ВОПРОСЫ ПОЛИТОЛОГИИ

ВЫПУСК 1(65), 2021

Научный журнал

Журнал «Вопросы политологии» включен
в Перечень рецензируемых научных изданий
ВАК Министерства образования и науки 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, 2021

ВОПРОСЫ ПОЛИТОЛОГИИ

Научный журнал

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

АСТАЦАТУРОВА
Майя Арташесовна

д.п.н., профессор, директор Центра этнополитических исследований, профессор кафедры креативно-инновационного управления и права Пятигорского государственного университета, координатор Сети этнологического мониторинга и раннего предупреждения конфликтов в СКФО (Россия, г. Пятигорск)

БОЖАНОВ
Владимир Александрович

д.и.н., профессор, зав. кафедрой мировой и отечественной культуры Белорусского Национального технического университета (Белоруссия, г. Минск)

ВЕДРИН
Оливье

профессор, главный редактор русской версии французского журнала «Национальная оборона» (Revue Défense Nationale), спикер Европейской комиссии, редактор франко-германского журнала по вопросам внешней политики «European Union Foreign Affairs Journal» и ректор «Континентального университета в Киеве» (Франция, г. Париж)

ДОНАЙ
Лукаш

д.п.н., профессор факультета политологии и журналистики Департамента международных отношений Университета им. Адама Мицкевича в Познани (Польша, г. Познань)

ЖИЛЬЦОВ
Сергей Сергеевич

д.п.н., заведующий кафедрой политологии и политической философии Дипломатической академии МИД РФ (Россия, г. Москва)

ИРХИН
Юрий Васильевич

д.ф.н., профессор кафедры политологии и политического управления РАНХ и ГС при Президенте РФ (Россия, г. Москва)

КАРАДЖЕ
Татьяна Васильевна

д.ф.н., заведующая кафедрой политологии и социологии МПГУ (Россия, г. Москва)

КЕТЦЯН
Григор Ваникович

к.п.н., заместитель Главного редактора журнала, Председатель Попечительского Совета научного журнала «Вопросы политологии» (Россия, г. Москва)

КОВАЛЕНКО
Валерий Иванович

д.ф.н., зав. кафедрой российской политики МГУ им. М.В. Ломоносова (Россия, г. Москва)

КРИВОКАПИЧ
Борис

д.ю.н., профессор факультета бизнеса и права Унион – Никола Тесла университета (Сербия, Белград)

МЕДВЕДЕВ
Николай Павлович

д.п.н., профессор кафедры анализа и управления Российского университета дружбы народов, главный редактор журнала (Россия, г. Москва)

МИХАЙЛОВ
Вячеслав Александрович

д.и.н., зав. кафедрой национальных и федеративных отношений РАНХ и ГС при Президенте РФ (Россия, г. Москва)

НАСИМОВА
Гульнара Орленбаевна

д.п.н., профессор, зав. кафедрой политологии факультета философии и политологии Казахского Национального университета им. Аль-Фараби (Казахстан, г. Алматы)

НИСНЕВИЧ
Юлий Анатольевич

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

ПАХРУТДИНОВ
Шукритдин Ильясович

д.п.н., профессор, заведующий кафедрой основы духовности Института переподготовки и повышения квалификации руководителей и специалистов системы народного образования имени А. Авлони (Узбекистан, г. Ташкент)

ПЛЯЙС
Яков Андреевич

д.и.н., д.п.н., профессор Финансового университета при Правительстве РФ (Россия, г. Москва)

ПРЯХИН
Владимир Федорович

д.п.н., профессор кафедры зарубежного регионоведения и внешней политики РГГУ (Россия, г. Москва)

ПУСЬКО
Виталий Станиславович

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

ХОПЁРСКАЯ
Лариса Львовна

д.п.н., профессор кафедры международных отношений Киргизско-Российского славянского университета, (Киргизия, г. Бишкек)

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)

ISSN 2225–8922

**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

Рег. № 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 1, 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 25.01.2021
Формат 60×84/8. Объем 24,3.
Печать офсетная.
Тираж – 1000 экз.
(1-й завод – 500 экз.)
Заказ № 0000

Отпечатано
в типографии PrintUP
117105, г. Москва,
Нагорный проезд, 12, корп. 1
Тел.: +7 (495) 925-00-06

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

ТЕОРИЯ, ФИЛОСОФИЯ И ИСТОРИЯ ПОЛИТИКИ

<i>Ирхин Ю.В.</i> Переосмысление идей Кейнса и Рузвельта о государственном управлении в условиях пандемического кризиса и опыта России.....	10
<i>Федорищев К.М.</i> Элементы августицизма в политической теории Майкла Оукшотта.....	19

ПОЛИТИЧЕСКИЕ ИНСТИТУТЫ, ПРОЦЕССЫ И ТЕХНОЛОГИИ

<i>Ермаков Ю.А.</i> Зарождение и умножение коррупции в общественно- политических иерархиях: роль природных начал.....	25
<i>Алехнович С.О., Воронцов С.А., Понеделков А.В.</i> Актуальные проблемы противодействия коррупции в современной России: информируем и обсуждаем	44
<i>Великая Н.М., Моисеева А.Н.</i> Оценки эффективности деятельности органов местной власти: методология и методика	54
<i>Гоптарева И.Б.</i> Лоббизм в публичной политике.....	65
<i>Прончев Г.Б., Шишарина Е.В., Прончева Н.Г.</i> Киберугрозы для современной России в контексте пандемии коронавирусной инфекции	74
<i>Сурма И.В.</i> Информационная экспансия Запада в странах Центральной Азии	84
<i>Тушков А.А., Фоменко Д.А.</i> Поиск баланса интересов глобальных стран среди двух конкурирующих «евразийских проектов».....	96
<i>Вафин А.М.</i> Негатив в политике: 10 технологий «черного» PR в России и зарубежных странах.....	107
<i>Отроков О.Ю.</i> Современные тенденции, проблемы и перспективы развития интернет-каналов информирования молодежи с политической повесткой.....	115
<i>Овчинников П.С., Нечай Е.Е.</i> Ключевые барьеры на пути трансформации социально-политической системы России	124
<i>Еременко Ю.А., Жаворонкова З.А.</i> Эмоциональные триггеры внимания и запоминаемости визуального политического контента	130
<i>Ершов Н.А., Омерович А.Р., Попов С.И.</i> Протестный потенциал как инструмент предвыборной кампании (часть I: выборы в Московскую городскую Думу 2019 года).....	140

Фалалеев М.А., Ситдикова Н.А., Нечай Е.Е. Видеостриминг как канал политической коммуникации: опыт современной России.....	147
Устюжанинов И.Д. Роль партии «Единая Россия» в региональной политике в 2002-2007 годах (на примере Кировской области).....	154
Ахмедов Ж.И. Легитимность власти как современный фактор угрозоустойчивости общества.....	162
Воскресенский Ф.А. Исследование судебной власти как элемента политической системы в странах континентальной и англо-саксонской (на примере США) систем права.....	169
Комаров Н.А. Историография межгосударственных отношений Российской Федерации и Республики Молдова в 2009-2018 гг.....	180

ПОЛИТИЧЕСКАЯ КОНФЛИКТОЛОГИЯ

Штанько М.А., Тажева З.Б. Управление этническим конфликтом	188
---	-----

МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ И МИРОВАЯ ПОЛИТИКА

Михайленко А.Н., Умеров Д.А. Модель гармонизации стратегии и тактики российской внешней политики	193
Кулешова Н.С., Санжиева А.Д. Кибербезопасность как условие цифровизации Японии	206
Жерлицына Н.А. Виртуальный халифат: медиа технологии «ИГИЛ»	216
Бикбулатов Э.А. Образ «Фабрики Троллей» в противостоянии политических партий США.....	227
Курилкин А.В. Китайский кибердракон: к вопросу о возможностях КНР по проведению информационных и киберопераций	234
Полтавцева О.Н. Анти-иммиграционная риторика в Италии и США: сравнительный анализ контента новых медиа Д. Трампа и М. Сальвини	240
У Яньбинь. Развитие и особенности военной дипломатии КНР после реформы и открытости	247
Будник А.И., Григорьева Т.В., Кан А.А. Позиции России и Японии вокруг Курильской территориальной проблемы	253

СТУДЕНЧЕСКАЯ НАУКА

Богданова Е.А., Тимершова А.С. Социально-политический кризис в Чили: от протестов к плебисциту.....	264
Бурова А.С. К вопросу об испано-американских отношениях в XX в.	271

РАЗМЫШЛЕНИЯ НАД ПРОЧИТАННЫМ

Слизовский Д.Е. Умножение коррупции: поиски оснований продолжаются
(рецензия на статью Ю.А. Ермакова «Зарождение и умножение коррупции
в общественно-политических иерархиях: роль природных начал»)..... 278

НАШИ АВТОРЫ286

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ РУКОПИСЕЙ 295

КИБЕРБЕЗОПАСНОСТЬ КАК УСЛОВИЕ ЦИФРОВИЗАЦИИ ЯПОНИИ

Исследование кибербезопасности актуально для Японии, так как страна не обладает достаточными технологиями в этой сфере и лишь в последнее время предпринимаются активные действия в данном направлении. Анализ уровня кибербезопасности страны и правительственных мер в области кибербезопасности значимы с точки зрения прогнозирования дальнейшего курса внутренней и внешней политики Японии. Изучение особенностей информационной защищенности страны также представляет большой интерес в научном и практическом аспекте. Таким образом, предмет нашего исследования – процесс обеспечения мер безопасности для сохранения конфиденциальности, целостности и доступности данных в Японии, рассматривается в ракурсе работ российских и японских ученых с использованием эмпирического материала.

Ключевые слова: кибербезопасность, цифровизация, Япония, политический процесс, информационная безопасность.

Распространение информационно-коммуникационных технологий в различных сферах жизнедеятельности современных обществ позитивно влияет на их стабильное развитие. Однако новые информационные вызовы и угрозы безопасности актуализируют проблему международной информационной безопасности, превращая ее практически в глобальную проблему, решение которой требует консолидированных усилий всех государств. Проблематика международной информационной безопасности находит отражение в деятельности и документах международных организаций и форумов: ООН, ОБСЕ, ШОС, ОДКБ, НАТО и др. Национальная политика государств, направленная на обеспечение информационной безопасности и междуна-

родное взаимодействие в данной сфере, все чаще является объектом исследования как на экспертном, академическом, так и на политическом уровне. Возрастающая роль информационной составляющей в обеспечении национальной безопасности и международной безопасности существенно актуализируют данную проблему.

Поскольку кибербезопасность Японии представляет собой проблему, мало исследованную российскими учеными, мы опираемся в основном на работы японских исследователей и политиков, доклады и статьи, опубликованные японскими правительственными органами, а также материалы, выпущенные международными организациями, такими, например, как Организация экономического сотрудничества и развития, Организация Североатлантического договора.

Целью нашего исследования является определение роли кибербезопасности на современном этапе развития японского общества в условиях осуществления крупномасштабной цифровизации.

В литературе термин «кибербезопасность» используется достаточно широко, его определения часто разнятся, привязаны к контексту, субъективны и иногда неинформативны. Существует мало работ с точным определением данного термина. Отсутствие лаконичной, общепринятой дефиниции, которая отражала бы многомерность кибербезопасности, потенциально препятствует технологическим и научным достижениям, укрепляя преимущественно технический взгляд на проблему. Данное обстоятельство требует разделения дисциплин и особенностей подходов для комплексного решения сложных вопросов в этой сфере. Анализ изученной литературы, позволяет сделать вывод, что в мировой японистике мало исследований по данной тематике, несмотря на то, что проблема кибербезопасности в Японии имеет большое значение и широко освещается в японских и англоязычных средствах массовой информации. В англоязычной литературе можно отметить исследование сотрудника Центра стратегических и международных исследований Джеймса Эндрю Льюиса «Сотрудничество США и Японии в области кибербезопасности», доклад Вильгельма М. Воссе «Кибердипломатия Японии» и другие.

Очевидно, что в современных условиях мирового развития набор технических решений, обеспечивающих кибербезопасность уже недостаточен, только эти меры не позволяют полностью урегулировать проблему информационной безопасности. Множество практических примеров и научных работ демонстрируют, что в экономике, социологии, политике и других областях знаний остается большое количество нерешенных вопросов, связанных с кибербезопасностью. Фредрик Чанг, бывший директор по исследованиям в Агентстве национальной безопасности США, говорит о междисциплинарном характере кибербезопасности следующее: «Наука кибербезопасности предлагает много возможностей для достижений, осно-

ванных на междисциплинарном подходе. Люди должны защищать машины, которые атакуют другие люди, использующие машины. Таким образом, в дополнение к таким важнейшим традиционным областям, как информатика, электротехника и математика, необходимы разработки из других сфер» [6]. В попытке прийти к более широкому приемлемому определению, которое могло бы соответствовать истинному междисциплинарному характеру кибербезопасности, мы рассмотрели соответствующую литературу, чтобы обозначить диапазон определений, а также выделить аспекты кибербезопасности. Изученная литература охватывает широкий спектр работ в разных областях знаний, включая информатику, инженерию, политические исследования, психологию, менеджмент и социологию. Наиболее информативны оказались труды по техническим дисциплинам. В меньшей степени проблема защиты в киберпространстве затрагивается в работах по политике, праву, государственному управлению, менеджменту, социологии.

Следует отметить, что в Японии публикуется большое количество работ по кибербезопасности, особенно выросло количество публикаций по безопасному пользованию Интернета, в которых кибербезопасность чаще рассматривается как обеспечение защиты от кибератак. Однако, в целом, японские авторы отмечают, что технические меры – это лишь часть системы кибербезопасности, основную задачу видят в создании безопасной интернет-среды для пользователей Интернета, информационного и коммуникационного оборудования.

Характеризуя основные концептуальные подходы к рассматриваемой проблеме, следует назвать работу Такаити Санаэ «Защитим жизнь от кибератак!», в которой отражено понимание проблемы японскими властями. Автор книги – бывший министр внутренних дел и коммуникаций, ее работа опубликована в 2018 году при поддержке Либерально-демократической партии Японии. По мнению автора Такаити Санаэ, низкий уровень кибербезопасности в стране особенно критичен в следующих областях: обмен информацией; воздушный и железнодорожный транспорт и логистика; медицина; предоставление коммунальных услуг; химия и нефтехимия; финансы; правительство и административные услуги; обеспечение безопасности государства.

С понятием «кибербезопасность» тесно связано понятие «киберпреступность». Национальное полицейское агентство Японии определяет киберпреступления как «преступления с использованием информационных технологий и коммуникационных сетей, и преступления, направленные на компьютерные или электромагнитные записи».

Хамуро Эйтаро, главный инспектор по кибербезопасности Национального полицейского агентства, представил в своей книге «Введение в кибербезопасность» классификацию киберпреступлений, среди них: акты несанкционированного доступа, действия, направленные на вмешательство

в работу компьютерных систем, фальсификация электромагнитных записей, реклама и создание пирамидальных финансовых схем, шантаж, клевета и т.д. [5. С. 4]. Автор книги также поясняет, что японские власти включают в понятия «кибератака» и «кибертерроризм», парализующие функционирование критически важных инфраструктур, и «киберинтеллект», способный похищать конфиденциальную информацию у государственных компаний.

Таким образом, у японских исследователей и политиков существует теоретическое наполнение термина «кибербезопасность», разработана подробная классификация видов киберпреступлений, издается соответствующая литература.

Значимость проблематики информационной безопасности для политики Японии подтверждает принятый в 2014 году Основной закон о кибербезопасности и другие государственные инициативы в этой сфере. Данным законом в Японии определяется основное толкование «кибербезопасности». Закон формулирует понятие следующим образом: «необходимые меры, которые следует предпринять, чтобы безопасно управлять информацией, например, предотвращение утечки, исчезновения или повреждения информации, которая хранится, отправляется, передается или принимается электронными, магнитными или другими средствами, не распознаваемыми естественными воспринимающими функциями, и гарантировать безопасность и надежность информационных систем, информации и телекоммуникационных сетей (включая необходимые профилактические меры против злонамеренных действий, направленных на электронные компьютеры через информационную сеть или средства хранения информации); и поддерживать их в исправном состоянии» [3].

Закон состоит из четырех глав: Основные положения, Стратегия по обеспечению кибербезопасности, Основная политика в отношении кибербезопасности, Стратегические штабы по кибербезопасности. Каждая глава состоит из нескольких статей, всего в законе 35 статей.

В первой главе японские законодатели определяют главную цель закона – всестороннее и эффективное продвижение национальной политики в области кибербезопасности в условиях развития современных информационно-коммуникационных сетей и технологий, в условиях усиления угроз мировой кибербезопасности. Закон определяет основные принципы национальной политики в области кибербезопасности; уточнение обязанностей правительства, местных властей и других вовлеченных сторон; создание стратегических штабов по кибербезопасности и т.д.

Вместе с Основным законом о формировании передового информационного и телекоммуникационного общества (Закон № 144 от 2000 г.) закон 2014 года направлен на повышение экономического и социального уровня японского общества, на его устойчивое развитие. Также данный закон способствует обеспечению национальной безопасности и международной информационной безопасности.

Согласно основному закону, одним из важнейших принципов проведения политики кибербезопасности является эффективная координация действий между различными заинтересованными сторонами, включая правительство, местные органы власти и операторов СП, то есть операторов критической информационной инфраструктуры. Под последними понимаются предприятия, предоставляющие инфраструктуру, которая является основой условий жизни людей и экономической деятельности. Согласованные действия властей и частных операторов крайне важны, так как функциональные сбои и разрушения информационной инфраструктуры могут оказать огромное негативное влияние на жизнедеятельность людей. Также следует отметить и направленность закона на повышение уровня осведомленности каждого члена общества о проблемах в этой области и возможности поощрения граждан за добровольные действия в целях предотвращения ущерба, причиненного угрозами кибербезопасности. Данные меры способствуют созданию устойчивой системы, способной быстро восстанавливаться после повреждений или неисправностей.

Основной закон о кибербезопасности регулирует и зоны ответственности за реализацию политики. Эти обязательства подразделяются на несколько уровней: государство в целом; местное правительство (органы самоуправления, муниципалитеты); операторы критических информационных инфраструктур (СП-операторы); бизнес-структуры, связанные с киберпространством, и другие организации; образовательные и исследовательские организации; собственно, граждане Японии.

На всех уровнях ответственности предполагается сотрудничество и эффективная координация действий. Например, университеты должны прилагать усилия для развития людских ресурсов, специализирующихся на кибербезопасности, распространять результаты исследований в этой области и сотрудничать с правительством и местными органами власти [3]. Что касается конкретных действий правительства, то согласно статье 10, Кабинет министров должен предпринимать действия по разработке общих стандартов мер кибербезопасности для государственных административных органов; совместному использованию информационных систем государственными административными органами; мониторинга и анализа вредоносных действий в отношении информационных систем через информационно-коммуникационные сети или электронные или магнитные носители данных; реагированию на угрозы кибербезопасности совместно с соответствующими отечественными и зарубежными сторонами; по обмену информацией между административными органами, развивать курсы и тренинги по кибербезопасности [3].

Особенностью данного закона является его стратегическая составляющая, направленная на достижение основной цели политики кибербезопасности и на решение других вопросов, необходимых для всестороннего

и эффективного продвижения политики кибербезопасности. Функция координатора действий по составлению базового плана и его реализации передается вновь образованному Стратегическому штабу, органа государственной власти, который создан под эгидой Кабинета министров. В функции штаба входит разработка стратегии кибербезопасности и продвижение ее реализации, установление стандартов мер кибербезопасности для государственных административных органов и независимых административных агентств, а также проведение процедур анализа, аудита и оценки мер кибербезопасности на основе принятых стандартов. Среди других обязанностей штаба закон предусматривает: оценивание контрмер, предпринимаемых в критических случаях, затрагивающих государственные административные органы, включая проверку фактов и информации с целью определить источник проблемы. Помимо исполнения функций, перечисленных выше, ожидается, что штаб также включен в процесс изучения и исследования кибербезопасности, установления межправительственных планов, бюджета, составления рекомендаций для административных органов, координировать исполнение стратегии кибербезопасности. Принятый комплекс мер подчеркивает значимость и взаимосвязь информационной безопасности и национальной безопасности. Стратегический штаб должен функционировать в тесном сотрудничестве с Национальным советом безопасности, а также со Стратегическим штабом по продвижению передового информационного и телекоммуникационного сетевого общества.

Пост главы Стратегического штаба занимает генеральный секретарь Кабинета министров, который назначается премьер-министром. При необходимости он может давать рекомендации главам соответствующих административных органов, а также запрашивать отчеты о проделанных исправлениях. В отдельных случаях глава штаба может представлять на рассмотрение премьер-министра отчеты для принятия им окончательного решения. Членами Стратегического штаба являются: председатель Государственной комиссии общественной безопасности; министр внутренних дел и связи; министр иностранных дел; министр экономики, торговли и промышленности; министр обороны; а также и другие государственные министры. Состав штаба, включение в него ключевых фигур правительства подчеркивает значимость проблемы внутри страны, необходимость усиления кибербезопасности как условия дальнейшей цифровизации.

Важнейшим пунктом Основного закона является указание на необходимость содействия исследованиям и новым технологическим разработкам, что особенно важно для современной Японии, которая представляет собой страну, зависимую от импорта многих ресурсов, в том числе и продовольственных. Сегодня известно, что большинство высокотехнологичных готовых изделий и разнообразных деталей являются реимпортом продукции японских ТНК, произведенных за рубежом. По оценкам экономистов, се-

рьезной проблемой для Японии является низкий уровень импорта прямых инвестиций. В задачи нашего исследования не входит анализ экономической ситуации, которая, однако, является основой стабильного развития, а ее особенности в условиях современной глобализации требуют глубокого изучения. Но специфика страновой экономики на данном этапе в сочетании с демографической ситуацией, а сегодня более 26% – это пожилое население, требуют разработки новых политических и экономических подходов к формированию трудовых ресурсов и научно-технологическому развитию страны. В связи с этим необходимо развитие такой сферы экономики Японии, как НИОКР, что напрямую связано с инвестициями собственно в НИОКР, а также в образование и соответствующую инфраструктуру. Эффективность современных решений зависит от разработок и внедрения высоких технологий.

Анализируя политику Японии в сфере кибербезопасности, необходимо вспомнить и Акт о защите личной информации (закон № 57 от 2003 г., измененный в 2015 г.). Акт зафиксировал, что правильное распоряжение личной информацией и ее надежная защита способствуют повышению качества жизни в Японии. Основные обязанности по обеспечению безопасности личной информации возлагаются на правительство и местные органы власти, которые должны своевременно реагировать на появляющиеся жалобы в отношении некорректной обработки персональных данных. Законом запрещается приобретать информацию путем обмана или иными неправомерными способами, а также предоставлять сведения третьим лицам, исключая случаи, которые предусмотрены иными законами. Нарушение закона предусматривает наказание. Например, сотрудники компаний, занимающиеся обработкой личной информации, при предоставлении или краже данных с целью получения незаконной прибыли наказываются лишением свободы на срок до одного года или штрафом до 500 000 иен (около 4 657,44 долларов США) [2].

Наказания также предусмотрены Законом о запрете несанкционированного компьютерного доступа, принятым в 1999 году, последние поправки были внесены в 2013 году. Закон возлагает ответственность на такие ведомства, как Национальная комиссия по общественной безопасности, министерство внутренних дел и коммуникаций и министерство экономики, торговли и промышленности. Данные ведомства должны содействовать защите критически важных компьютеров от актов несанкционированного доступа к ним, предавать гласности статус возникновения подобных случаев и ход осуществления научных исследований и разработок в области технологий, связанных с функциями контроля доступа, не реже одного раза в год. Также они должны содействовать любым организациям, которые занимаются усилением контроля и разработкой методов обеспечения безопасности. Закон также содержит перечень наказаний, которым могут быть под-

вергнуты лица его нарушившие. Самый незначительный штраф составляет 300 000 иен (около 2785.83 долларов США), самый крупный – миллион иен (около 9 314,88 долларов США), предусмотрено и тюремное заключение от менее одного года до трех лет [1].

Уголовный кодекс Японии также регулирует незаконную деятельность в киберпространстве. Так, например, в статье 163-162, лицо, которое с целью ненадлежащего управления финансовыми средствами другого лица создает без должного разрешения электромагнитную запись, предназначенную для использования при таком ненадлежащем управлении, и закодированную в кредитной карте или других картах для оплаты расходов на товары или услуги, наказывается лишением свободы на срок не более 10 лет или штрафом не более 1 000 000 иен [4].

Планируемая цифровая трансформация общества возможна при обеспечении национальным правительством определенных мер. Это улучшение базы и условий для исследований; содействие фундаментальным исследованиям в области технологической безопасности, а также научным разработкам базовых технологий; укрепление сотрудничества между национальными исследовательскими институтами, университетами, частным сектором и другими сторонами; обмен знаниями, опытом и результатами исследований на международном уровне. Необходимость подготовки соответствующих кадров предполагает взаимодействие и координацию с университетами, технологическими колледжами, частными предприятиями и другими организациями в области обеспечения приемлемых условий занятости в сфере кибербезопасности, что позволит рабочей среде стать достаточно привлекательной для удовлетворения профессиональных способностей и ценностей. Также японские законодатели убеждены в том, что необходимо повышать уровень общественной осведомленности путем организации мероприятий с целью распространения информации и знаний в области кибербезопасности.

Реализация политики кибербезопасности осуществляется в рамках Стратегии кибербезопасности. Последняя Стратегия кибербезопасности Японии была принята в 2018 году. Таким образом, рассмотренная нормативно-правовая база и анализ отдельных факторов влияния позволяют отметить эволюцию политики Японии, стремление японского правительства решать задачи по ускорению научно-технического прогресса и обеспечению информационной безопасности. Японская «Белая книга по науке и технике» представляет оценки показателей развития и отдельных факторов влияния на научно-техническое развития страны (например, «гидзюцуреку» – достигнутый уровень научно-технического развития, «гидзюцукайхацуреку» – возможности к дальнейшему повышению этого уровня).

Условия современной глобализации усиливают обострение борьбы за доступ к природным ресурсам, разрыв экономического и технологиче-

ского развития между странами, что существенно влияет на социальную дифференциацию. Очевидна взаимозависимость цифровизации и процессов развития общества, сдвиги в «научно-технической структуре» приведут к структурным изменениям в японском обществе. Также необходимо учитывать, что интенсивное развитие информационных технологий является инструментом реализации новых вызовов, таких как международный терроризм, транснациональная преступность, миграция. Развитие цифровизации ускоряет и усиливает возможность влияния на массовое сознание. Эволюция японской политики в рассмотренной сфере свидетельствует о понимании необходимости осуществления комплекса мер по обеспечению информационной безопасности внутри страны и одновременно по расширению взаимодействия стран в области кибербезопасности в целях продвижения национальных интересов Японии на международной арене. Комплексное обеспечение национальной безопасности Японии в современных условиях развития включает информационную безопасность как основу для обеспечения разных аспектов национальной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Закон о запрете несанкционированного компьютерного доступа // https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=411AC0000000128.
2. Закон о защите личной информации // https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000057.
3. Основной закон о кибербезопасности Японии // https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104.
4. Уголовный кодекс Японии // https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=140AC0000000045.
5. *Хамуро Э.* Введение в кибербезопасность. Keio University Press, 2018.
6. *Chang F.R.* Guest Editor's Column // *The Next Wave*. 2012. № 19 (4).

N.S. KULESHOVA

*Doctor of philosophical science,
Professor of the Department of Political Science
of the East of the Institute of Asia and Africa,
Moscow State University Lomonosov,
Moscow, Russia*

A.D. SANZHIEVA

*Graduate student of Department of Political
Science of the East of the Institute of Asia and Africa,
Moscow State University Lomonosov,
Moscow, Russia*

CYBERSECURITY AS A CONDITION FOR DIGITALIZATION IN JAPAN

The research of cybersecurity is relevant to Japan, as the country does not possess sufficient technology in this area and only recently active actions have been taken in this direction. Analysis of the country's level of information security and government measures in the field of cybersecurity is significant in terms of forecasting the future course of Japan's domestic and foreign policies. The study of the country's information security is also of great scientific and practical interest. Thus, the subject of our study – the process of providing security measures to preserve the confidentiality, sustainability and availability of data in Japan – is examined from the perspective of the works of Russian and Japanese scholars using empirical material.

Key words: *cybersecurity, digitalization, Japan, political process, information security.*