КОНЦЕПТУАЛЬНЫЕ ВЗГЛЯДЫ СТРАН ЗАПАДА НА КИБЕРВОЙНЫ

А. Л. Баньковский[1)], П. И. Савков[2)]

1) Государственный секретариат Совета Безопасности Республики Беларусь, ул. К. Маркса, 38, 220016, г. Минск, Беларусь, iau@sssc.gov.by

2) Государственный секретариат Совета Безопасности Республики Беларусь, ул. К. Маркса, 38, 220016, г. Минск, Беларусь, iau@sssc.gov.by

На основе комплексного анализа доктринальных документов стратегического характера расмотрены концептуальные взгляды военно-политического руководства США, других стран-членов НАТО и ЕС на применение наступательного киберпотенциала и ведение «проактивной кибероборонs» в повседневных условиях и в ходе конфликтов различной интенсивности. Обоснована необходимость развития национальных концептуально-прикладных подходов в данной сфере.

Ключевые слова: кибербезопасность; киберпространство; противоборство в киберпространстве; киберстратегия; кибервойска.

CONCEPTUAL VIEWS OF WESTERN COUNTRIES ON THE CYBERWARS

A. L. Bankovsky[a], P. I. Savkov[b]

[a]State Secretariat of the Security Council of the Republic of Belarus, K. Marx Street, 38, 220016, Minsk, Belarus

[b]State Secretariat of the Security Council of the Republic of Belarus, K. Marx Street, 38, 220016, Minsk, Belarus, iau@sssc.gov.by

Based on a comprehensive analysis of strategic doctrinal documents, the author considers the conceptual views of the military-political leadership of the United States, other NATO and EU member states on the use of offensive cyber potential and the conduct of «proactive cyber defense» in everyday conditions and during conflicts of varying intensity. The necessity of developing national conceptual and applied approaches in this area has been substantiated.

Key words: cybersecurity; cyberspace; confrontation in cyberspace; cyberstrategy; cybertroops.

За последние два десятилетия за рубежом системно проработаны подходы к обеспечению кибербезопасности и использованию информационно-коммуникационных технологий в военно-политических целях, что нашло отражение в ряде концептуальных документов – национальных стратегиях кибербезопасности, доктринах кибероперaций военных ведомств и методических документах Североатлантического альянса.

Объективное превосходство США по уровню развития теории и практики ведения противоборства в киберпространстве оказывает определяющее влияние на деятельность других стран – членов НАТО в области кибероборонs. В доктринальных документах США термин «кибервойна» не применяется и, как правило, используется в СМИ и в неофициальной коммуникации. В американских документах стратегического характера в данной области получил распространение термин «операции в киберпространстве», под которыми понимается использование возможностей кибернетических средств для обеспечения превосходства над противником в киберпространстве, а также за его пределами [1].

Соответственно применяемые в киберпространстве силы и средства относятся к полноценным инструментам защиты национальных интересов наряду с

дипломатическими, информационными, военными, экономическими, финансовыми и правоохранительными мерами. Этот же набор инструментов используется для реагирования на враждебные кибератаки [2]. Согласно словарю военных терминов МО США кибератака представляет собой преднамеренные действия по изменению, разрушению, искажению, запрещению, нарушению или уничтожению информации и программ, находящихся в компьютерных системах и сетях, или самих компьютеров и сетей противника.

В качестве потенциального противника в киберпространстве военно-политическое руководство США рассматривает как государства, так и негосударственные структуры. При этом государства могут использовать негосударственных акторов как прикрытие, что серьезно усложняет задачу выявления основных заказчиков кибератаки. Вследствие этого Соединенные Штаты ожидают рост наступательных киберпотенциалов у своих противников и распространение практики регулярного использования кибератак для получения политических, экономических и военных преимуществ [2].

Как правило, противоборство в киберпространстве относится к конфликтам низкой интенсивности, на которые не распространяется международное гуманитарное право. В то же время, следует согласиться с мнением различных экспертов о том, что злонамеренное использование информационно-коммуникационных технологий способно нанести вред, иногда сравнимый с применением традиционного (кинетического) оружия, а в ряде случаев – с применением оружия массового уничтожения, что представляет серьезную угрозу международному миру и безопасности и должно порождать неотъемлемое право государства на самооборону в рамках Статьи 51 Устава ООН [3].

Учитывая военный потенциал кибероперaций, военно-политическое руководство США с 2004 года рассматривает киберпространство как новую сферу ведения военных действий наряду с наземной, морской, воздушной и космической сферами. В настоящее время основным доктринальным документом США в сфере киберпространства является «Стратегия национальной кибербезопасности Соединенных Штатов Америки» 2018 года (далее – Национальная киберстратегия) [4]. В ней перечислены основные источники угроз – Россия, Китай, Иран, КНДР и международный терроризм. Национальная киберстратегия предполагает активизацию усилий федерального правительства США с вовлечением частного сектора и других заинтересованных сторон на четырех основных направлениях:

1. Защита американского народа, отечества и американского образа жизни, включая повышение киберзащищенности информационных сетей федеральных ведомств, обеспечение кибербезопасности критически важной инфраструктуры, а также борьбу с киберпреступлениями и реагирование на киберинциденты.

2. Содействие американскому процветанию путем развития рынка совместимых и безопасных IT-продуктов, продвижения инноваций в сфере информационно-коммуникационных технологий, а также стимулирования роста числа высококвалифицированных специалистов.

3. Поддержание мира посредством силы за счет укрепления глобальной стабильности в киберпространстве, определения источника кибератак и сдерживания неприемлемого поведения в киберспространстве.

4. Продвижение американского влияния в киберпространстве путем поддержки открытого, основанного на совместимых технологиях, надежного и безопасного Интернета, а также наращивания международного потенциала и ресурсов в области обеспечения кибербезопасности.

В настоящее время решение о проведении кибероперациий за пределами США, включая проактивные кибероперации и операции с существенными последствиями, может быть принято без предварительного утверждения президентом США. В Национальной киберстратегии отмечается, что Соединенные Штаты будут использовать «все доступные средства», в том числе политико-дипломатические, экономические и военные меры воздействия, включая действия в киберпространстве и применение кинетических вооружений [6].

В рамках продвижения американского влияния в киберпространстве США рассчитывают выстроить «стратегические партнерские отношения» со своими союзниками и государствами-единомышленниками, которые будут иметь решающее значение для оказания влияния на «плохих акторов» в киберпространстве. Ключевая роль при этом отводится США т. н. «инициативе киберсдерживания», которая предусматривает координацию общего ответа широкой коалиции государств-единомышленников на «серьезные злонамеренные инциденты в киберпространстве».

Кардинальный пересмотр приоритетов военно-политического руководства США в сторону наступательных, превентивных силовых действий в киберпространстве подтверждают опубликованные в 2018 году «Общие положения киберстратегии минобороны США» [7]. Основные из них:

США вовлечены в «стратегическое состязание» с Китаем и Россией, действия этих двух государств в киберпространстве представляют долгосрочный стратегический риск для американской нации и ее союзников;

министерство обороны США планирует проводить кибероперации с целью сбора разведданных и наращивания военного потенциала на случай полномасштабного кризиса, а также осуществлять операции в рамках проактивной кибероборонs для пресечения, предупреждения и противодействия враждебной активности в киберпространстве, даже если такая активность не достигает порога применения силы по смыслу международного права;

в «обстановке военного времени» вооруженные силы США задействуют «наступательный киберпотенциал» и «инновационные решения» для проведения кибероперациий на всех театрах военного конфликта.

Анализ содержания этого документа показывает, что основной целью Пентагона в киберпространстве является «обеспечение проактивной обороны, отладка работы в формате каждодневного состязания со стратегическими соперниками, а также обеспечение готовности к войне», в т. ч. за счет «создания более смертоносных» вооруженных сил в части деятельности в киберпространстве. Продвигать интересы США посредством операций в киберпространстве можно будет во всем спектре интенсивности конфликтов: от повседневных опе-

раций до военного времени [6]. При этом кибервозможности будут использоваться и в упреждающем порядке.

В соответствии с положениями киберстратегии МО США в 2018 году обновлена и «Единая доктрина кибероперaций» [8]. Ддокумент посвящен вопросам планирования, ведения и оценки кибероперaций, использования возможностей киберпространства для других видов операций. Также в единой доктрине приведена классификация кибероперaций и киберсил. Так, по содержанию решаемых задач кибероперации классифицируются США как наступательные, оборонительные и операции в собственных информационных сетях МО США.

С целью обеспечения операций в киберпространстве МО США в 2013 году инициировало создание кибервойск общей численностью около 6,2 тыс. человек [2]. Задачи и структура этого нового рода войск ориентированы на ведение информационно-технического противоборства, объектами воздействия которого являются информационно-технические системы. В рамках информационно-психологического противоборства кибервойска выполняют скорее обеспечивающие задачи по сбору разведывательной информации, проведению кибератак на назначенные Интернет-ресурсы.

Таким образом, США признают, что противоборство в киберпространстве меняет сложившийся стратегический баланс сил, поэтому американское руководство рассматривает свои кибервозможности в неразрывной связи с другими элементами национальной мощи. В американских доктринальных документах официально заявлено о переходе к «проактивной кибероборонe» и проведении кибероперaций во всем спектре интенсивности конфликтов – от повседневных условий до военного времени.

Государственная политика стран – членов НАТО в сфере кибербезопасности в целом соответствует концептуальным подходам США. В отсутствие универсальных международных договоров, регулирующих отношения в области использования информационно-коммуникационных технологий в качестве средств вооруженного насилия, страны НАТО ориентируются на международные обычаи применительно к вооруженным конфликтам в киберпространстве. При этом их толкование возлагается, по существу, на участвующие в конфликте стороны [3].

В целях выработки единого подхода к оценке опасности кибератак в рамках НАТО в 2012 году разработано «Таллиннское руководство по международному праву, применимое к кибервойне» [9], согласно которому под кибератакой понимается наступательная или оборонительная кибероперация, которая причиняет ранения или смерть людям либо ущерб объектам. Ключевой критерий применения силы в киберпространстве в рамках НАТО – серьезность последствий кибератаки, которые могут проявляться в физических разрушениях критической инфраструктуры и иных объектов, либо в человеческих жертвах, которые непосредственно повлекло воздействие в киберпространстве.

В сентябре 2014 года по итогам саммита Североатлантического альянса в Уэльсе одобрена «Углубленная политика кибероборонe НАТО» и решено, что право стран – членов НАТО на коллективную оборону, распространяется и на те случаи, когда одно из государств альянса становится жертвой нападения в ки-

берпространстве. Кибератака на страну – члена организации, повлекшая гибель людей или масштабное разрушение инфраструктуры, и, по мнению альянса, совершенная напрямую государством или его посредниками, может повлечь вооруженный ответ НАТО с использованием всего доступного ей военного потенциала, не ограничиваясь киберпространством [9].

На саммите Североатлантического союза в Варшаве (8-9 июля 2016 г.) также принято решение об интенсификации процесса развития национальных потенциалов кибероборонны и укрепления кибербезопасности информационных сетей, от которых в том числе зависит выполнение основных задач альянса. В феврале 2017 года по итогам заседания Североатлантического совета на уровне министров обороны приняты обновленный «План кибероборонны» и «Дорожная карта по освоению киберпространства как новой сферы операций» [10].

Благодаря усилиям США, практически завершено создание системы реагирования на компьютерные угрозы в НАТО. Входящие в ее состав силы и средства предназначены для своевременного выявления и нейтрализации киберугроз, а при необходимости для восстановления в кратчайшие сроки работоспособности компьютерных сетей органов управления государств – членов альянса. В 2018 году объявлено о создании центра кибероперацій НАТО (Монс, Бельгия), который к 2023 году должен достичь полной готовности к выполнению задач по предназначению [7].

В рамках взаимодействия между альянсом и национальными органами по вопросам ведения кибероперацій в Эстонии создан Объединенный центр изучения передового опыта по совместной защите от киберугроз НАТО [10]. Принципы и подходы уставных и рекомендательных документов Североатлантического союза закладываются в доктринальные документы ведущих стран Запада и учитываются при формировании соответствующих национальных органов управления и войск (сил). В составе вооруженных сил ведущих европейских стран – членов альянса создаются кибервойска и осуществляется их плановая подготовка к применению по предназначению.

Сотрудничество НАТО и Европейского союза в целом развивается на основе подписанной в июле 2016 года совместной Декларации, где в качестве одного из приоритетов отмечена кибербезопасность и кибероборона [10]. Основная цель – разграничение сфер ответственности. Североатлантический союз взял на себя обязательство по киберзащите своих государств-членов, а ЕС – задачи мониторинга киберугроз, обмена информацией, быстрого реагирования и развития инвестиционного партнерства. На данном этапе подобное сотрудничество дает возможность ЕС получить опыт и нарастить свой собственный киберпотенциал, а НАТО избавляет от необходимости в одиночку обеспечивать кибербезопасность на уровне отдельно взятых государств.

Таким образом, в странах Запада кибероперации признаются полноценным инструментом защиты национальных интересов наряду с дипломатическими, информационными, военными, экономическими, финансовыми, правоохранительными и иными специальными мерами. Для сдерживания кибератак потенциального противника западные государства выступают за переход к «проактивной кибероборонне» и применение наступательного киберпотенциала

во всем спектре интенсивности конфликтов – от повседневных условий до военного времени. Кроме того, США и страны – члены НАТО допускают возможность реагирования на враждебные кибератаки, которые причиняют ранения или смерть людям либо ущерб объектам, как на вооруженную агрессию [11].

В современных условиях обозначена настоятельная необходимость разработки и дальнейшего развития концептуальных, правовых и организационных основ обеспечения кибербезопасности Беларуси в военной, а также иных сферах жизнедеятельности государства. Для этого необходимы комплексные исследования вопросов кибербезопасности в преломлении к национальной безопасности Республики Беларусь.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms, 15 February 2016. [Электрон. ресурс]. URL: https://fas.org/irp/doddir/jp1_02.pdf. Дата доступа: 28.08.2019.
2. Селянин, Я. В. Роль Пентагона в обеспечении кибербезопасности США // Проблемы обеспечения национальной стратегии. 2017. № 3 (42). С.130-147.
3. Стрельцов, А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству // Право и государство: теория и практика. 2014. № 3 (111). С. 75–88.
4. National Cyber Strategy of the United States of America. September 2018 [Электрон. ресурс]. URL: https:/www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Дата доступа: 28.08.2019.
5. Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений / О. Демидов, М. Ангмар. // Индекс безопасности. М.: Триалог, 2019. 27 с.
6. США усиливают онлайновые атаки на российскую энергосистему / The New York Times [Электрон. ресурс]. URL: https://inosmi.ru/politic/20190617/245288329. Дата доступа: 28.08.2019.
7. Смирнов, И., Алексеев, Г. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств / Зарубежное военное обозрение. 2017. № 6. С.8-14.
8. Joint Publication 3-12 Cyberspace Operations (JP 3-12), 8 June 2018 [Электрон. ресурс]. URL: https://publicintelligence.net/jcs-cyberspace-operations. Дата доступа: 28.08.2019.
9. Применение международного права в киберпространстве / М. С. Гаврилова, О. В. Демидов, А. Л. Козик, А. А. Стрельцов // Индекс безопасности. 2015. Т. 21. С. 99–116.
10. Карасев, П. Кибервойска Европы и НАТО [Электрон. ресурс]. URL: http://expert.ru/2018/03/13/kibervojska-evropyi-i-nato/. Дата доступа: 28.08.2019.
11. Зарубежный опыт обеспечения информационной безопасности: концептуально-правовые подходы: монография / В. Ю. Арчаков, А. Л. Баньковский [и др.]: под общ. науч. ред. В. П. Вишневской, О. С. Макарова Минск: ИПС РБ, 2020. 345 с.

КОНЦЕПЦИИ (СТРАТЕГИИ) НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАН БЛИЖНЕГО И ДАЛЬНЕГО ЗАРУБЕЖЬЯ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

А. Л. Баньковский[1)], Э. Г. Головко[2)], Д. В. Свириденок[3)]

1) Государственный секретариат Совета Безопасности Республики Беларусь, ул. К. Маркса, 38, 220016, г. Минск, Беларусь, iau@sssc.gov.by