Недавняя российская киберактивность, похоже, указывает на то, что это перестало быть сдерживающим фактором» [Annual report 2016–2017…, 2018, p. 31].

Великобритания придаёт большое значение обеспечению контроля систем критической национальной инфраструктуры, что включает в себя защиту британской политической системы от кибератак. Целями таких атак могут быть подрыв целостности политических процессов в Великобритании, подрыв конкретных выборов или референдума с выгодой для предпочитаемой стороны враждебного актора, нанесение вреда общественному дискурсу по чувствительным политическим вопросам и выявление людей, которые могут быть открыты для подрывной деятельности или политического экстремизма в интересах враждебного актора [Annual report 2016–2017…, 2018, p. 32–33].

Для решения этих проблем NCSC отслеживает известных преступников, предоставляет наиболее эффективные методы защиты уязвимым лицам, сотрудничает в борьбе с враждебной пропагандой, а также повышает безопасность данных. Великобритания также инвестирует в наступательный киберпотенциал через Национальную наступательную киберпрограмму (National Offensive Cyber Programme, NOCP) для разработки специальных возможностей контратак в киберпространстве, которые будут выступать сдерживающим фактором [Annual report 2016–2017…, 2018, p. 43].

Финляндия

Финляндия является ещё одним примером комплексного подхода к обеспечению безопасности, при котором жизненно важные функции общества обеспечиваются за счёт сотрудничества между органами власти, бизнес-сообществом, организациями гражданского общества и отдельными гражданами [Cederberg, Eronen, p. 9, 2015]. Такой масштабный подход необходим для эффективной защиты от гибридных угроз, поскольку такие атаки не делают различий между отраслями экономики, гражданскими лицами, органами власти и военными целями. Министерство обороны Финляндии опубликовало Стратегию безопасности для общества в качестве основы для гибридной обороны [Security Strategy for Society, 2010].

Помимо простой публикации стратегических документов, Финляндия также предприняла конкретные шаги по укреплению своего потенциала. Ярким примером является создание Европейского центра передового опыта по противодействию гибридным угрозам (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE). Государство работает над улучшением национальной ситуационной осведомлённости в киберпространстве и является активным партнёром в региональных оборонных инициативах и учениях. Правительство также создало Национальный центр кибербезопасности (National Cyber Security Centre). Создается и совершенствуется группа реагирования на компьютерные инциденты (GOVCERT) для круглосуточного функционирования государственного сектора в информационно-телекоммуникационных сетях. Тщательно проработаны полномочия и ресурсы для полиции и военных, включая разведку, работающих в кибербласти. Что касается регионального партнёрства, то финские эксперты были направлены в Центры передового опыта НАТО (NATO's Centres of Excellence) в Таллине и Риге, а все подразделения Вооружённых сил Финляндии принимали участие в военных учениях, организованных в регионе Балтийского моря [Cederberg, Eronen, 2015, p. 9].

В то же время Финляндия разработала законодательство, предусматривающее предоставление более широких полномочий по проведению сбора разведывательной информации внутри и за пределами Финляндии» своим военным и силовым ведомствам, что позволит расширить полномочия вооружённых сил по проведению разведывательных операций с помощью агентурных каналов, радиоканалов связи, информационных и телекоммуникационных систем [Finland launches national…, 2017].

Швеция

В январе 2018 г. премьер-министр Ст. Лёвен также объявил об инициативе создания нового органа, ответственного за укрепление «психологической защиты» шведской общественности путём выявления, анализа и реагирования на «кампании внешнего влияния» [Rettman, Kirk, 2018]. Это будет воссозданием версии 2.0 предыдущего агентства, действовавшего в период Холодной войны – Комитета по психологической защите (The Board of Psychological Defence), который был поглощён в 2009 г. Агентством по гражданским чрезвычайным ситуациям (The Civil Contingencies Agency, MSB), которое взяло на себя и разработало функцию по управлению национальными кризисными ситуациями. Под руководством правительства Швеции MSB задействовалось в противодействии враждебным операциям влияния. Воссоздание нового органа, занимающегося вопросами контрпропаганды, станет частью более масштабных мер, в том числе по обеспечению безопасности выборов. Другие шаги буду включать в себя увеличение финансирования шведских разведывательных служб и служб киберзащиты.

Франция

Президент Франции Э. Макрон предложил изменить законодательство для борьбы с фальшивыми новостями и вмешательством в выборы [Chrisafis, 2018]. Хотя это не соответствует полноценной стратегии противодействия гибридным угрозам, оно нацелено на борьбу с манипуляциями во время прошедших президентских выборов, которые якобы имели место со стороны России. В ходе предвыборной кампании Э. Макрон обвинил Россию в использовании «гибридной стратегии, сочетающей в себе военное запугивание и информационную войну». Предлагаемое законодательство предусматривает требование к веб-сайтам раскрывать информацию о том, кто их финансирует, а также ограничение расходов на спонсорский контент. Закон идёт ещё дальше, чтобы противостоять тому, что Э. Макрон называет «пропагандой, выраженной тысячами учётных записей социальных сетей» в предвыборный период, позволяя властям удалять контент или блокировать вебсайт. Высшему совету аудиовизуальных средств (Conseil supérieur de l'audiovisuel, CSA), наблюдательному агентству страны, будет предоставлено больше полномочий для борьбы с любой попыткой дестабилизации со стороны телевизионных каналов, контролируемых или находящихся под влиянием иностранных государств [Serhan, 2018].

Эстония

В 2008 г. в Эстонии был открыт Центр передового опыта совместной киберзащиты НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE) в Таллинне. Он поддерживает создание возможностей по сотрудничеству и обмену информацией между странами НАТО и партнёрами в области киберзащиты на основе профессионального образования, научных исследований и разработок, извлечённых уроков и консультаций [NATO Cooperative Cyber…, 2019]. Центр был создан после того, как в 2007 г. Эстония «подверглась политически мотивированной» трехнедельной российской кибератаке в связи с перемещением советского мемориала времён Великой Отечественной войны [Ian Traynor, 2007]. Атака была направлена на сайты президента Эстонии, парламента, правительственных министерств, политических партий, трёх из шести крупных новостных организаций, двух крупных банков и компаний связи.

В 2011 г. в Эстонии было сформировано подразделение киберзащиты Лиги обороны (Cyber Defence Unit of the Defence League). Подразделение киберзащиты является частью Лиги обороны Эстонии, добровольной организации, связанной с вооружёнными силами Эстонии [Government formed Cyber Defence Unit…, 2011]. Киберобъединение состоит из патриотически настроенных волонтёров, которые являются специалистами в ключевых областях кибербезопасности, владеющих навыками в области информационных технологий, а также экс-

пертами в других областях (например, юристы и экономисты) [Ruiz, 2018]. Его цель – повысить готовность населения защищать независимость Эстонии и её конституционный порядок, опираясь на свободу воли и личную инициативу [Kaska et al., 2013, p.11].

В 2013 г. CCDCOE опубликовал анализ работы этого подразделения, в котором был подтвержден положительный опыт участия сотрудников подразделения киберзащиты в различных мероприятиях, предусмотренных законом, как для повышения потенциала и возможностей самого подразделения киберзащиты, так и повышения киберустойчивости и способности реагировать на угрозы государства в целом. Группа киберзащиты занимается одним из ключевых аспектов противодействия гибридным угрозам – формированием устойчивости к ним, повышением способности реагировать на потенциальную кибератаку [Kaska et al., 2013, p. 27–28].

Выводы

Современные технологии, изменяя привычную картину мира и восприятия реальности, приводят к кардинальным переменам во всех сферах жизнедеятельности общества. Появляются новые формы и способы ведения боевых действий, что привело к появлению гибридных войн. Гибридные угрозы стали одним из современных вызовов национальной безопасности любого государства. Они отражают значительные изменения в характере международной безопасности. В рамках гибридных угроз противником могут одновременно использоваться комбинации обычных и иррегулярных методов ведения войны наряду с политическими, военными, экономическими, социальными и информационными средствами. В этой связи можно выделить следующие передовые практики ведущих государств по подготовке, реагированию и противодействию гибридным угрозам, которые имеют ряд общих черт:

– они охватывают все системы управления государством с одновременным подключением возможностей всего общества;

– они оценивают уязвимости. В первую очередь необходимо сосредоточиться на информационной сфере, против угроз в телекоммуникационной среде: шпионажа, цифровых атак и манипулирования информацией [Cederberg, Eronen, 2015];

– они уделяют особое внимание кибербезопасности, поскольку киберсфера, наряду с социальными сетями, являются основными компонентами гибридных угроз;

– они проявляют творческий подход к работе с негосударственным сектором, в чьих руках находятся телекоммуникационная инфраструктура, подлежащая государственной защите. Так, например, подразделение киберзащиты Эстонии является частью Лиги обороны Эстонии, добровольной военной организации национальной обороны;

– они зависят от общей ситуационной осведомлённости, получаемым разведывательным сведениям, проводимому высококачественному анализу и активных контрразведывательных действий. В некоторых странах это потребовало изменения законов, чтобы предоставить разведывательным службам больше полномочий для сбора информации как внутри страны, так и за её пределами.

Список литературы:
References

1. «2017 Annual Review», National Cyber Security Centre, October 3, 2017, URL: https://www.ncsc.gov.uk/news/2017-annual-review (дата обращения: 18.01.2020).

2. «About the NCSC», National Cyber Security Centre, 2017. URL: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do (дата обращения: 18.01.2020).

3. Andrew Rettman, Lisbeth Kirk, 2018. «Sweden Raises Alarm on Election Meddling», EU Observer. URL: https://euobserver.com/foreign/140542 (дата обращения: 18.01.2020).

4. Angelique Chrisafis, 2018. «Emmanuel Macron promises ban on fake news during elections», The Guardian. URL: https://www.theguardian.com/world/2018/jan/03/emmanuel-macron-ban-fake-news-french-president (дата обращения: 18.01.2020).

5. Annual report 2016–2017, Intelligence and Security Committee of Parliament, 2018. URL: https://www.gov.uk/government/publications/intelligence-and-security-committee-annual-report-2016-2017 (дата обращения: 18.01.2020).

6. Cederberg, A., Eronen, P., 2015. How can societies be defended against hybrid threats? Strategic Security Analysis, Geneva Centre for Security Policy, 9(1): 1–10. URL: https://www.fdd.org/analysis/2015/10/05/how-are-societies-defended-against-hybrid-threats/ (дата обращения: 18.01.2020).

7. Frank Hoffman, 2009. «Hybrid Warfare and Challenges», National Defense University. Institute for National Strategic Studies. URL: https://smallwarsjournal.com/documents/jfqhoffman.pdf (дата обращения: 18.01.2020).

8. «Finland launches national security initiatives defending against hybrid threats», Pentagon Defense News, 2017. URL: https://www.defensenews.com/pentagon/2017/04/28/finland-launches-national-security-initiatives-defending-against-hybrid-threats/ (дата обращения: 18.01.2020).

9. «Government formed Cyber Defence Unit of the Defence League», Republic of Estonia Ministry of Defence, 2011. URL: http://www.kaitseministeerium.ee/en/news/government-formed-cyber-defence-unit-defence-league (дата обращения: 18.01.2020).

10. Ian Traynor, 2007. «Russia accused of unleashing cyberwar to disable Estonia», The Guardian, May 16, 2007, URL: https://www.theguardian.com/world/2007/may/17/topstories3.russia (дата обращения: 18.01.2020).

11. «Joint Framework on countering hybrid threats – a European Union response», European Commission, 2016. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (дата обращения: 18.01.2020).

12. «Joint Staff Working Document – EU operational protocol for countering hybrid threats 'EU Playbook'», Council of the European Union, 2016. URL: http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf (дата обращения: 18.01.2020).

13. Kaan Sahin, «Liberal Democracies and Hybrid War», International Institute for Strategic Studies, 2016. URL: https://www.iiss.org/blogs/military-balance/2016/12/liberal-democracies-hybrid-war (дата обращения: 18.01.2020).

14. Kadri Kaska et al., 2013. «The Cyber Defence Unit of the Estonian Defence League – Legal, Policy and Organisational Analysis», NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (дата обращения: 18.01.2020).

15. Monica M. Ruiz, 2018. «Is Estonia's Approach to Cyber Defense Feasible in the United States?» War on the Rocks, January 9, 2018. URL: https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/ (дата обращения: 18.01.2020).

16. «NATO Cooperative Cyber Defence Centre of Excellence – About Us», NATO, 2019. URL: https://ccdcoe.org/about-us/ (дата обращения: 18.01.2020).

17. «Russia: Implications for UK defence and security - First Report of Session 2016-17», House of Commons Defence Committee, 2016. URL: https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf (дата обращения: 18.01.2020).

18. «Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead», European Commission, 2017. URL: http://europa.eu/rapid/press-release_IP-17-2064_en.htm (дата обращения: 18.01.2020).

19. «Security Strategy for Society», Ministry of Defence of Finland, 2010. URL: https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf (дата обращения: 18.01.2020).

20. Yasmeen Serhan, 2018. «Macron's War on 'Fake News'», The Atlantic. URL: https://www.theatlantic.com/international/archive/2018/01/macrons-war-on-fake-news/549788/ (дата обращения: 18.01.2020).

Ссылка для цитирования статьи
Link for article citation

Попов П.В. 2020. Возможности демократических государств по реагированию и противодействию гибридным угрозам. Via in tempore. История. Политология, 47(1): 187–193. DOI

Popov P.V. 2020. Capabilities of democratic states to respond and counter hybrid threats. Via in tempore. History and political science, 47(1): 187–193 (in Russian). DOI