исследовательские статьи

Трансформация компетенций специалистов-международников в условиях вызовов информационной безопасности России

Макеева Екатерина Дмитриевна
МГИМО МИД России
Факультет управления и политики, 2 курс
Научный руководитель: к.полит.н. Соловьева Дарья Денисовна
МГИМО МИД России, Кафедра сравнительной политологии

РЕЗЮМЕ

В данной работе рассматривается ряд актуальных компетенций специалистов международного профиля, которые формируются в процессе «цифровизации» международных отношений и отвечают на вызовы, порождаемые использованием новейших цифровых технологий в деструктивных целях. Рассмотрены понятия «цифровой безопасности» и «информационной безопасности», под которыми понимаются, соответственно, практики защиты цифровых ресурсов, устройств и систем и защита целостности, доступности, конфиденциальности и достоверности данных в любой форме. В статье обозначены прежде всего вызовы информационной безопасности России. На основании сопоставления исследований российских и зарубежных специалистов и контент-анализа основополагающих документов России в области национальной безопасности составлен перечень аспектов информационной безопасности, таких как прогнозирование угроз, управление рисками, навыки работы с нейросетями, цифровая коммуникация, анализ данных и управление данными. В соответствии с выделенными аспектами разработана авторская классификация компетенций специалистов-международников нового поколения.

КЛЮЧЕВЫЕ СЛОВА

информационная безопасность; международные отношения; цифровые компетенции; цифровизация; искусственный интеллект.

Для связи с автором makeevae255@gmail.com

research articles

Transformation of International Relations Experts' Competencies in the Context of Information Security Challenges in Russia

Ekaterina D. Makeeva
MGIMO University
School of Governance and Politics, 2nd Year
Research Supervisor PhD in Politics Darya D. Soloveva
MGIMO University, Department of Comparative Politics

ABSTRACT

This paper examines a number of relevant competencies of international relations experts, which are formed due to digitalization of international relations, responding to the challenges posed by the use of the latest digital technologies for destructive purposes. The concepts of digital security and information security are considered. The first means the practices of protecting digital resources, devices and systems, while the latter refers to protecting the integrity, availability, confidentiality and reliability of data in any form. The article identifies the challenges of information security in Russia. Based on the comparison of Russian and foreign specialists' studies and content analysis of Russia's core documents in the field of national security, a list of information security aspects is designed. It includes such aspects as threat forecasting, risk management, neural network skills, digital communication, data analysis and data management. In accordance with the highlighted aspects, the author's classification of competencies of the new generation of international specialists has been developed.

KEYWORDS

information security; international relations; digital competencies; digitalization; Artificial Intelligence.

Contact the author via makeevae255@gmail.com

ВВЕДЕНИЕ

XXI век стал эпохой цифровых технологий и цифровых угроз, оказавших колоссальное влияние на изменение ключевых характеристик специалистов в различных отраслях, отвечающих за обеспечение информационного и социокультурного суверенитета государств по всему миру. Подобные угрозы зачастую воплощаются в различных формах дезинформации, которая циркулирует в пространстве СМИ и глобальной сети Интернет. Критичность данной проблемы обостряется детерминированием этих угроз со стороны различных заинтересованных субъектов — как праворадикальных и террористических структур и преступных синдикатов, так и некоторых политических фигур, режимов и даже правительств. Это явление ставит специалистов-международников перед новым вызовом в сфере международной безопасности, на который необходимо ответить с учетом эволюции информационного пространства международного сообщества и его площадок.

Для того, чтобы определить новые приоритеты в подготовке экспертов международного профиля, особенно в сфере международной безопасности, необходимо определить, какими будут наиболее востребованные в современных условиях компетенции подобных специалистов, чтобы они были способны эффективно справляться с актуальными вызовами в информационной среде. Для этого в рамках данной работы предлагается рассмотреть современные угрозы в международной цифровой среде, охарактеризовать актуальные потребности политической среды в компетентных специалистах нового поколения, которые будут способны успешно реагировать на эти угрозы, а также синтезировать полученные данные с целью установления необходимых компетенций экспертов международного профиля в сфере информационной безопасности.

Таким образом, целью данной статьи является определение основных компетенций специалистов-международников в сфере информационной безопасности и цифровых технологий. Актуальность работы заключается в рассмотрении новейших навыков специалистов международного профиля при работе с современными информационными технологиями, включая искусственный интеллект и нейросети, которые могут быть успешно применены для обеспечения информационной безопасности России сегодня и завтра. В качестве методов исследования были использованы контент-анализ, сравнительный метод.

СОВРЕМЕННЫЕ УГРОЗЫ В ИНФОРМАЦИОННОЙ СРЕДЕ

На сегодняшний день информационное пространство международных отношений является площадкой для ведения целенаправленных информационных и когнитивных войн, оказывающих внушительное влияние на информационно-психологическую безопасность общества[1]. Трансграничные социальные сети и Интернет-медиа выступают ключевой площадкой для распространения фейковых новостей, продуктов генеративных нейросетей, которые используются для повышения эффективности внушаемости населения и переформатирования сознания общества, и других цифровых

[1] Федоров А.В. Информационная безопасность: политическая теория и дипломатическая практика: монография / А.В. Федоров, Е.С. Зиновьева. – М.: МГИМО-Университет, 2017. – С. 120.

инструментов и механизмов, использующихся для формирования ложных представлений в обществе, навязывания чуждых ценностей, дестабилизации общественного порядка и т. д.

Деструктивное воздействие со стороны вредоносного кибер-сообщества оказывается на цифровую безопасность российского информационного пространства как в информационно-технической сфере, так и в информационно-психологической. Технологический вред наносится кибер-террористами, отдельными государствами, криминальными группами преимущественно по цифровой защите и объектам собственности России в Интернете, под угрозой психологического характера находится российское общество и его сознание, управление над восприятием которого становится целью субъектов кибератак.

В данном контексте уместно разграничить понятия «информационной безопасности» и «цифровой безопасности». Информационная безопасность преимущественно представляет собой сбалансированную защиту целостности, доступности, конфиденциальности и достоверности данных в любой форме. Цифровая безопасность включает в себя, в первую очередь, практики защиты цифровых ресурсов, устройств и систем, и только потом защиту данных. В рамках данной работы внимание будет уделено преимущественно вопросу компетенций информационной безопасности, во вторую очередь — ресурсам и инструментам цифровой безопасности, которыми могут воспользоваться специалисты-международники.

Массированное воздействие на информационно-психологическую сферу жизни общества в Интернете осуществляется посредством конструирования особого информационного фона в социальных сетях, информационных вбросов в крупные медиа, подстраивания определенной повестки и ее единой оценочной позиции в СМИ и т.д. Это влияет на повышение уровня тревожности общественного состояния, снижает способность социума воспринимать новости критически. Для 70% интернет-пользователей мессенджеры, социальные сети и Telegram-каналы являются на сегодняшний день единственным источником информации[1]. Во время выборов президента России в 2024 году Роскомнадзор удалил больше 485 Telegram-каналов и более 12 800 материалов, содержащих призывы к экстремизму и недостоверную информацию о спецоперации, выборах и пр[2]. Эти цифры указывают на необходимость привлечения колоссального внимания к проблематике безопасности российской информационной среды, а также на значительное количество информационных «вбросов» и атак, которым подвергается наше государство извне, что впоследствии провоцирует необходимый разбор этих информационных поводов внутри нашего медийного и новостного сообщества, рефлексию над ними и отражения общественного восприятия этого внешнего давления.

Нередки также случаи информационных манипуляций, например, намеренного удаления администрациями социальных сетей и платформ

[1] Эксперты обсудили, как обеспечить информационную безопасность // Российская газета: интернет-портал. – 18.11.2020. – URL.: https://rg.ru/2020/11/18/eksperty-soiuznogo-gosudarstva-obsudili-kak-obespechit-informacionnuiu-bezopasnost.html (дата обращения: 03.05.2024).

[2] РКН удалил почти 500 каналов в Telegram с фейками о терактах во время выборов // Ведомости: сетевое издание. – 21.03.2024. – URL: https://www.vedomosti.ru/society/news/2024/03/21/1027025-rkn-udalil (дата обращения: 03.05.2024).

контента из Интернета, связанного с объектами и событиями, относящимися к исторической памяти. Так, 9 мая 2022 года фотография Е.А. Халдея «Знамя Победы над Рейхстагом» была удалена администрацией Facebook[1] из социальной сети[2], позднее представители сети прокомментировали этот инцидент, назвав его технической ошибкой.

Отдельно стоит упомянуть про СМИ с большой аудиторией в своем регионе и международных СМИ, осознанно занимающихся дезинформацией. В данном случае СМИ, газеты и телеканалы нередко абсолютно сознательно и открыто обманывают свою аудиторию, выдавая откровенные «фейки» за достоверную информацию и реальные события. Так, например, уже делала Daily Mirror, когда заявила, что российские военные, а не ВСУ, якобы обстреляли Донецк[3]; те же заявления прозвучали и в телеэфире немецкой Das Erste[4].

Международная правозащитная организация Amnesty International, опубликовавшая в августе 2022 года доклад[5] о нарушениях гуманитарного и военного права со стороны ВСУ, в очередной раз обстрелявших мирное население Донецка, позже столкнулась с давлением со стороны политического руководства Украины и ее геополитических союзников и была вынуждена принести извинения «за гнев и страдания украинцев». Данный пример иллюстрирует проявление практики искусственного конструирования конкретного информационного фона через СМИ. Подобный агрессивный информационный фон принудительно насаждается обществу через общедоступные социальные сети и прочие Интернет-платформы, на которых пользователи могут столкнуться с проявлениями дезинформации. В таких условиях особенно востребован оказывается навык распознавания дезинформации в общем потоке новостей.

Для противодействия волне дезинформации со стороны недружественных стран, МИД России на своем официальном сайте создало специальный раздел «Опровержения»[6], где публикуются разоблачения на фейковые новости, которые в качестве «информационных бомб» периодически вбрасываются в информационное поле России. Этот кейс доказывает, что на сегодняшний день необходимость разоблачать клевету вызвана сложившейся беспрецедентной по историческим меркам ситуацией, в которой ложь и обман становятся универсальными инструментами формирования общественного сознания и продвижения в международном пространстве любых искусственно скорректированных идей, в том числе самых радикальных и опасных.

В результате перечисленные угрозы (фейки, манипуляции, произвольная дезинформация) создают запрос не только на аналитические

[1] Принадлежит Meta Platforms Inc. (входит в реестр экстремистских организаций, деятельность на территории России запрещена).
[2] Facebook объяснил, почему удалял фотографию водружения Знамени Победы на Рейхстаге // ТАСС: информационное агентство. – 09.05.2020. – URL: https://tass.ru/obschestvo/8437501 (дата обращения: 03.05.2024).
[3] The Daily Mirror выдала обстрелы ВСУ Донецка за «российскую бомбежку» // Телеканал РЕН ТВ: интернет-сайт. – 05.07.2022. – URL: https://ren.tv/news/v-mire/996469-daily-mirror-vydalo-obstrely-vsu-donetska-za-rossiiskuiu-bombezhku (дата обращения: 03.05.2024).
[4] На немецком телевидении в обстрелах Донецка обвинили российских военных. // Первый канал: интернет-сайт. – 14.06.2022. – URL: https://www.1tv.ru/news/2022-06-14/431166-na_nemetskom_televidenii_v_obstrelah_donetska_obvinili_rossiyskih_voennyh (дата обращения: 03.05.2024).
[5] Amnesty извинилась за «страдания и гнев» украинцев из-за своего доклада // РБК: сетевое издание. – 07.08.2022. – URL: https://www.rbc.ru/politics/07/08/2022/62efaa479a7947609e5cff3f (дата обращения: 03.05.2024).
[6] Опровержения // Министерство иностранных дел Российской Федерации: официальный сайт. – URL: https://www.mid.ru/ru/press_service/publikacii-i-oproverzenia/oproverzenia1/ (дата обращения: 03.05.2024).

навыки работы с информацией, чья достоверность ставится под сомнение, но и навыки прогнозирования рисков и управления рисками, которые могут быть спровоцированы решениями, принимаемыми на основе дезинформации.

Компетенции специалистов-международников, профессиональная среда которых напрямую затрагивает аспекты информационной безопасности государства, международного противостояния в глобальной информационной сфере, оказываются под непосредственным влиянием подобных тенденций, которые создают запрос на новые навыки углубленного и всестороннего изучения этих явлений и сопротивления их негативным факторам. Для определения направлений трансформации таких компетенций необходимо охарактеризовать, какие новые вызовы стоят перед цифровой безопасностью России сегодня и какие существуют запросы на актуальные компетенции экспертов-международников в условиях «цифровизации международных отношений».

ОБЗОР НАУЧНОЙ ЛИТЕРАТУРЫ

Последние современные исследования в области компетентностных характеристик специалистов международного профиля в основном рассматривают факторы-следствия трансформации международных отношений в контексте цифровизации глобального пространства геополитики и проникновения цифровых технологий в структуры политической информационной циркуляции, становления многополярности в контексте изменения расстановки сил в международном поле. Эти тенденции выступают новыми корректирующими факторами компетентностных характеристик экспертов-международников, которые формируют у граждан и профессионального сообщества запрос на новое поколение специалистов международного профиля и, соответственно, новый «портфель» их компетентностных характеристик — более гибких с точки зрения коммуникации, более глубоких с точки зрения аналитического аппарата.

Выше уже было рассмотрено, как информационные технологии нового поколения успешно используются не только во благо международному сообществу, но и против его благополучия. Проникновение дезинформации в общемировые информационные структуры, охватывающие все пространство глобальных медиа-коммуникаций, в которых беспрерывно происходит обмен информацией, приводит к усилению её резистентности и практически бессрочному хранению в архивах памяти глобальной сети. Это, в свою очередь, ставит экспертное сообщество перед новым вызовом, требует структуризации практического исследования и применения инструментария обеспечения информационной безопасности государства — в том числе формирования конкретного набора компетенций, которые в ближайшем будущем могут стать стандартными для специалистов-международников нового поколения.

В качестве источников, описывающих методы и инструменты формирования новых компетенций специалиста-международника, в этой статье будут рассматриваться преимущественно данные исследований за последние пять лет, поскольку в этот период информационные технологии нового поколения стали особенно распространены и доступны, а после 2022 года нейросети и их массовое распространение перевернули

многие современные подходы к работе с информацией.

В области коммуникативных компетенций в сфере информационного и медиапространства исследователи обращают внимание на формирование новых навыков, ориентированных на повышение эффективности взаимодействия субъектов информационного поля с аудиторией на актуальных цифровых площадках, способностей толкования медиа-дискурса, информационных символов в нем, поверхностной коррекции и модуляции позиционной ориентации аудитории. Н.М. Романенко, профессор Кафедры педагогической культуры и управления в образовании МГИМО МИД России, а также ее коллеги М.В. Натуркач из Белорусского государственного университета и Л.П. Илларионова из Государственного университета просвещения, выделяют медиадискурсивную компетенцию для студентов-международников[1], под которой они понимают навыки «медиатизированного диалога» и критического мышления при работе с информационным фоном. По мнению исследователей, медиатекст и его модуляции составляют когнитивные, аналитические и идеологические интерпретации реальности и ее отражений в информационной среде, поэтому должны стать одной из ключевых компетенций современных специалистов международного профиля.

Исследователь МГИМО МИД России А.В. Калита выделяет среди основных групп профессиональных навыков специалистов-международников группы компетенций «цифрового строительства» и «мягких навыков»[2]. Под «мягкими навыками» современности теперь понимаются уже не только коммуникация, креативность, развитый аналитический аппарат, но «социальный, творческий и критический интеллект». В блоке компетенций «цифрового строительства» автор выделяет навыки анализа данных, управления данными и цифровой безопасности.

Д.философ.н. А.П. Кочетков и его коллега по Кафедре российской политики К.В. Маслов в рамках подхода к национальной безопасности России с точки зрения цифрового суверенитета обращают внимание на необходимость минимизации рисков в поле государственной политики в условиях цифровизации[3], а также указывают на актуальный феномен «цифровых капсул», которые формируют определенную точку зрения в цифровом пространстве с учетом позиции отдельных групп интересов.

К.ф-м.н. А.В. Федоров определяет психологическую борьбу как одно из направлений информационного противоборства, как и международный информационный терроризм, под которым понимается децентрализованная сеть террористов, наносящих точечные удары по цифровой инфраструктуре других стран[4]. Автор подчеркивает, что одним из ключевых инструментов психологического противоборства является дезинформация как целенаправленные, информационно-психологические

[1] Натуркач М.В. Формирование медиадискурсивной компетенции студентов международного профиля: результаты практики / М. В. Натуркач, Н. М. Романенко, Л. П. Илларионова // Московский педагогический журнал. – 2023. – №3. – С. 84-104.

[2] Калита А.В. Формирование новых профессиональных компетенций студентов-международников / А. В. Калита // Проблемы современного педагогического образования. – 2022. – №76(3). – С. 114-116.

[3] Кочетков А.П. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе / А. П. Кочетков, К.В. Маслов // Вестник Московского Университета. Политические науки. – 2022. – №2. – С. 31-45.

[4] Федоров А.В. Информационная безопасность: политическая теория и дипломатическая практика: монография / А.В. Федоров, Е.С. Зиновьева. – М.: МГИМО-Университет, 2017. – С. 120.

манипулятивные воздействия, эффективной защитой от которых может выступать только интеллектуализация на уровне отдельных личностей и высокий позитивный самообраз «мы» в массовом сознании гражданского общества[1]. Автор также указывает, что одним из ключевых инструментов ИКТ, использующихся специалистами-международниками, является так называемая «цифровая дипломатия» — широкое использование в дипломатической практике ИКТ, медиа, социальных сетей, блогов и прочих медиаплощадок в глобальной сети для взаимодействия с зарубежными и региональными пользователями интернета, которое в качестве инновационного метода в практике международных отношений впервые представили госструктуры США[2]. Составными частями этого феномена выступают понятия дипломатии социальных сетей (публичной дипломатии в социальных сетях, например, официальных аккаунтов МИД), Web 2.0 дипломатии (практики влияния на зарубежную аудиторию посредством медиа-платформ в Интернете) и другие.

Д.и.н. А.И. Смирнов рассматривает четыре ступени развития информационных технологий, которые повлияли на трансформацию профессиональных компетенций специалистов международного профиля[3], из которых последние две, Web 3.0 («semantic web», работа с метаданными (знаниями)) и Web 4.0 (когнитивный интернет, агенты которого способны к самообучению) охватывают самый близкий к современности период времени после 2010 года. Соответственно, на сегодняшний день мы рассматриваем преимущественно цифровую дипломатию Web 3.0 и Web 4.0. Преимущество искусственных когнитивных систем нашего времени в том, что они способны повторить сложные поведенческие функции нервной системы и даже мыслительные процессы человека.

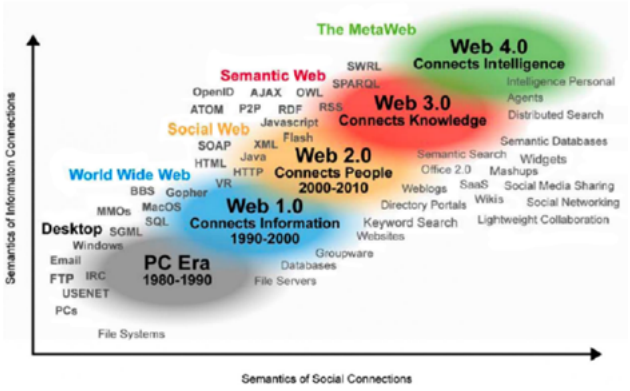

Рис. 1. Ступени развития интернет-технологий. Источник: Evolution of Web[4].

Из практических методов цифровой дипломатии современности автор выделяет навык работы с когнитивным компьютингом (компьютинг со способностью к мышлению, которое по своему уровню опережает машинное обучение, но стоит перед искусственным интеллектом)[5], навык распознавания манипуляций в информационном пространстве на стадии «постправды» по эффекту SEME (эффект манипулирования поисковой системой)[6], навык распознавания микротаргетирования (точной настройки социальных медиа для

[1] Там же, с. 131.
[2] Там же, с. 276.
[3] Смирнов А.И. Современные информационные технологии в международных отношения. – М: МГИМО-Университет, 2017. – С. 36.
[4] Aarnio H. International Digital Marketing Strategy as a Growth Opportunity. Case: Finnish startup / Heli Aarnio // Master's Thesis Report. – Haaga-Helia University of Applied Sciences, 2017. – С. 19. – URL: https://core.ac.uk/download/pdf/161417236.pdf (дата обращения: 03.05.2024).
[5] Смирнов А.И. Современные информационные технологии в международных отношения. – М: МГИМО-Университет, 2017. – С. 55.
[6] Там же, с. 118.

работы с целевой аудиторией, предполагающей подробное знание любого пользователя соцсети)[1], метод прогнозирования фазово-факторной модели международного конфликта (в котором конфликт изображается как динамический процесс с цепью нескольких фаз)[2], навык работы с моделью информационного поискового запроса (МИПЗ для автоматического определения цитируемости факторов в документах)[3], когнитивная система анализа[4].

О наборе технологических инструментов дипломатической службы, уже использующихся сотрудниками МИД Великобритании («Форин-офиса»), еще в 2012 году писала Лариса Пермякова, к.полит.н., сотрудник Дипломатической академии России[5]. «Инструментарий цифровой дипломатии» (Digital diplomacy toolbox) включает в себя инструменты «Твипломатии» (Twiplomacy), краудсорсинга (подхода к решению проблемы совместными усилиями), экспертной помощи и оказания консультации дипломатам, а также предлагает электронные решения для сотрудников ведомства. «Инструментарий цифровой дипломатии» (Digital diplomacy toolbox) существует до сих пор и иллюстрирует актуальный пример применения современных технологий с целью повышения эффективности работы специалистов-международников.

Доктор философии Американского международного университета Бангладеш Продхан Махбуб Ибна Серадж в своем исследовании, посвященном изучению влияния технологий искусственного интеллекта на повышение уровня критического мышления у студентов[6], подчеркивает, что взаимодействие специалистов с ИИ при выполнении задач, требующих навыков анализа больших массивов данных или моделирования конкретных ситуаций, значительно повышает качество выполняемой работы. Исследователь отмечает, что сегодня ИИ еще не может справляться с подобной работой настолько же качественно, как человек, являющийся экспертом в своей области, но взаимодействие человека и технологий подобного уровня способно разительно ускорить темпы работы специалиста-международника при выполнении его профессиональных задач. Автор выделяет качественные и количественные методы работы при взаимодействии с искусственным интеллектом. Качественные методы представлены преимущественно осуществлением исследовательских процедур, а количественные — систематическим анализом случайных кейсов, выборок или больших массивов данных. При проведении практического эксперимента со своими студентами исследователь выявил, что использование ИИ значительно повысило скорость аналитических навыков испытуемых при работе над профильными задачами.

Дамиан Тусет Варела, исследователь из Хаэнского Университета Испании и начальник отдела Министра иностранных дел Эквадора, описывая «кризисные сценарии»

[1] Там же, с. 120.
[2] Там же, с. 155.
[3] Там же, с. 157.
[4] Там же, с. 159-160.
[5] Пермякова Л. Цифровая дипломатия: направления работы, риски и инструменты // Российский совет по международным делам (РСМД): интернет-сайт. – 27.09.2012. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovaya-diplomatiya-napravleniya-raboty-riski-i-instrumen/ (дата обращения: 03.05.2024).
[6] Muthmainnah P.M.I.S. Playing with AI to Investigate Human-Computer Interaction Technology and Improving Critical Thinking Skills to Pursue 21st Century Age / Muthmainnah Prodhan Mahbub Ibna Seraj, Ibrahim Oteir // Education Research International. – 2022. – URL: https://doi.org/10.1155/2022/6468995 (дата обращения: 03.05.2024).

пересечения дипломатии и искусственного интеллекта в современном пространстве международных отношений, выделяет три проблемы[1], в которых применение ИИ может сыграть ключевую роль: необходимость принять решение в условиях ограниченной или потенциально недостоверной информации; осуществление управления в условиях, сопряженных с большими рисками; работа с большими массивами данных. Исследователь выделяет три типа взаимодействия ИИ и дипломатии: «когда ИИ служит дипломатии», «когда дипломатия влияет на управление ИИ» и «когда ИИ используется в целях дипломатии». В первом случае искусственный интеллект создает для экспертов инновационные решения, которые они оценивают, редактируют и дополняют. Во втором случае на специалистов-международников возлагается задача оценки возможностей и рисков, связанных с технологиями искусственного интеллекта, а также коррекция характера осуществления сотрудничества и инициатив, исходящих от лиц и организаций, взаимодействующих с ИИ. В третьем случае предполагается, что искусственный интеллект может помочь экспертам-международникам улучшить их профессиональные навыки, выполняя консультирующую и обучающую функцию при принятии решения в условиях кризисной ситуации или выполнения симуляционного упражнения. Автор подчеркивает, что искусственный интеллект не может полноценно выполнять функции реальных специалистов международного профиля, он способен только улучшить их навыки, поэтому работа ИИ и экспертов-международников должна происходить исключительно в кооперации. Таким образом, может быть значительно улучшен блок навыков экспертов, который отвечает за критическое мышление и реагирование в кризисных ситуациях.

Исследователи из Саутгемптонского университета Великобритании Эрин Ригли, Джошуа Крук и Сарвапали Р. Рамчурн, а также их коллега из Королевского Колледжа Лондона Кейтлин Бентли в своем совместном исследовании, посвященном оценке международной политики в области навыков искусственного интеллекта[2], рассмотрели существующие запросы профессионального сообщества в 17 странах мира на внедрение навыков работы с ИИ в компетентностную характеристику специалиста в области мировой политики, государственной политики и международных отношений. В соответствии с результатами исследования, в большинстве рассмотренных в их работе стран существует определенный уровень общественных опасений ввиду негативного влияния ИИ на динамику формирования профессиональных навыков и распределения мест на рынке труда. При этом в странах, лидирующих по уровню внедрения ИИ в профессиональные политические структуры (США, Сингапур, Великобритания, Канада, Китай, и др.), требования к умениям специалистов международного профиля работать с информационными технологиями с недавнего времени закреплены в государственных стандартах и национальных стратегических документах. Лидеры использования ИИ в политических структурах (США, Сингапур) придерживаются подхода массового предоставления

[1] Damián T.V. Diplomacy in the Age of AI: Challenges and Opportunities / Damián Tuset Varela // Journal of Artificial Intelligence General science. – 2024. – №1. – P. 98-109.
[2] Rigley E. Evaluating international AI skills policy: A systematic review of AI skills policy in seven countries / Eryn Rigley, Caitlin Bentley, Joshua Krook, Sarvapali D. Ramchurn // Global policy. – 2024. – №1. – P. 204-217.

дополнительного образования по обучению навыкам профессиональной работы с искусственным интеллектом, отстающие от них (Китай, Канада) — меритократического или инклюзивного принципа (для отдельных социальных групп или слоев общества). Подчеркивая острую нехватку компетентных специалистов в области международной политики, которые были бы способны использовать в своей работе возможности ИИ и других технологий, исследователи выделяют следующие навыки, отвечающие за эффективную работу с информацией: навыки STEM (комплекс навыков универсальной технической образовательной политики), прогностическое моделирование, машинное обучение, разработка алгоритмов, цифровая грамотность, компьютерное мышление (метод постановки и решения проблемной ситуации при участии компьютерных технологий).

На основе рассмотренных выше источников можно сформировать спектр из нескольких аспектов информационной безопасности: аналитический аспект работы с информацией (оценивание достоверности информации, навыки поиска данных), коммуникативный аспект (получение и передача данных), инновационный аспект (производство новых данных), прогностический аспект (предиктивная аналитика) и управленческий аспект (предупреждение рисков, управление информационными ресурсами). При соотнесении этих аспектов с актуальными запросами на совершенствование навыков специалистов международного профиля можно определить конкретные компетенции международников «нового поколения», отвечающие текущим тенденциям.

НОВЫЕ КОМПЕТЕНЦИИ СПЕЦИАЛИСТОВ-МЕЖДУНАРОДНИКОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

За последние несколько лет в экспертном сообществе были выработаны конкретные запросы на обновленные навыки специалистов-международников в соответствии с общемировыми тенденциями, которые задают развитие цифровых технологий. На основании этих запросов и влияния технологических драйверов происходит трансформация компетенций экспертов международного профиля, в том числе в области информационной безопасности.

В апреле 2024 года на международной выставке-форуме «Россия» прошла панельная дискуссия «Дипломат в цифровую эпоху». Представителями МИД России, МГИМО МИД России, МГТУ им. Баумана, Российского общества «Знание» обсуждалась трансформация универсальных компетенций специалиста-международника в условиях «цифровизации международных отношений» и проникновения современных технологий в политический ландшафт общества[1]. В ходе дискуссии о важности использования искусственного интеллекта «международниками» в интересах граждан и экспертного сообщества таких сфер, как государственное управление и международные отношения, заявил ректор МГИМО МИД России, академик Российской академии наук А.В. Торкунов.

[1] Международники нового поколения: цифровую дипломатию будущего обсудили на выставке // Национальный центр «Россия»: интернет-сайт. – 05.04.2024. – URL: https://russia.ru/news/mezdunarodniki-novogo-pokoleniia-cifrovuiu-diplomatiiu-budushhego-obsudili-na-vystavke (дата обращения: 03.05.2024).

Вовлеченность той или иной страны и ее профессиональных кадров в цифровизацию международных отношений показательно отображают статистические показатели общемировых индексов. По данным Индекса глобальной дипломатии (Global Diplomacy Index)[1], «топ-5» стран рейтинга составляют Китай, США, Турция, Япония и Франция. Россия находится на шестом месте. Индекс учитывает классические количественные показатели, отражающие показатель «нетворкинга», т.е. сетевого взаимодействия стран: число имеющихся у них дипломатических связей с другими государствами и находящихся там представительств, консульств, посольств, постоянных миссий и т.д. (см. рис. 2).

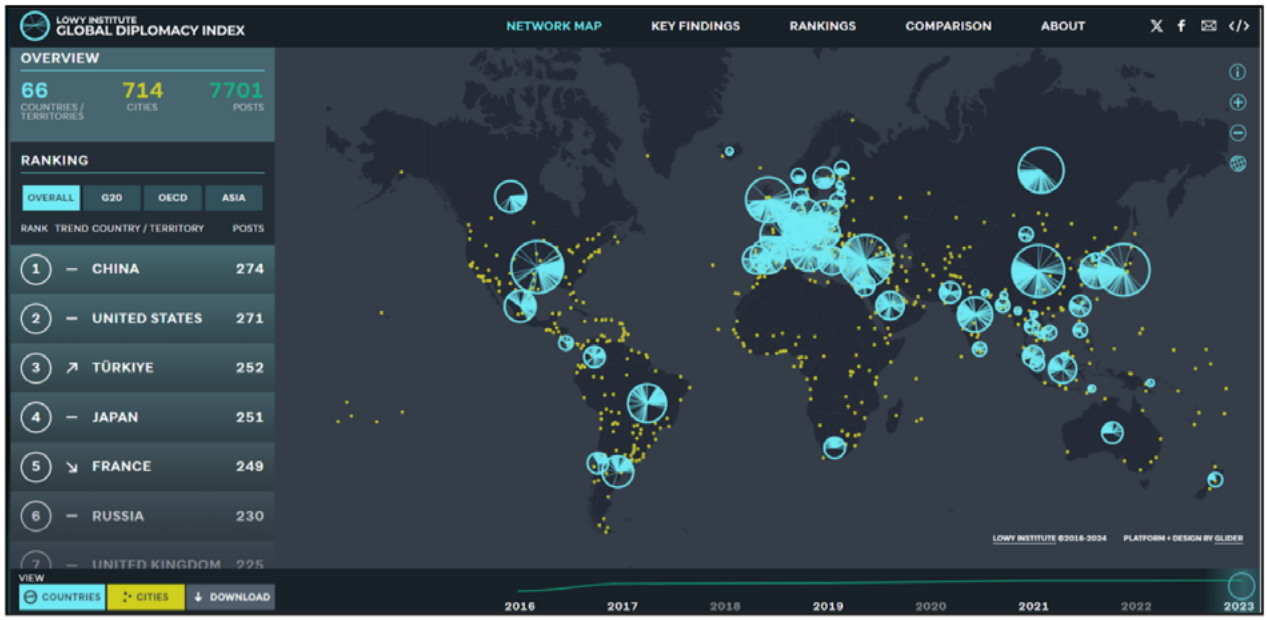

Рис. 2. Global Diplomacy Index. Network map.

Другим примечательным показателем является Индекс цифровой дипломатии (Digital Diplomacy Index)[2], который учитывает только показатели «цифрового нетворкинга» стран: охват дипломатической сети, вес дипслужбы государства в международном пространстве, грамотность ее риторики, эффективность передачи информации, узнаваемость страны по всему миру, владение профессиональным форматом деятельности, важность дипломатической деятельности страны для остального мира, языковое разнообразие, которым владеет дипслужба. По данным индекса на 2023 год в «топ-5» входят США, Россия, Индия, Индонезия и Франция, при этом показатель России вырос на единицу за предыдущий год (см. рис. 3).

[1] Global Diplomacy Index. Rankings. – URL: https://globaldiplomacyindex.lowyinstitute.org/country_ranking (дата обращения: 03.05.2024).
[2] Digital Diplomacy Index. Rankings. – URL: https://digital-diplomacy-index.com/index/ (дата обращения: 03.05.2024).

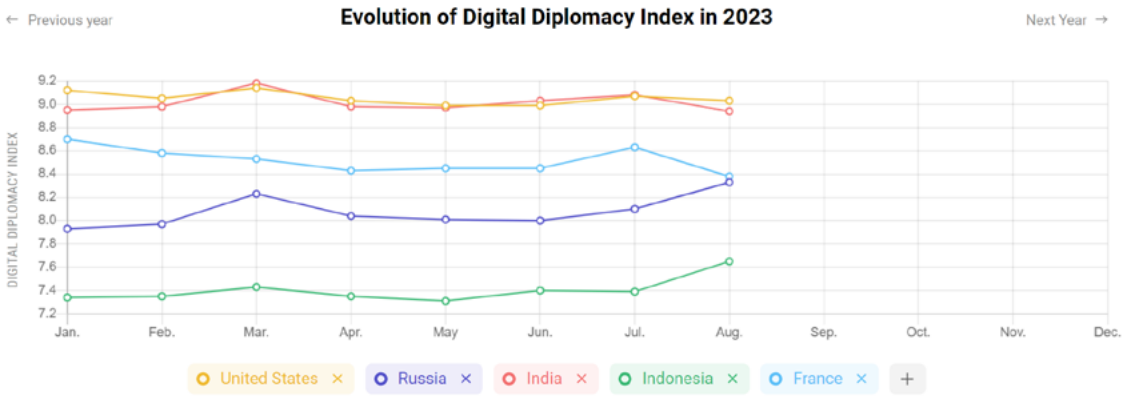

Рис. 3. Evolution of Digital Diplomacy Index in 2023.

Актуальные компетенции цифрового профиля в сфере безопасности необходимы и востребованы по многим причинам, одна из которых — важность охраны и защиты цифрового суверенитета России, как отметила к.полит.н. Н.П. Ромашкина[1]. Несмотря на то, что на сегодняшний день не существует единой дефиниции понятия «цифрового суверенитета», которое было бы способно всеобъемлюще передать его смысловое и функциональное содержание, одна из характеристик, присутствующая преимущественно во всех определениях «цифрового суверенитета» — состояние защищенности от внешних угроз в пространстве ИКТ. Для его обеспечения также необходимы навыки специалистов международного профиля нового поколения.

Подробно обо всех угрозах информационной безопасности России, включая кибероружие, фейковые новости, информационные «вбросы», манипуляции, и прочие инструменты информационной войны, цифровым плацдармом которой выступает на текущий момент Украина, рассказала на онлайн-платформе Российского общества «Знание» д.полит.н., профессор Кафедры мировых политических процессов МГИМО МИД России Е.С. Зиновьева[2]. Спикер подчеркнула важность корректного использования цифрового потенциала страны для того, чтобы эффективно отражать атаки в информационном пространстве России и не допускать пагубного влияния враждебных нашему обществу идей и пропаганды (в том числе терроризма и экстремизма) в пространстве глобальной сети.

Стратегические принципы обеспечения цифрового суверенитета России изложены в ряде политико-правовых документов, отражающих основные направления работы государства с проблемой борьбы с киберпреступностью. Такими документами являются Доктрина информационной безопасности России, Стратегия национальной безопасности РФ от 2 июля 2021 г., Концепция внешней политики РФ от 31 марта 2023 г., Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон

[1] Ромашкина Н. Информационный суверенитет или почему России нужна стратегия информационной безопасности // Российский совет по международным делам (РСМД): интернет-сайт. – 06.08.2019. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ (дата обращения: 03.05.2024).

[2] Информационная безопасность Российской Федерации (лекция) / Зиновьева Е.С. // Российское Общество «Знание»: интернет-сайт. – 13.05.2022. – URL.: https://znanierussia.ru/library/video/informacionnaya-bezopasnost-rossijskoj-federacii-979 (дата обращения: 03.05.2024).

«О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон «О персональных данных», Федеральный закон «О критической информационной инфраструктуре».

Согласно Доктрине[1], основными направлениями обеспечения информационной безопасности России в информационно-психологическом аспекте являются следующие пункты:

Номер	Пункт
№2	Развитие системы прогнозирования, выявления и предупреждения угроз ИБ России, определения их источников, оперативной ликвидации последствий реализации таких угроз;
№4	Создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
№10	Развитие сил и средств информационного противоборства;
№11	Противодействие использованию информационной инфраструктуры РФ экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество;
№12	Совершенствование средств и методов обеспечения ИБ на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;
№14	Укрепление сотрудничества РФ с иностранными партнёрами в области обеспечения ИБ, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий;
№15	Доведение до российской и международной общественности достоверной информации о внутренней и внешней политике РФ.

Тбл. 1. Главные направления обеспечения информационной безопасности России в информационно-психологическом аспекте. Источник: составлено автором.

Также стоит отдельно обратить внимание на специализированные документы, предписывающие оказывать сопротивление целенаправлен-

[1] Указ Президента Российской Федерации от 05.12.2016 г. № 646. // Президент России: официальный сайт. – URL.: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 03.05.2024).

ным манипуляциям в информационной среде всеми возможными силами государств и их представителей. Так, в «Основах государственной политики РФ в области международной информационной безопасности»[1] была обозначена новая группа угроз информационной безопасности России — «использование ИКТ для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию».

На современном этапе, опираясь на данные исследований и программных документов, рассмотренных выше, возможно составить перечень актуальных компетенций специалистов-международников в сфере информационной безопасности, который выходит за рамки одних только навыков «мягкой силы» ввиду своего слияния с инструментами и методами современных информационных технологий. В качестве основных направлений, в которых выделены конкретные профессиональные навыки, используются аспекты информационно-психологической безопасности (как состояния защищенности общества от факторов информационного воздействия на психологию и сознание этого общества), сформированные и описанные в Доктрине информационной безопасности России. Эти аспекты напрямую пересекаются с теми аспектам информационной безопасности, которые были выделены ранее на этапе обзора научной литературы. На их пересечении можно конкретно определить, какие актуальные компетенции отвечают определённым тенденциям в данной области.

Аспект информационной безопасности	Компетенция
Прогнозирование угроз	• Ситуационное моделирование; • Прогностическое моделирование; • Моделирование кейсов; • Прогнозирование фазово-факторной модели международного конфликта; • Моделирование международных отношений.
Управление рисками	• Компьютерное мышление; • Предупреждение кризисов.
Навыки работы с ИИ и нейросетями	• Разработка инновационных практик с помощью медиаконтента; • Когнитивная аналитика (на основе когнитивного компьютинга).

[1] Указ Президента Российской Федерации от 12.04.2021 г. № 213. // Президент России: официальный сайт. – URL: http://www.kremlin.ru/acts/bank/46614 (дата обращения: 03.05.2024).

Аспект информационной безопасности	Компетенция
Цифровая коммуникация	• Медиадискурсивная компетенция (формирование медиатекста); • Метафорическое моделирование дискурса; • Когнитивное моделирование.
Анализ данных	• Критическое мышление; • Навык распознавания эффекта SEME; • Навык распознавания микротаргетирования; • Навык работы с моделью информационного поискового запроса (МИПЗ); • Когнитивная система анализа; • Цифровая грамотность и цифровой этикет.
Управление данными	• Навыки STEM.

Тбл. 2. Перечень актуальных компетенций специалистов-международников в сфере информационной безопасности. Источник: составлено автором.

Перечисленные выше компетенции позволяют осуществлять непрерывную работу с информацией с использованием актуальных технологий, начиная от этапа проверки данных на достоверность и первичной аналитики вплоть до составления прогнозов и рекомендаций для коррекции конкретных ситуаций, подверженных влиянию потока данных в информационной среде.

Привлекая к выполнению своих профессиональных задач инструменты искусственного интеллекта, нейросетей и цифровых платформ, эксперты международного профиля смогут еще успешнее справляться с прогнозированием угроз и кризисных ситуаций, принимать решения в условиях ограниченной или противоречивой информации, анализировать большие массивы данных, содержащие в себе недостоверную информацию, взаимодействовать с аудиторией в информационной среде с целью коррекции общественного восприятия и рефлексии над новостным фоном в глобальной сети. В условиях непрерывного развития и стандартизации данного перечня профессиональных компетенций, специалисты-международники будут способны гораздо эффективнее противодействовать угрозам в общемировом информационном пространстве, представляющим опасность для безопасности и благополучия общества.

ЗАКЛЮЧЕНИЕ

Таким образом, трансформация профессиональных компетенций специалистов международного профиля в условиях актуальных вызовов информационной безопасности происходит в условиях сформировав-

шихся экспертных и общественных запросов на новое поколение специалистов-международников, владеющих навыками работы с современными технологиями, способных справляться с различными угрозами международной и национальной безопасности в информационной среде в разы эффективнее, чем раньше. Подобные специалисты, обладающие актуальным портфелем профессиональных навыков, смогут не только успешно анализировать данные, но и управлять ими, модулируя их в целях позитивной коррекции информационного фона, поступающего через цифровые площадки общемировой коммуникации, а также провоцировать ускорение инновационных разработок и прогностического моделирования для автоматизирования подбора наиболее благоприятных сценариев в различных ситуациях.

СПИСОК ЛИТЕРАТУРЫ:

1. Информационная безопасность Российской Федерации (лекция) / Зиновьева Е.С. // Российское Общество «Знание»: интернет-сайт. — 13.05.2022. — URL.: https://znanierussia.ru/library/video/informacionnaya-bezopasnost-rossijskoj-federacii-979 (дата обращения: 03.05.2024).
2. Калита А.В. Формирование новых профессиональных компетенций студентов-международников / А.В. Калита // Проблемы современного педагогического образования. — 2022. — №76(3). — С. 114-116.
3. Кочетков А.П. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе / А. П. Кочетков, К.В. Маслов // Вестник Московского Университета. Политические науки. — 2022. — №2. — С. 31-45.
4. Натуркач М.В. Формирование медиадискурсивной компетенции студентов международного профиля: результаты практики / М.В. Натуркач, Н.М. Романенко, Л.П. Илларионова // Московский педагогический журнал. — 2023. — №3. — С. 84-104.
5. Пермякова Л. Цифровая дипломатия: направления работы, риски и инструменты // Российский совет по международным делам (РСМД): интернет-сайт. — 27.09.2012. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovaya-diplomatiya-napravleniya-raboty-riski-i-instrumen/ (дата обращения: 03.05.2024).
6. Ромашкина Н. Информационный суверенитет или почему России нужна стратегия информационной безопасности // Российский совет по международным делам (РСМД): интернет-сайт. — 06.08.2019. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ (дата обращения: 03.05.2024).
7. Смирнов А.И. Современные информационные технологии в международных отношения. — М: МГИМО-Университет, 2017. — 341 с.

8. Федоров А.В. Информационная безопасность: политическая теория и дипломатическая практика: монография / А.В. Федоров, Е.С. Зиновьева. — М.: МГИМО-Университет, 2017. — 357 с.

9. Aarnio H. International Digital Marketing Strategy as a Growth Opportunity. Case: Finnish startup / Heli Aarnio // Master's Thesis Report. — Haaga-Helia University of Applied Sciences, 2017. — 69 c. — URL: https://core.ac.uk/download/pdf/161417236.pdf (дата обращения: 03.05.2024).

10. Damián T.V. Diplomacy in the Age of AI: Challenges and Opportunities / Damián Tuset Varela // Journal of Artificial Intelligence General science. — 2024. — №1. — P. 98-109.

11. Muthmainnah P.M.I.S. Playing with AI to Investigate Human-Computer Interaction Technology and Improving Critical Thinking Skills to Pursue 21st Century Age / Muthmainnah Prodhan Mahbub Ibna Seraj, Ibrahim Oteir // Education Research International. — 2022. — URL: https://doi.org/10.1155/2022/6468995 (дата обращения: 03.05.2024).

12. Rigley E. Evaluating international AI skills policy: A systematic review of AI skills policy in seven countries / Eryn Rigley, Caitlin Bentley, Joshua Krook, Sarvapali D. Ramchurn // Global policy. — 2024. - №1. — P. 204-217.

REFERENCES:

1. Aarnio H. International Digital Marketing Strategy as a Growth Opportunity. Case: Finnish startup / Heli Aarnio // Master's Thesis Report. — Haaga-Helia University of Applied Sciences, 2017. — 69 p. — URL: https://core.ac.uk/download/pdf/161417236.pdf (accessed: 03.05.2024).

2. Damián T.V. Diplomacy in the Age of AI: Challenges and Opportunities / Damián Tuset Varela // Journal of Artificial Intelligence General Science. 2024. — №1. — P. 98-109.

3. Fedorov A.V. Informatsionnaya bezopasnost': politicheskaya teoriya I diplomaticheskaya praktika: monografiya [Information Security: Political Theory and Diplomatic Practice: A Monograph] / A.V. Fedorov, E.S. Zinovieva. M.: MGIMO-Universitet [MGIMO University], 2017. — 357 p.

4. Informatsionnaya bezopasnost' Rossiiskoi federatsii [Information Security of the Russian Federation (Lecture)]. / Zinovieva E.S. // Rossiiskoe Obshchestvo «Znanie» [Znanie Russia]: official site. — 13.05.2022. — URL: https://znanierussia.ru/library/video/informacionnaya-bezopasnost-rossijskojfederacii-979(accessed: 03.05.2024).

5. Kalita A.V. Formirovanie novykh professional'nykh kompetentsii studentovmezhdunarodnikov [Formation of New Professional Competences of International Students] / A. V. Kalita // Problemy sovremennogo pedagogicheskogo obrazovaniya [Problems of Modern Pedagogical Education]. 2022. — №76(3). — P. 114-116.

6. Kochetkov A.P. Tsifrovoi suverenitet kak osnova natsional'noi bezopasnosti Rossii v global'nom tsifrovom obshchestve [Digital Sovereignty as the Basis of Russia's National Security in a Global Digital Society] / A. P. Kochetkov, K.V. Maslov // Vestnik Moskovskogo Universiteta. Politicheskie nauki [Moscow University Bulletin. Series 12. Political Science]. — 2022. — №2. — P. 31-45.
7. Muthmainnah P.M.I.S. Playing with AI to Investigate Human-Computer Interaction Technology and Improving Critical Thinking Skills to Pursue 21st Century Age / Muthmainnah Prodhan Mahbub Ibna Seraj, Ibrahim Oteir // Education Research International. — 2022. — URL: https://doi.org/10.1155/2022/6468995 (accessed: 03.05.2024).
8. Naturkach M.V. Formirovanie mediadiskursivnoi kompetentsii studentov mezhdunarodnogo profilya: rezul'taty praktiki [Developing the Media Discursive Competence of International Students: Experimental Work Results] / M.V. Naturkach, N.M. Romanenko, L.P. Illarionova // Moskovskii pedagogicheskii zhurnal [Moscow Pedagogical Journal]. — 2023. — №3. — P. 84-104.
9. Permyakova L. Tsifrovaya diplomatiya: napravleniya raboty, riski I instrumenty [Digital Diplomacy: Areas of Work, Risks and Tools]. // RSMD [Russian International Affairs Council (RIAC)]: site. — 27.09.2012. — URL.: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovayadiplomatiya-napravleniya-raboty-riski-i-instrumen/ (accessed: 03.05.2024).
10. Rigley E. Evaluating International AI Skills Policy: A Systematic Review of AI Skills Policy in Seven Countries / Eryn Rigley, Caitlin Bentley, Joshua Krook, Sarvapali D. Ramchurn // Global Policy. — 2024. — №1. — P. 204-217.
11. Romashkina N. Informatsionnyi suverenitet ili pochemu Rossii nuzhna strategiya informatsionnoi bezopasnosti [Information Sovereignty or Why Russia Needs an Information Security Strategy] // RSMD [Russian International Affairs Council (RIAC)]: site. — 06.08.2019. — URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitetili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ (accessed: 03.05.2024).
12. Smirnov A.I. Sovremennye informatsionnye tekhnologii v mezhdunarodnykh otnosheniyakh [Modern Information Technologies in International Relations]. M: MGIMO-Universitet [MGIMO University], 2017. — 341 p.