ВОПРОСЫ ПОЛИТОЛОГИИ

ВЫПУСК 1(77), 2022

Научный журнал

Журнал «Вопросы политологии» включен
в Перечень рецензируемых научных изданий
ВАК при Министерстве науки и высшего образования РФ
по политическим наукам, в которых должны быть опубликованы
основные научные результаты на соискание ученой степени кандидата
наук, на соискание ученой степени доктора наук

Журнал включен в Перечень научных изданий
рекомендованных ВАК Республики Узбекистан
для публикации основных научных результатов диссертаций
по политическим и философским наукам

МОСКВА, 2022

ВОПРОСЫ ПОЛИТОЛОГИИ

Научный журнал

ISSN 2225–8922

Председатель Редакционного Совета – ПЛАТОНОВ В.М.,
к.ю.н., заведующий кафедрой политического анализа и управления РУДН,
Председатель Московской городской Думы (1994–2014 гг.)

Редакционный Совет

АВАЗОВ
Камиль Халиевич

АСТАПАТУРОВА
Майя Арташеговна

БЛОХИН
Владимир Владимирович
БОЖАНОВ
Владимир Александрович
ВАНКОВСКА
Биляна

ВЕДРИН
Оливье
ВЕЛИКАЯ
Наталья Михайловна
ГОНЧАРОВ
Пётр Константинович
ГРАЧЁВ
Михаил Николаевич
ДЭМБЭРЭЛ К.

ДОНАЙ
Лукаш
ЖИЛЬЦОВ
Сергей Сергеевич
КАРАДЖЕ
Татьяна Васильевна
КАССАЕ НЫГУСИЕ
В. МИКАЭЛЬ
КОВАЛЕНКО
Валерий Иванович
КОМЛЕВА
Валентина Вячеславовна
КРИВОКАПИЧ
Борис
МЕДВЕДЕВ
Николай Павлович
МИХАЙЛОВ
Вячеслав Александрович
НАЗАРОВА
Елена Александровна
НАЗАРОВ
Александр Данилович
НАСИМОВА
Гульнара Орленбаевна
НИСНЕВИЧ
Юлий Анатольевич
ОРЛОВ
Игорь Борисович
ПАХРУТДИНОВ
Шукритдин Ильясович

ПЛЯЙС
Яков Андреевич
ПРЯХИН
Владимир Федорович
ПУСЬКО
Виталий Станиславович
РУБАН
Лариса Семёновна

СЛИЗОВСКИЙ
Дмитрий Егорович
СЫЗДЫКОВА
Жибек Сапарбековна
ХОПЕРСКАЯ
Лариса Львовна
ШАРКОВ
Феликс Изосимович
ЯН ФУЛИНЬ

д.ф. (PhD) по полит. наукам, Региональный центр переподготовки
и повышения квалификации работников народного образования
Сурхандарьинской области (Узбекистан, г. Ташкент)

д.п.н., профессор, Пятигорский государственный университет
(Россия, г. Пятигорск)

д.и.н., профессор, РУДН (Россия, г. Москва)

д.и.н., профессор, Белорусский Национальный технический
университет (Белоруссия, г. Минск)
профессор политологии и международных отношений
факультета философии Университета Святых Кирилла и Мефодия
(Македония, г. Скопье)
профессор, ректор «Континентального университета в Киеве»
(Франция, г. Париж)
д.п.н., профессор, ИСПИ ФНИСЦ РАН, РГГУ (Россия, г. Москва)

д.с.н., профессор, Российский университет транспорта (МИИТ)
(Россия, г. Москва)

д.п.н., профессор, РГГУ (Россия, г. Москва)

доктор (PhD), Институт международных отношений АН Монголии
(Монголия, г. Улан-Батор)

д.п.н., профессор, Университет им. Адама Мицкевича в Познани
(Польша, г. Познань)

д.п.н., профессор, Дипломатическая академия МИД РФ
(Россия, г. Москва)

д.ф.н., профессор, МПГУ (Россия, г. Москва)

д.и.н., профессор, РУДН (Россия, г. Москва)

д.ф.н., профессор, МГУ им. М.В. Ломоносова (Россия, г. Москва)

д.с.н., профессор, РАНХиГС при Президенте РФ (Россия, г. Москва)

д.ю.н., Унион—Никола Тесла университет (Сербия, г. Белград)

д.п.н., профессор, главный редактор журнала (Россия, г. Москва)

д.и.н., профессор, РАНХиГС при Президенте РФ (Россия, г. Москва)

д.с.н., профессор, МГИМО МИД России (Россия, г. Москва)

д.и.н., профессор, МАИ (Россия, г. Москва)

д.п.н., профессор, Казахский Национальный университет
им. Аль-Фараби (Казахстан, г. Алматы)

д.п.н., профессор, НИУ «Высшая школа экономики»
(Россия, г. Москва)

д.и.н., профессор, НИУ «Высшая школа экономики»
(Россия, г. Москва)

д.п.н., профессор, Институт переподготовки и повышения
квалификации руководителей и специалистов системы народного
образования имени А. Авлони (Узбекистан, г. Ташкент)

д.и.н., д.п.н., профессор, Финансовый университет при Правительстве РФ
(Россия, г. Москва)

д.п.н., профессор, РГГУ (Россия, г. Москва)

д.ф.н., профессор, ВА РВСН им. Петра Великого (Россия, г. Москва)

д.с.н., профессор, отдел исследования проблем международного
сотрудничества Института социально-политических исследований ФНИСЦ
РАН (Россия, г. Москва)

д.и.н., профессор, РУДН (Россия, г. Москва)

д.и.н., профессор, ИСАА МГУ им. М.В. Ломоносова
(Россия, г. Москва)

д.п.н., профессор, Киргизско-Российский славянский университет
(Киргизия, г. Бишкек)

д.с.н., профессор, РАНХиГС при Президенте РФ (Россия, г. Москва)

проректор Хэйлунцзянского института иностранных языков
(КНР, г. Харбин)

Редакционная коллегия

Главный редактор – МЕДВЕДЕВ Н.П., д.п.н., профессор

Абрамова О.Д. (д.п.н.)

Насимова Г.О. (д.п.н.)

Кетцян Г.В. (к.п.н. – зам. гл. редактора)

Шкурина С.С. (к.п.н. – ответ. редактор)

**ЖУРНАЛ ВКЛЮЧЕН
В ПЕРЕЧЕНЬ ВАК РФ**

**УЧРЕЖДЕН
ООО «Издательство
«Наука сегодня»**

Журнал зарегистрирован
Федеральной службой
по надзору в сфере массовых
коммуникаций, связи и охраны
культурного наследия

Per. № ПИ № ФС77–46176
от 12 августа 2011 г.

Журнал издается ежемесячно

Журнал включен в базу РИНЦ
(Российский индекс
научного цитирования)

Включен в каталог
Ulrich's Periodicals Directory

Пятилетний импакт-фактор: 1,489.

Адрес редакции:
115598, г. Москва, ул. Загорьевская,
д. 10, корп. 4, цокольный этаж,
помещение I, комната 7-1, офис 4
Тел.: (910) 463-53-42

Интернет-ресурс:
www.voprospolitolog.ru
E-mail: voprospolitolog@yandex.ru

Мнение авторов может
не совпадать с мнением редакции.
При перепечатке ссылка
на журнал обязательна.

Научные статьи, публикуемые
в журнале подлежат обязательному
рецензированию.

Ответственный редактор
Шкурина С.С.

Перевод
Чернышова Е.В.

Компьютерная верстка
Анциферова А.С.

Подписано в печать 27.01.2022

Формат 60×84/8. Объем 24,3.

Печать офсетная.

Тираж – 1000 экз.

(1-й завод – 500 экз.)

Заказ № 000.

Отпечатано в типографии
ООО «Белый ветер»

115054, г. Москва, ул. Шипок, 28

Тел.: (495) 651-84-56

ISSN 2225-8922 (print)

12 выпусков в год и

4 выпуска в год переводной (англ.) версии

Языки: русский, английский

<http://voprosplitolog>

Входит в перечень рецензируемых научных изданий ВАК РФ

Включен в каталог периодических изданий Ульрих

(Ulrich's Periodicals Directory: <http://www.ulrichsweb.com>)

Материалы журнала размещаются на платформе РИНЦ

Российской научной электронной библиотеки, Electronic Journals Library Cyberleninka

Подписной индекс издания в каталоге агентства Роспечать 70035

Цели и тематика

Журнал ВОПРОСЫ ПОЛИТОЛОГИИ – периодическое международное рецензируемое научное издание в области политических исследований. Журнал является международным как по составу редакционного совета и редколлегии, так и по авторам и тематике публикаций.

Научный журнал издается с 2011 года в издательстве «Наука сегодня». С 2016 года издается переводная (англ.) версия журнала. С момента своего создания, журнал ориентировался на высокие научные и этические стандарты и сегодня является одним из ведущих политологических журналов России.

Цель журнала – способствовать научному обмену и сотрудничеству между российскими и зарубежными политологами.

Журнал предназначен для публикации результатов фундаментальных и прикладных научных исследований. Тематическая направленность журнала отражается в следующих постоянных рубриках: «История и философия политики», «Политические институты, процессы и технологии», «Политическая регионалистика и этнополитика», «Политическая культура и идеологии», «Политические проблемы международных отношений и глобализации».

Формат публикаций: научные статьи, обзорные научные материалы, материалы круглых столов, научные рецензии, научные сообщения, посвященные исследовательским проблемам в сфере политики и политологии.

В своей деятельности редакционный совет и редколлегия журнала руководствуется принципами, определяемыми ВАК России для научных журналов, в том числе: наличие института рецензирования для экспертной оценки качества научных статей; информационная открытость издания; наличие и соблюдение правил и этических стандартов представления рукописей авторами.

Целевой аудиторией журнала являются российские и зарубежные специалисты-политологи, а также аспиранты и магистры, обучающиеся по направлениям политология, государственное и муниципальное управление и международные отношения.

Журнал строго придерживается международных стандартов публикационной этики, обозначенных в документе COPE (Committee on Publication Ethics) <http://publicationethics.org>

Полные сведения о журнале и его редакционной политике, требования о подготовке и публикации статей, архив (выпуски с 2011 года) и дополнительная информация размещена на сайте: <http://voprosplitolog.ru>

Электронный адрес: voprosplitolog@yandex.ru

ISSN 2225-8922 (print)

12 issues a year plus

4 issues a year of the translated (eng.) version

Languages: Russian and English

<http://voprosplitolog>

Included in the list of peer-reviewed scientific publications of the Higher Attestation Commission of the Russian Federation

Included in the Ulrich's Periodicals Directory

Materials of the journal are placed on the RSCI platform of the Russian scientific electronic library – Electronic Journals Library Cyberleninka

Subscription index of the journal in the Rospechat Agency catalogue is: 70035

Objectives and themes

Academic journal “Political Science Issues” is an international peer-reviewed scientific periodical in the field of political studies. The journal has an international character because of the composition of its Editorial Board, its editors, its contributing authors and topics of its publications.

The scientific journal is published since 2011 at the “Publishing House “Science Today”. Translated (eng.) version of the journal is published since 2016. Since its inception, the journal was guided by high scientific and ethical standards and today it is one of the leading political science journals in Russia.

The purpose of the journal is to promote scientific exchange and cooperation between Russian and foreign political scientists.

The journal is intended for the publication of the results of fundamental and applied scientific research. Thematic focus of the journal is reflected in the following permanent headings: “History and philosophy of politics,” “Political institutions, processes and technologies,” “Political regionalism and ethno-politics,” “Political culture and ideologies,” “Political problems of international relations and globalization.”

Format of publications: scientific articles, reviews, scientific materials, materials of round tables, scientific reviews, scientific reports devoted to research problems in the field of politics and political science.

The Editorial Board and the editors of the journal in their activities are guided by the principles defined by VAK of Russia for scientific journals, including: presence of the institute of peer review for the expert quality assessment of scientific articles; information openness of the publications; availability and compliance with the rules and ethical standards for the submission of manuscripts by the authors.

The target audience of the journal is Russian and foreign specialists-political scientists, as well as graduate students and masters in the fields of political science, state and municipal management and international relations.

The journal strictly adheres to the international publishing standards and publication ethics identified in the COPE (Committee on Publication Ethics) document. <http://publicationethics.org>.

Full details of the journal and its editorial policy, requirements to the preparation and publication of articles, archive (issues since 2011) and additional information are available on the website: <http://voprosplitolog.ru>

E-mail address: voprosplitolog@yandex.ru

СОДЕРЖАНИЕ

ИСТОРИЯ И ТЕОРИЯ ПОЛИТИКИ

- Йозеф Храбина.** The Problem of Stability and Durability of Multipolar Structures/Проблема устойчивости и надежности многополярных структур.....10
- Добромыслов А.С.** Демографические исследования в рамках политической науки.....17

ПОЛИТИЧЕСКАЯ ИСТОРИЯ РОССИИ

- Чемшиш А.А., Стаценко О.С., Чемшиш Д.А.** О цивилизационной гордости великороссов.....22

ПОЛИТИЧЕСКАЯ СОЦИОЛОГИЯ

- Чимирис Е.С.** Использование методики анализа фреймов для изучения доверия: опыт построения исследовательской модели..... 32
- Федотова В.А.** Идентичность как детерминанта доверия к власти и политической активности на примере российской молодежи.....47

ПОЛИТИЧЕСКИЕ ИНСТИТУТЫ, ПРОЦЕССЫ И ТЕХНОЛОГИИ

- Зимин В.А.** Мигранты на российском рынке труда56
- Малахов А.А.** Борьба с бедностью как этическая проблема и политическая стратегия..... 65
- Внук В.К.** Сравнительный анализ предвыборных программ парламентских политических партий на выборах в Государственную Думу ФС РФ VIII созыва 73
- Золотарев Н.А., Попов С.И., Гришин В.О.** Миграционные процессы как глобальное социально-политическое явление.....84

ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ И ОТРАСЛЕВЫЕ ПОЛИТИКИ

- Гончарова И.В.** Устойчивое развитие государства и социальные технологии..... 92
- Чижевский Я.А.** К вопросу о внедрении модели ценностно-ориентированного здравоохранения в России111

ТЕОРИЯ И ИСТОРИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ВНЕШНЕЙ ПОЛИТИКИ

- Михайленко А.Н., Храмова А.В.** Потенциал развития Евразийского экономического союза.....124
- Сурма И.В.** Североатлантический альянс и угрозы цифровому суверенитету России.....135
- Титов В.Б., Макаров А.В.** Комплексные подходы России к формированию образовательного пространства в геополитическом измерении.....148

Тушков А.А., Алехина А.П. Этико-философские учения как паттерн формирования культурной идентичности Китая	157
Бобров А.К. Циклы российско-американских отношений в постбиполярный период (1991-2021 гг.).....	164
Шангараев Р.Н. Перспективы российско-турецких отношений в контексте строительства канала «Стамбул» и напряженности в Черноморском регионе	181
Вафин А.М. Идеология государственного служения в Японии.....	188
Васецова Е.С., Фатхуллина Д.В. «Мягкая сила» во внешней политике Объединенных Арабских Эмиратов	196
Кичаев П.А., Малик Е.Н. Политическая система Афганистана в новой архитектуре международных отношений	201
Осташова Я.В. Инструменты мягкой силы высшего образования России в контексте сотрудничества с Казахстаном	212
Телегин Д.С. Теоретические основы политики Соединенных Штатов Америки по сдерживанию Китайской Народной Республики в Индо-Тихоокеанском регионе	218
Бозоян Т.Р. Особенности политики АСЕАН в вопросе трудовой миграции	223
Аржанов И.А. Международно-правовой статус Арктики как элемент регионального геополитического соперничества	230
Власенко К.А. Сравнительный анализ санкционных политик ЕС и США	237
Гао Дай. Вейбо как инструмент общественного надзора в Китае	244
Финкельзон С.С. Реакция израильских харедим на борьбу с пандемией COVID-19 в стране.....	250
У Яньбинь. Основа геополитической концепции «Индо-Тихоокеанского региона»	267
Санжиева А.Д. Агентство цифровизации Японии как актор цифровой трансформации государства.....	273
Басов О.Н. Инструменты внутриэлитной борьбы за политическую власть и влияние с участием некоммерческих организаций (на примере современных США).....	280
Хазели Реза. Международная трудовая миграция и трансферты мигрантов	294
Баракат Кайс Абдулла Махмуд, Сеифи Мустафа Салеем Мустафа, Абахра Мушир Ибрагим Хасан. Палестино-израильский конфликт в контексте внешней политики России.....	301

СТУДЕНЧЕСКАЯ НАУКА

Тарасочкина Д.Д., Степанькова Д.С., Зряева Е.С. Дискурс-анализ в исследовании СМИ на примере прессы в странах Северо-Восточной Азии.....	307
---	-----

<i>Баранова Ю.В., Леонова А.А., Фам Тхи Минь Хуен.</i> Проблемы международно-правового регулирования предотвращения загрязнения морской среды в Северной Пацифике	314
<i>Кражан А.С.</i> Актуальность введения антикоррупционного комплаенс-контроля в российский бизнес.....	321
<i>Дубинин А.А.</i> Терроризм в Сахельском регионе: опыт Франции и новые вызовы	327
НАШИ АВТОРЫ	336
ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ РУКОПИСЕЙ	345
РЕДАКЦИОННЫЙ СОВЕТ	347

кандидат экономических наук,
заведующий кафедрой государственного управления
во внешнеполитической деятельности Дипломатической
академии МИД РФ, член-корреспондент РАЕН,
Россия, г. Москва

СЕВЕРОАТЛАНТИЧЕСКИЙ АЛЬЯНС И УГРОЗЫ ЦИФРОВОМУ СУВЕРЕНИТЕТУ РОССИИ

Представлены основные действующие киберструктуры и Центры передового опыта НАТО, показана их ключевая функция в подготовке международно-правовых обоснований милитаризации киберпространства. Показана роль координационно-технического центра Сил реагирования НАТО на компьютерные инциденты NCIRC (National Criminal Intelligence Resource Center), обеспечивающего киберзащиту всех информационных ресурсов НАТО. Отмечается потенциал Центра стратегических коммуникаций (NATO Strategic Communications Centre of Excellence), соучредителями которого явились Латвия, Литва, Эстония, Польша, Германия, Италия и Великобритания, а основными функциями этого центра в Риге стали работа со СМИ, информирование о деятельности НАТО с помощью инструментов публичной дипломатии, развитие гражданско-военных связей и проведение информационно-психологических операций. Представлена российская позиция по вопросам обеспечения международной информационной безопасности и цифрового суверенитета государства. Рассмотрена российская система противодействия кибератакам, важную роль в которой выполняет Центр реагирования на компьютерные инциденты в информационно-телекоммуникационных сетях органов государственной власти России, который координирует действия организаций и ведомств в области предотвращения, выявления и ликвидации последствий компьютерных инцидентов. Автор отмечает, что у границ России традиционные и кибернетические войска Североатлантического альянса никого не защищают, а наоборот разрабатывают и планируют новые ударные, десантные и наступательные операции.

Ключевые слова: Агентство НАТО по связи и информации, НАТО, Центр Сил реагирования НАТО на компьютерные инциденты, кибервойны, социально-политическая дестабилизация, цифровой суверенитет, международная информационная безопасность.

В настоящее время информационно-коммуникационная инфраструктура НАТО охватывает более 60 различных объектов, начиная от военно-политической штаб-квартиры в Брюсселе и военного командования, и заканчивая объектами конкретных операций НАТО. Более 100 тысяч человек непосредственно работают в информационных сетях Североатлантического альянса, которые за последнее десятилетие все чаще и чаще становятся объектом для кибератак.

Настроенные системы киберзащиты НАТО ежедневно регистрируют сотни тысяч подозрительных действий: от попыток проникновения невысокого уровня, до технологически сложных атак на информационные сети НАТО. Практически большая часть таких атак обнаруживается и обрабатывается автоматически. Но, тем не менее, некоторые из них требуют дополнительного анализа и ответной реакции экспертов [17]. Сформированная команда киберспециалистов из двухсот человек обеспечивает круглосуточную защиту информационно-коммуникационной сети НАТО. Эта команда предотвращает несанкционированный доступ, обнаруживает, анализирует и обменивается информацией о кибератаках и вредоносных программах, предотвращает потерю данных и проводит компьютерную экспертизу, анализ и оценку уязвимостей, включая пост инцидентные расследования.

В современном информационном мире у любого международного конфликта имеется кибернетическая составляющая, но критерии и точность определения противника, признаков его агрессии и начала ответной (превентивной) операции выглядят достаточно расплывчато, так как, например, правовые основы для DDoS-атак отсутствуют, а из-за сложности атрибуции кибератак под удар могут попасть непричастные к ней страны.

С другой стороны, наиболее серьезным киберпротивником может являться государство, входящее, как минимум, в пятерку «Глобального индекса кибербезопасности», а это США, Великобритания, Франция, Литва и Эстония. Россия или Китай не попадают даже в первую десятку. Например, численность кибервойск в США – 19 тысяч, в Германии – 12 тысяч, в России – около 1 тысячи военнослужащих.

У границ России традиционные и кибернетические войска Североатлантического альянса никого не защищают, а наоборот разрабатывают и планируют ударные, десантные и наступательные операции. А ядерная держава может оказаться уязвимой для кибернетических диверсий против АЭС, космических систем и систем ПВО-ПРО, ударных ракетных комплексов. Поэтому в Российской Федерации осенью 2019 г. все оперативно-тактические комплексы «Искандер-М» были интегрированы в единую сеть управления с подключением «военному интернету» и готовы получать боевую задачу в режиме реального времени. А эта система может стать целью для кибератак, технологии которых вероятнее всего отрабатывают на учениях НАТО Cyber Coalition (1).

Центры передового опыта НАТО. Следует отметить, что ключевую роль в подготовке международно-правовых обоснований милитаризации киберпространства играют Центры передового опыта НАТО (Centres of Excellence), которые отвечают также за проведения международных конференций и крупномасштабных киберучений. Всего в настоящее время у альянса действует 19 таких полноценных центра и три находятся еще в стадии формирования. Все специализированные центры разбросаны по миру, главным образом распределены по Европе и находятся под управлением штаб-квартиры НАТО в Брюсселе [14]. Особенности и специфика этих центров позволяют глубже закрепляться в различных странах, включая государства, не являющиеся членами альянса, вовлекая при этом в свой процесс как военных, так и гражданских лиц этих стран.

Наиболее яркими примерами центров передового опыта могут являться центры, открытые НАТО в Эстонии, Литве и Латвии [11]. В Таллине еще в 2008 г. был создан Объединенный Центр в области киберобороны НАТО (CCD COE) имеющий полноценный статус военной организации. Уникальность этого центра состоит в том, что в нем одновременно работают военные, гражданские лица и представители правительства. Главные функции этого Центра: техническая подготовка и обучение специалистов, консультирование и проведение исследований в сфере кибербезопасности и международного информационного права, а также организация курсов по правовым аспектам действий в киберпространстве. Так как общепризнанных международных норм и правил поведения в Интернет-пространстве до настоящего времени еще не выработано, работа центра в Таллине направлена на то, чтобы в ускоренном режиме внедрить западную, прежде всего американскую, точку зрения и подходы к правовым аспектам поведения в Интернете. Так в 2013 году Объединенный Центр в области киберобороны НАТО (CCD COE) в Таллинне опубликовал так называемое Таллиннское руководство по вопросам применения международного права к условиям конфликтов в киберпространстве (Tallinn Manual 2013) [18]. На 300-х страницах документа по сути легитимируются конфликты в киберпространстве как форма поведения стран и действующих в их интересах посредников. Ряд положений руководства фактически санкционирует применение широкого спектра кинетического оружия против источников киберугроз, а также силовые действия военных по отношению к гражданским лицам, причастным к кибератакам (причисляя их к комбатантам), и военные кибероперации, направленные против критических информационных инфраструктур. Можно сделать вывод, что Таллиннское руководство пытается формировать международно-правовую базу для ведения наступательной кибервойны, активно связывая правила ведения кибервойн с системой международного права, делая акцент на проактивных операциях, на кибернападении. Именно против этого выступают российские эксперты, отстаивая позицию России и ее

партнеров о недопустимости информационных войн и голосуя против легитимации конфликтов в информационном пространстве и за предотвращение использования информационно-коммуникационных технологий в военных целях.

Следующая итерация, вышедшая в феврале 2017 г. – Таллиннское руководство – 2.0 (Tallinn Manual 2.0, 2017) [19], практически, как и другие многочисленные разработки Центра в области киберобороны НАТО, показали, что позиция Североатлантического альянса существенно не меняется.

Следует отметить, что центр в Таллине не выступает операционно-функциональным подразделением по борьбе с киберпреступниками, но здесь проводятся тренинги для специалистов разных стран, которые в последствие обеспечивают национальную кибербезопасность своих государств, а также обмениваются информацией с НАТО и партнерами. К тому же, Таллинский центр, являясь лидером европейской кибербезопасности и имея аккредитацию НАТО, формально не входит в его организационно-командную структуру, но, тем не менее, он оказывает существенное влияние на действия альянса в области защиты от киберугроз. Начиная с 2012 г. центр передового опыта НАТО в Таллине на регулярной основе организует киберучения, привлекая к ним не только страны-члены НАТО.

В Риге с января 2014 г. начал свою работу другой центр передового опыта НАТО – Центр стратегических коммуникаций (NATO Strategic Communications Centre of Excellence), соучредителями которого выступили Латвия, Литва, Эстония, Польша, Германия, Италия и Великобритания и который получил официальную аккредитацию в сентябре этого же года. Идея стратегической коммуникации стала новой концепцией, включающей в себя целый спектр возможностей публичной дипломатии и общественных отношений, начиная от убеждений при помощи информационно-психологических операций и заканчивая непосредственно применением силы.

Основными функциями центра в Риге являются работа со СМИ, информирование о деятельности НАТО с помощью инструментов публичной дипломатии, развитие гражданско-военных связей и проведение информационно-психологических операций. Рижский центр регулярно организует различные конференции, издает журналы и публикует доклады о результатах проведенных исследований. Сектор рассматриваемых проблем включает различные аспекты, такие как [8]:

1) особенности тактики ведения информационной войны с применением «мемов»;

2) кибервойна;

3) основные нарративы экстремистских организаций;

4) безопасность в Европейском союзе;

5) биометрические технологии;

6) национализм и др.

В работе центра передового опыта в Риге России уделяется достаточно пристальное внимание. Изучаются особенности применения современных информационных технологий в российской армии. Кроме того, публикуются материалы о якобы «российском вмешательстве на Украине», а также обзоры санкций против России. Продвигая мысль об активном вмешательстве России и о ведении ею гибридной войны [15], Рижский центр стратегической коммуникации НАТО (STRATCOM) ранее опубликовал несколько аналитических исследований «Кремлевский Сборник Пьес. Понимание российского влияния в Центральной и Восточной Европе» [4], «Когда гибридная война поддерживает идеологию: Россия сегодня» [3] и «Кибервойна Путина: государственная политика России в пятой области» (2016) [13], а также исследования о военных маневрах России (2020) [2].

В Вильнюсе еще в 2012 г. начал свою работу центр передового опыта в области энергетической безопасности. Ключевыми задачами Вильнюсского центра являются: экспертная оценка и аналитика, на основании которой вырабатываются рекомендации по широкому спектру вопросов энергетической безопасности, а также сотрудничество и взаимодействие между научными и академическими кругами и промышленным сектором, включая военную логистику и помощь стратегическому командованию НАТО, странам-членам и партнерам. Кроме того, центр проводит курсы и организует студенческие практики, причем расходы по практике и проживанию студентов оплачивает альянс. Центр издает несколько тематических журналов, основная направленность которых связана с необходимостью избавиться от «российской энергетической зависимости». Также постоянной темой является угроза энергетической безопасности Украины, исходящая от России. Поэтому на проводимых мероприятиях и материалах центра, внимание акцентируется на «энергетической войне» с Россией. При этом вовлекаются в сферу интересов альянса государства, не входящие в НАТО, и, как правило, расположенные на границах с Россией (например, конференция, организованная в ноябре 2018 г. при участии министерства обороны Грузии, была посвящена инновационным решениям в энергетике для применения в военной сфере» и др.).

Отметим, что в работе центров передового опыта НАТО в прибалтийских странах принимают активное участие различные мозговые центры, такие как британский Королевский институт международных отношений (Chatham House), корпорация РЭНД (RAND Corporation), Центр стратегических и международных исследований в Вашингтоне (Center for Strategic and International Studies или CSIS), а также специальные научные центры ряда стран-членов НАТО [9].

Еще одна сторона медали заключается в том, что эти же центры – центры киберразведки, действующие под контролем НАТО в Польше, Таллине и Риге, уже долгие годы ведут антироссийскую деятельность. Эти центры

являются центрами стратегической пропаганды НАТО, ключевая задача которых состоит в мониторинге социально-политической обстановки внутри России, вербовка россиян, готовых заниматься подрывом российских государственных устоев, и планирование информационных операций для дестабилизации социально-политической обстановки внутри страны [6].

Цифровой суверенитет и российская практика противодействия кибератакам [10]. В действительности «кибероборону» НАТО правильней называть наступательными операциями в киберпространстве против России и ее союзников. Именно через центры НАТО шли кибератаки на гражданскую инфраструктуру нашей страны, волны звонков о «минировании» объектов, фейковые вбросы во время объявленной ВОЗ пандемии COVID-19 и активные сетевые воздействия. Последняя масштабная кибероперация проводилась против Республики Беларусь накануне и после президентских выборов в июле-сентябре 2020 года. Примечателен тот факт, что во время протестов в Белоруссии, когда правительство республики ограничило доступ в социальные сети, видео с «ужасными преступлениями силовиков» оперативно переправлялись в Интернет через ресурсы посольств Польши, Литвы и Украины.

Цель такой дестабилизации общественно-политической ситуации в стране состоит в генерировании протестного потенциала в обществе и создание политической сингулярности, что приводит к инфляции власти, ее дискредитации и т.д. После прохождения точки политической нестабильности государство должно либо качественно измениться, либо быть уничтожено. При этом используются кибератаки с высоким уровнем социального инжиниринга и применением комбинированных систем, включающих возможности искусственного интеллекта и различные роботизированные устройства (боты). В число задач кибервойны входит, помимо нанесения ущерба инфраструктуре противника, и защита собственных данных, вследствие этого обеспечение кибербезопасности является неотъемлемой частью таких противостояний. Кибервойна представляет собой один из видов информационной войны, направленной на достижение определенных целей в политической, экономической, социальной, военной и других областях через воздействие на власти и общество информацией, специально подготовленной для этой цели.

Поэтому сегодня информационные ресурсы России комплексно включают в себя информационно-телекоммуникационные сети, информационные и автоматизированные системы управления, находящиеся, как на территории государства, так и в дипломатических представительствах и консульских учреждениях Российской Федерации в мире. В России для предотвращения компьютерных инцидентов и кибератак на эту критическую государственную информационную систему Указом Президента России от 15 января 2013 г. № 31с301 [12] было предусмотрено создание «Государственной системы

обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА). В дальнейшем на базе этого Указа была подготовлена и утверждена Президентом России Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (12 декабря 2014 г. № К 1274) [5].

ГосСОПКА – это единый территориально распределенный комплекс, в который входят силы и средства, необходимые для обнаружения, предупреждения и ликвидации последствий компьютерных атак и оперативного реагирования на компьютерные инциденты. В целях дальнейшего совершенствования и развития этой государственной системы и в соответствии с 6-ой статьей Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» был принят указ Президента РФ от 22.12.2017 №620, в рамках которого ответственность за функционирование системы ГосСОПКА возлагается на Федеральную службу безопасности РФ, а сама система предназначена для выполнения четырех ключевых задач:

- 1) контроль степени защищенности информационных ресурсов РФ от кибератак;
- 2) взаимодействие организаций-владельцев информационных ресурсов, включая субъектов критической информационной инфраструктуры, в ходе работ по обнаружению, предупреждению и ликвидации последствий кибератак;
- 3) прогнозирование в области информационной безопасности России;
- 4) расследование компьютерных инцидентов.

Отметим, что ключевую роль в системе выполняет Центр реагирования на компьютерные инциденты (Computer Emergency Response Team – CERT) в информационно-телекоммуникационных сетях органов государственной власти России (GOV-CERT.RU), который координирует действия организаций и ведомств в области предотвращения, выявления и ликвидации последствий компьютерных инцидентов. Прежде всего GOV-CERT.RU осуществляет реагирование на различные компьютерные инциденты, связанные с объектами информационной инфраструктуры России, принадлежащие органам государственной власти и объектам, размещенным в сегменте RSNET (Russian State Network) сети Интернет.

Отдельную роль в системе российских центров противодействия компьютерным инцидентам занимает RU-CERT, основная задача которого заключается в минимизации уровня угроз информационной безопасности для пользователей российского сегмента сети Интернет и оказание помощи российским и зарубежным юридическим и физическим лицам при предупреждении, выявлении и пресечении противоправной деятельности по отношению к размещенным на территории Российской Федерации сетевым ресурсам.

Кроме того, RU-CERT входит в состав международных объединений CSIRT/CERT центров FIRST и Trusted Introducer (своего рода МЧС в цифровом мире), и в рамках данных объединений является официальной контактной стороной в России.

Рассматривая в целом российскую позицию по вопросам международной информационной безопасности (МИБ), следует отметить, что Генеральная Ассамблея ООН 5 декабря 2018 г. приняла российскую резолюцию по МИБ «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/73/27) [16], соавторами которой были 30 стран из всех регионов мира и которая была поддержана подавляющим большинством государств. Данный этап открыл следующую страницу глобальной дискуссии по МИБ и Генеральной Ассамблее удалось принять ряд решений, направленных на укрепление этой дискуссии [7]. Ключевая идея заключается в защите интересов всех стран в цифровой сфере, причем независимо от их уровня информационно-технологического развития. С исторической точки зрения это инновационный документ, включающий тринадцать правил, норм и принципов ответственного поведения стран в информационном пространстве, основная задача которых создать базу мирного сосуществования государств в нем и обеспечить предотвращение конфронтации, войн и любых агрессивных действий. Заслуживают внимания такие нормы, как обязательства соблюдать в информационном пространстве принцип государственного суверенитета и использовать информационно-коммуникационные технологии исключительно в мирных целях, сотрудничать в борьбе с применением современных технологий в преступных и террористических целях, а также предотвращать распространение скрытых вредоносных функций в ИТ-продукции (то есть, так называемых «закладок»).

Важным является тот факт, что в принятом документе закрепляются следующие базовые принципы:

- 1) государства несут главную ответственность за поддержание безопасной и мирной информационной среды;
- 2) ООН должна играть ведущую роль в дискуссиях по международной информационной безопасности;
- 3) любые обвинения в злонамеренном использовании информационно-коммуникационных технологий (ИКТ) должны быть доказаны;
- 4) государства не должны использовать посредников для злонамеренного применения ИКТ;
- 5) суверенитет государств и международные нормы и принципы, происходящие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над интернет-инфраструктурой, расположенной на их территории.

Кроме того, Россия инициировала демократический подход к переговорному процессу по международной информационной безопасности на пло-

щадке ООН, сделав его более открытым и прозрачным и предложив с этой целью в рамках Организации создать рабочую группу открытого состава (РГОС). В работе этой группы смогут участвовать все без исключения страны-члены ООН. РГОС будет рассматривать широкий спектр вопросов обеспечения международной информационной безопасности. Приоритетное направление работы РГОС будет уделяться нормам, правилам и принципам ответственного поведения в информационном пространстве, вопросам применимости международного права в этом пространстве и развитию цифрового потенциала развивающихся стран. В отличие от прежней группы правительственных экспертов (ГПЭ) ООН новая структура является полноценным органом Генеральной Ассамблеи, который может вырабатывать и рекомендовать государствам-членам любые документы вплоть до проектов международных соглашений и договоров. С одной стороны, такая группа повышает сам статус дискуссии по международной информационной безопасности, а с другой, подобная переговорная структура ООН получает такой мандат впервые в мировой практике.

Новой особенностью мандата, предоставленного РГОС, стала возможность проведения регулярного институционального диалога под эгидой ООН с широким кругом участников. Рабочая группа должна рассмотреть возможность создания постоянно действующей переговорной структуры по МИБ. Еще одной важной особенностью резолюции Генеральной Ассамблеи ООН является впервые предусмотренный механизм межсессионных консультаций РГОС с негосударственными акторами – бизнесом, неправительственными организациями и научным сообществом – для обмена взглядами по вопросам международной информационной безопасности, что позволяет подключить к обсуждению специалистов и экспертов по принципиально важным аспектам использования ИКТ.

К сожалению, противопоставив себя международному сообществу США и страны-члены ЕС коллективно выступили против инновационных идей. Именно эти страны формируют в медийном пространстве атмосферу недоверия и распространяют обвинения в кибератаках в адрес других государств. Таким образом, они не заинтересованы в придании переговорному процессу по теме обеспечения международной информационной безопасности честного и открытого для всех участников характера и в реальности преследуют собственные цели [1. С. 44-54]. Этим и объясняется начало работы в конце 2019 г. новой группы правительственных экспертов на основе справедливого географического распределения, инициированной США в рамках Резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности». Российская Федерация высказала свое мнение о взаимном сотрудничестве и выступила за координацию и взаимодействие этих групп, но США пока молчат. Однако сам феномен принятия двух ре-

золюций Генеральной Ассамблеи ООН по одной и той же тематике еще раз подчеркивает высокую значимость и актуальность проблемы обеспечения международной информационной безопасности.

Показательно, что в настоящее время более 140 государств мира разрабатывают свои собственные стратегии кибербезопасности и программы ведения кибервойны, а это значительно подрывает информационную стабильность, поскольку оперативно обнаружить источник информационной атаки достаточно сложно, а последствия ее могут стать причиной ответного удара, в том числе с использованием не только обычных видов вооружений. В этих условиях весьма актуальна позиция Российской Федерации, предлагающей выработать конструктивные правила ответственного поведения стран в информационном поле и демилитаризировать информационное пространство с целью обеспечения международной безопасности. И перед внешнеполитическим ведомством нашей страны сегодня встают задачи совершенствования инструментов внешней политики для более эффективной работы на различном международном уровне с целью продвижения российской позиции по вопросам международной информационной безопасности.

В заключение подчеркнем, что чрезвычайно важной линией киберполитики НАТО и коллективного Запада, вообще, является восприятие Российской Федерации как одного из главных агрессоров в киберпространстве. Более того, они имеют достаточно согласованную позицию и политику по вопросам кибербезопасности. Экспертные сообщества и политический истеблишмент стран Запада склонны обвинять Россию в организации массовых кибератак на их информационную инфраструктуру. Тем не менее, позиция Запада основывается на многочисленных и порой противоречащих друг другу идеях, включая различия в подходах к обеспечению кибербезопасности, особенно в вопросах активной киберзащиты и ответных мер. Каждая страна имеет достаточно четкую позицию по этим вопросам, определяемую, прежде всего, национальными интересами. Но так как Интернет не признает государственных границ, поэтому будущее как национальной, так и международной кибербезопасности будет зависеть от того, насколько государства будут готовы к конструктивному диалогу и сотрудничеству в решении актуальных проблем информационной безопасности.

ПРИМЕЧАНИЯ:

(1) НАТО только в 2019 г. было проведено 335 разных видов учений и большинство из них у границ России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Аникин В.И., Абдеев Р.Ф., Сурма И.В. Философские аспекты информационной цивилизации и современные проблемы управления в ракурсе глобальной безопасности // Вопросы безопасности. 2017. № 2.

2. Бартош А. Гибридные войны в стратегии США и НАТО // <https://top-war.ru/60101-gibridnye-voyny-v-strategii-ssha-i-nato.html>.
3. Когда Гибридная Война Поддерживает Идеологию // Russia Today // <https://www.stratcomcoe.org/when-hybrid-warfare-supports-ideology-russia-today>.
4. Конли Дж. Мина, Стефанов Р., Владимиров М. «Кремлевский Сборник Пьес. Понимание российского влияния в Центральной и Восточной Европе» // <https://www.stratcomcoe.org/hconley-jmina-rstefanov-mvladimirov-kremlin-playbook-understanding-russian-influence-central-and>.
5. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Утверждена Президентом РФ 12.12.2014 № К 1274 // Справочно-правовая система «Консультант Плюс» // http://www.consultant.ru/document/cons_doc_LAW_181661/7327668c04c0470317b26d354e36cb828a4af319/.
6. Москва знает о центрах антироссийской пропаганды в Прибалтике – мнение // <https://regnum.ru/news/polit/3341326.html>.
7. Резолюция Генеральной Ассамблеи ООН 73/266 от 22 декабря 2018 года. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности // <https://undocs.org/ru/A/RES/73/266>.
8. Смирнов А.И. Новейшие киберстратегии США – преамбула войны? // Международные процессы. 2018. Том 16. № 4 (55).
9. Смирнов А.И. Современные информационные технологии в международных отношениях: монография. Москва: МГИМО-Университет, 2017.
10. Сурма И.В. Цифровая дипломатия в дискурсе глобальной политики // Вестник МГИМО Университета. 2014. № 6 (39).
11. Сурма И.В. Международные исследовательские центры по проблемам войны, мира и безопасности // В сборнике: Государственное управление во внешнеполитической деятельности и международная безопасность. Москва, 2013.
12. Указ Президента России от 15 января 2013 г. № 31 с. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Информационно-правовой портал «ГАРАНТ.РУ» // <https://www.garant.ru/products/ipo/prime/doc/70199068/>.
13. Фоксхолл А. «Кибервойна Путина: государственная политика России в пятой области» // <https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain>.
14. Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018 // https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
15. Hybrid Threats Description 1500/CPPCAM/FCR/10-270038 AND 5000 FXX/0100/TT-0651/SER: NU0040 Dated 25 August 2010: BI-SC Input for a new

Capstone Concept for The Military Contribution to Countering Hybrid Threats dated (para 7) // https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

16. Resolution adopted by the General Assembly on 5 December 1973. 73/27. Developments in the field of information and telecommunications in the context of international security // <https://undocs.org/A/RES/73/27>.

17. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization // https://www.nato.int/cps/ru/natohq/topics_82705.htm.

18. Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt. Cambridge University Press, 2013.

19. Tallinn manual 2.0 on the international law applicable to cyber operations / ed. by M.N. Schmitt. Cambridge University Press, 2017.

I.V. SURMA

*Candidate of Economic Sciences,
Head of the Department of Public Administration
in Foreign Policy of the Diplomatic Academy of the Ministry
of Foreign Affairs of the Russian Federation, Ph.D. Corresponding
Member of the Russian Academy of Natural Sciences,
Moscow, Russia*

THE NORTH ATLANTIC ALLIANCE AND THREATS TO RUSSIA'S DIGITAL SOVEREIGNTY

The main operating cyber structures and NATO Centers of Excellence are presented, their key function in the preparation of international legal justifications for the militarization of cyberspace is shown. The role of the NCIRC (National Criminal Intelligence Resource Center), the coordinating and technical center of the NATO Computer Incident Response Force, which provides cyber protection for all NATO information resources, is shown. The potential of the Center for Strategic Communications (NATO Strategic Communications Center of Excellence), co-founded by Latvia, Lithuania, Estonia, Poland, Germany, Italy and the United Kingdom, is noted, and the main functions of this center in Riga are working with the media, informing about NATO activities using tools public diplomacy, the development of civil-military relations and the conduct of information and psychological operations. The Russian position on the issues of ensuring international information security and digital sovereignty of the state is presented. The Russian system of counteracting cyberattacks is considered, in which an important role is played by the Center for Response to Computer Incidents in the Information and Telecommunication Networks of the Government

of Russia, which coordinates the actions of organizations and departments in the field of preventing, detecting and eliminating the consequences of computer incidents. The author notes that the traditional and cybernetic troops of the North Atlantic Alliance do not protect anyone near the borders of Russia, but rather develop and plan new strike, landing and offensive operations.

Key words: *NATO Communications and Information Agency, NATO, NATO Response Force Center for Computer Incidents, cyber warfare, socio-political destabilization, digital sovereignty, international information security.*