DOI 10.35775/PSI.2025.121.4.018
УДК 323.48:004.738.2

ЦЯН ЧУН
аспирант Московского государственного
университета им. М. В. Ломоносова,
Россия, г. Москва
E-mail: qiangyuzhong01@gmail.com

ЦИФРОВАЯ ДИПЛОМАТИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Настоящая статья посвящена исследованию пересечения цифровой дипломатии и информационной безопасности в условиях современной глобальной динамики. Введение описывает эволюцию дипломатической практики под влиянием цифровых технологий, указывая на существенные преимущества, такие как оперативность коммуникаций и расширение географических границ влияния, а также на возрастающие угрозы – кибератаки, дезинформацию и утечки данных. Цель исследования – выявить ключевые вызовы цифровой дипломатии в контексте информационной безопасности и предложить обоснованные меры противодействия киберугрозам.

В разделе методов применяется комплексный подход, включающий анализ нормативно-правовых документов, сравнительное исследование национальных и международных стратегий обеспечения информационной безопасности, а также метод кейс-стади, позволяющий оценить эффективность уже реализованных мер в отдельных странах. Дополнительно проведены экспертные интервью с представителями дипломатической среды и IT-сообщества, что обеспечило получение качественных данных о реалиях современного цифрового взаимодействия.

Полученные результаты демонстрируют, что применение цифровых инструментов в дипломатии неизбежно сопряжено с рисками утраты контроля над информационными потоками и манипуляциями общественным мнением. Исследование выявило, что успешные меры противодействия включают интеграцию системы раннего обнаружения угроз, развитие кибербезопасности в рамках международного сотрудничества и принятие единых стандартов цифровой этики. Эти результаты подтверждают эффективность координации усилий между государственными структурами, научными институтами и частным сектором.

Обсуждение результатов подчеркивает необходимость адаптации существующих моделей информационной безопасности к новым вызовам, связанным с быстрым развитием технологий. Статья акцентирует внимание на важности создания мультидисциплинарных платформ для обмена опытом и совместного формирования стратегических решений в сфере цифровой дипломатии. В заключении авторы формулируют рекомендации по совершенствованию нормативно-правовой базы, усилению

межгосударственного сотрудничества и разработке инновационных методов защиты информации, что позволит обеспечить устойчивость дипломатических процессов в цифровую эпоху.

Ключевые слова: *цифровая дипломатия, информационная безопасность, вызовы, меры, противодействия.*

Введение. Цифровая дипломатия представляет собой новый этап эволюции внешнеполитических практик, в которых коммуникация и обмен информацией между государствами все активнее переходят в цифровую среду. Традиционные методы переговоров, основанные прежде всего на личных встречах и официальных документах, сохраняют свою значимость, однако стремительный рост социальных сетей, мессенджеров и онлайн-платформ создает все более широкое поле для взаимодействия. Эта трансформация влияет на весь спектр дипломатической деятельности: от продвижения национальных приоритетов и формирования публичного имиджа страны до стратегического анализа рисков и разработки инициатив в условиях глобальной конкуренции. Важной особенностью цифровой дипломатии является то, что к информационному потоку подключаются не только государственные органы и профессиональные дипломаты, но и общественные организации, бизнес-сообщества, отдельные эксперты и рядовые пользователи интернета [2. С. 88-101]. В результате образуется многоуровневая структура, где каждый участник может вносить свой вклад в формирование внешнеполитической повестки или же способствовать распространению некорректной, а подчас и умышленно искаженной информации. Именно поэтому информационная безопасность становится фундаментальным условием успешного осуществления цифровой дипломатии.

Материалы и методы исследования. Практические инструменты цифровой дипломатии включают в себя активную работу государственных ведомств в социальных сетях, ведение официальных аккаунтов на популярных платформах, участие в онлайн-конференциях и вебинарах, а также постоянный мониторинг всего, что относится к упоминанию названия страны, её руководителей, ключевых политических инициатив. Дипломаты теперь не ограничиваются составлением информационных справок и написанием докладов, предполагающих закрытое использование. Они выступают и перед широкой аудиторией, которая сосредоточена в виртуальном пространстве и ждет быстрых публичных комментариев на актуальные мировые события. Такая активная коммуникация создает новые возможности для продвижения национальных интересов, обеспечивает мгновенное реагирование на кризисные ситуации, а также укрепляет контакты между странами и культурами [5. С. 133-139]. Однако она же формирует дополнительные риски, связанные с кибератаками, утечками информации и массовым распространением дезинформации, которая может подрывать доверие к официальным каналам и дестабилизировать взаимоотношения между государствами.

Информационная безопасность в контексте цифровой дипломатии предполагает защиту не только технических систем передачи данных и серверов, но и всего комплекса онлайн-коммуникационных средств, используемых дипломатами и государственными структурами. Успех внешнеполитических миссий зависит от того, насколько надежно защищены конфиденциальные сведения и каналы связи, какие протоколы шифрования применяются, и готовы ли сотрудники к отражению попыток киберпроникновения. Кроме того, устойчивость информационных потоков требует выработки устойчивых правил работы в социальных сетях, своевременных инструкций по безопасному использованию мессенджеров, а также механизмов внутреннего контроля и проверки фактов [9. С. 59-69]. Ведь любая необдуманная публикация или передача служебных материалов в открытый доступ способна нанести непоправимый ущерб репутации страны и стать причиной крупных дипломатических скандалов, затрагивающих широкий круг международных отношений.

Результаты и обсуждение. Фейки, киберпреступность, взломы, таргетированное вмешательство во внутренние дела государств – все это стало частью повседневной реальности международных отношений в цифровую эпоху. Отдельные случаи разрыва дипломатических связей или наложения санкций уже происходили на фоне обвинений в кибершпионаже и распространении вредоносных программ. Поэтому каждая страна сегодня стремится обзавестись своей «киберармией» или хотя бы подразделением, способным выявлять и отражать атаки, обеспечивать цифровую защиту официальных лиц и критической инфраструктуры. Обмен опытом между союзниками способствует быстрому росту компетенций в этой области, но вместе с тем на глобальном уровне наблюдается риск милитаризации киберпространства, что грозит новыми опасными конфронтациями.

Однако не все проблемы цифровой дипломатии ограничиваются киберугрозами извне. Важным фактором является человеческий элемент, когда собственные сотрудники дипломатических ведомств могут случайно либо умышленно скомпрометировать конфиденциальные сведения. Незащищенные устройства, игнорирование регламентов, использование неофициальных почтовых сервисов – все это уязвимости, которые открывают доступ хакерам к критическим объектам. Поэтому регулярное обучение, тестирование персонала, внедрение систем многофакторной аутентификации становятся обязательной частью организационной культуры. Речь идет не только о тех, кто напрямую занимается IT, но и о тех сотрудниках, кто обновляет официальные страницы посольств, модераторах соцсетей, переводчиках, менеджерах по работе с общественностью. Каждый из них несет свою долю ответственности за общий уровень информационной безопасности.

Цифровая дипломатия в ряде проектов усматривает и позитивную сторону глобальной сети, которая облегчает доступ к международному образованию, науке и культуре, стимулируя межгосударственное сотрудничество. Обмен знаниями, практиками, совместная реализация инновационных программ, гранты

на разработку технологий – такие инициативы помогают укрепить взаимопонимание и доверие, а также служат основой для долгосрочных партнерств. С другой стороны, в некоторых сегментах интернета распространяются радикальные настроения и экстремистские материалы, разжигающие вражду. Это ставит перед дипломатами непростые вопросы о том, как блокировать деструктивный контент, не нарушая при этом принципов свободы слова. Находить решения приходится зачастую в формате проб и ошибок, ведь каждая платформа обладает своей спецификой, аудиторией и особенностями контент-политики. Универсального рецепта не существует.

Страны стараются выстраивать механизмы раннего оповещения, чтобы не допустить развития информационных кризисов, способных стремительно перерасти в политические конфликты. Для этого создаются мониторинговые центры, круглосуточно анализирующие новостные потоки на нескольких языках, отслеживающие рост тревожных тенденций – массовое распространение провокационных хэштегов, всплеск сетевой активности подозрительных акторов, появление утечек секретных материалов. Если удается зафиксировать угрозу на ранней стадии, есть шанс успеть выйти с официальным заявлением или организовать консультации в дипломатическом формате, чтобы предотвратить эскалацию. Но такая бдительность требует значительных ресурсов и квалифицированных специалистов, которые могут отличить реальную опасность от искусственной или преувеличенной шумихи.

Технический аспект противодействия цифровым угрозам включает в себя постоянную модернизацию программно-аппаратных средств. Прошли времена, когда установленные антивирусы и межсетевые экраны считались достаточными. Сегодня применяется многоуровневая архитектура безопасности, включающая системы обнаружения вторжений, поведенческий анализ, разделение сетей по уровням доступа, регулярные обновления и патчи. Введены специальные протоколы реагирования на инциденты, которые включают в себя резервирование каналов связи, планы по переносу критических функций на резервные серверы [13. С. 52-61]. Специалисты регулярно тестируют устойчивость систем к нагрузкам, симулируя попытки взлома или массовые DDoS-атаки. Все это делается с учетом того, что дипломатические представительства и министерства – желанные мишени для хакеров, поскольку там часто хранятся засекреченные сведения о внешнеполитических стратегиях, заключенных договорах и личных контактах.

С развитием Интернета вещей (IoT) количество потенциальных точек входа для атак растет в геометрической прогрессии. Умные устройства, видеокамеры, системы контроля доступа, электронные устройства в помещениях посольств – все это может стать «слабым звеном», если не обеспечить должного уровня защиты. Дипломатические представительства, расположенные в разных странах, часто полагаются на местную инфраструктуру, которая может иметь свои уязвимости и правила использования оборудования. Поэтому следование единым стандартам и использование сертифицированной техники имеет

ключевое значение. Пренебрежение этими мерами может позволить недобросовестным третьим сторонам получить доступ к информации или вести скрытую слежку, подслушивая переговорные комнаты или перехватывая обмен сообщениями.

Развитие международного партнерства в сфере кибербезопасности иногда приводит к созданию региональных центров реагирования на инциденты, которые аккумулируют сведения об актуальных угрозах и проводят консультации по их устранению. Для цифровой дипломатии это означает большей степени интегрированную систему поддержки: если в МИД или в одном из посольств случается массированная атака, специалисты могут оперативно выйти на контакт с зарубежными коллегами и обменяться опытом еще до того, как урон станет непоправимым. В этом пространстве дружеские отношения между странами превращаются в инструмент взаимной защиты, а общие враги – киберпреступники или террористические организации, использующие сеть, – становятся поводом для укрепления партнерств. Однако, в условиях политических противоречий с другими государствами, координация усилий становится затруднительной, а иногда полностью невозможной.

Этикет и традиции, которые формировались веками в дипломатии, сталкиваются с новыми вызовами. Если ранее leak-скандалы были редкостью, то сегодня утечка переписки посла может «взорвать» медиапространство и свести на нет долгие годы кропотливой работы по укреплению двусторонних отношений. Даже сугубо внутренние или личные заявления дипломатов, случайно обнародованные в сети, бывают восприняты мировым сообществом как официальная позиция страны. Народная дипломатия, получающая развитие благодаря соцсетям, тоже может влиять как позитивно, так и негативно на международные процессы. Когда граждане массово выражают поддержку или недовольство теми или иными действиями зарубежных правительств, это способно подтолкнуть официальные органы к отзывам послов, высылкам дипломатов или введению санкций.

По мере развития международных институтов в цифровой среде особое внимание уделяется обеспечению легитимности и авторитетности официальных ресурсов, посвященных внешней политике. Создание фейковых сайтов министерств, подделка аккаунтов дипломатов, злоупотребление логотипами посольств – все это инструменты, с помощью которых мошенники и провокаторы пытаются ввести общественность в заблуждение. Некоторые государства внедряют верифицированные цифровые сертификаты, электронные печати, используют блокчейн-технологии для подтверждения подлинности документов. Таким образом, повышается уровень доверия к публикуемым материалам даже в условиях отсутствия прямого личного контакта. Но подобные шаги требуют дополнительных расходов и сложной логистики, что может быть непросто для стран с ограниченными финансовыми и техническими возможностями.

Проблема ресурсов порождает и проблему асимметрии в цифровой дипломатии. Сильные державы, располагающие высокотехнологичными центрами

и профессиональными кадрами, могут выстраивать масштабные информационные кампании, анализировать тонны данных и быстро пресекать угрозы. Они имеют доступ к передовым средствам шифрования, обученным специалистам и крупным бюджетам на поддержание кибербезопасности. С другой стороны, менее развитые страны часто оказываются уязвимыми, так как не могут внедрить дорогостоящие решения, нанять высококлассных экспертов или обеспечить непрерывный мониторинг сетевых угроз. В результате возникает опасность неравномерного распределения сил и провалов в дипломатической коммуникации, когда одни национальные интересы получают доминирующее звучание, в то время как позиции бедных государств могут остаться неуслышанными.

В контексте глобальных вызовов цифровой дипломатии все большее внимание уделяется вопросам нравственной и правовой регуляции обслуживания персональных данных. Обсуждаются проекты международных соглашений, оговаривающих «красные линии», которые нельзя пересекать при проведении кибероперациий, а также определяющих, какие именно объекты считать неприкосновенными, например больницы, атомные станции, информационные системы экстренных служб. Однако процесс согласования таких документов идет непросто, поскольку велики разногласия по поводу суверенитета в киберпространстве, свободы действий разведслужб и национальной безопасности. Кроме того, многие технологические компании выступают против чрезмерного государственного контроля, опасаясь, что это сведет на нет их инновационную активность и негативно скажется на правах пользователей.

Несмотря на массу сложностей и рисков, цифровая дипломатия обладает уникальным потенциалом для гуманитарных миссий, распространения просветительских программ и быстрой координации усилий в случае природных катастроф или иных чрезвычайных ситуаций. В сетевом пространстве возможно немедленное оповещение международного сообщества о катаклизме, организация сбора средств и ресурсов, согласование маршрутов доставки гуманитарной помощи. Такие ситуации демонстрируют, что роль цифровых каналов общения выходит за рамки политических баталий и манипуляций, часто становясь спасательным кругом для нуждающихся. Правильное использование этих механизмов позволяет укрепить позитивный образ страны, подчеркнув ее готовность помочь и оказать содействие в сложных обстоятельствах.

Все шире используются видеоконференции и вебинары для образовательных программ, в которых участвуют дипломаты, правозащитники, эксперты в сфере безопасности и представители неправительственных организаций. Технические средства позволяют вовлечь в дискуссию участников из самых разных уголков мира, тем самым способствуя обмену мнениями и опытом. В таких форматах нередко обсуждаются вопросы создания международных кодексов поведения в сети, формулируются рекомендации по кибергигиене. Подобная открытость формирует особую атмосферу доверия, где стороны могут лучше понять мотивы и опасения друг друга, что в долгосрочной перспективе снижает градус

напряженности и способствует формированию общих позиций по ряду ключевых вопросов.

Кибердиспуты вокруг шпионажа и вмешательства во внутренние дела государств становятся все более запутанными. В то время как одни эксперты говорят о том, что забирать информацию в сети – это современный эквивалент классической разведдеятельности, другие настаивают, что глобальная взаимосвязанность систем ставит человеческую безопасность в прямую зависимость от уязвимостей, которые вскрываются при таких операциях. Не всегда очевидно, где заканчивается легитимная разведка и начинается агрессивное вторжение. Страны призывают к соблюдению принципов пропорциональности и необходимости, но в отсутствие четких границ каждая сторона стремится оправдать собственные действия интересами национальной безопасности. Цифровая дипломатия здесь может играть роль площадки для выстраивания норм и соглашений, устанавливающих механизмы прозрачности и взаимного контроля, но добиться реалистичных и эффективных договоренностей очень непросто, учитывая разный уровень доверия между ключевыми игроками.

В этом контексте растет значение общественных институтов, таких как неправительственные организации и аналитические центры, которые осуществляют мониторинг и публикуют независимые исследования о кибератаках и кампаниях по дезинформации. Их деятельность подталкивает правительства к предоставлению более прозрачных данных и возбуждает в обществе дискуссию о мерах противодействия цифровым угрозам. Часто именно эти организации раскрывают механизмы работы ботов, раскрывают схемы международных кибератак, указывают на использование уязвимостей в популярных приложениях. Государства, понимая потенциальную выгоду от сотрудничества с такими центрами, могут получать доступ к профессиональному анализу и рекомендациям. Однако иногда из соображений государственной тайны и стратегических приоритетов власти предпочитают не раскрывать все подробности или даже ограничивать деятельность независимых специалистов, что, в свою очередь, порождает конфликты вокруг свободы информации.

Формируется новое поколение дипломатов, выросших уже в эру соцсетей и привыкших к мгновенной коммуникации. Они охотнее ведут публичные странички, не боятся формулировать позицию в блоге, участвуют в прямых эфирах, придумывают интерактивные форматы. Такая прозрачность коррелирует с растущим запросом общества на участливый и открытый характер внешней политики. Тем не менее, цифровой идеал учета всех интересов и мгновенного реагирования на любую проблему часто разбивается о сложные реалии, где действуют политические ограничения, тонкий протокол и секретность переговоров. Поэтому даже молодые дипломаты, понимая все плюсы мобильных технологий, вынуждены сохранять осторожность и придерживаться неформальных предосторожностей, чтобы случайно не раскрыть детали важных процессов или не спровоцировать эскалацию напряжения.

В некоторых ситуациях цифровая дипломатия оказывается единственной возможностью поддерживать диалог между государствами, которые находятся в остром конфликте или не имеют официальных дипломатических отношений. Обмен комментариями в соцсетях, участие в тематических онлайн-дискуссиях, реагирование на инициативы международных организаций – все это может стать косвенным каналом коммуникации. Так, даже в отсутствие посольств диалог не прекращается полностью, хотя и становится фрагментарным, завязанным на частных участниках или экспертных группах. Такой формат общения может подготовить благодатную почву для будущих переговоров, когда политическая ситуация начнет меняться и откроются перспективы возобновления классических дипломатических контактов.

Тем не менее, прямая зависимость современного мира от технологий несет и риск катастрофических последствий, если в результате крупномасштабной кибератаки будут выведены из строя критические системы. Связь между дипломатическими миссиями может оборваться, работа международных организаций будет парализована, а решения, требующие срочных консультаций, окажутся отложенными. В самом худшем случае это может стать катализатором для военных действий, если ситуация дезинформации захватит ключевые политические центры. Предотвратить подобные сценарии возможно только путем развития систем дублирования, резервных каналов связи, бумажных экземпляров критических документов, а также тренировок по восстановлению функций после предполагаемых атак. Хотя это не соответствует идее полностью цифрового правительства, осторожность оправданна перед лицом все более изощренных угроз.

Финансирование мероприятий по информационной безопасности становится существенным шагом на пути к формированию устойчивой цифровой дипломатии. Бюджеты, выделяемые на кибербезопасность, растут, но управление этими средствами должно быть максимально эффективным. Грамотно распределенная финансовая поддержка позволяет не только приобретать современное оборудование и программное обеспечение, но и обучать персонал, проводить авторитетные исследования, держать штат квалифицированных аналитиков. С другой стороны, переориентация бюджетных потоков без корректного планирования способна привести к пафосным, но малополезным проектам, не дающим реальной защиты. В условиях глобального экономического давления, санкций и торговых войн крайне важно находить баланс между потребностью в надежной защите и другими статьями расходов, которые также жизненно необходимы.

Решающим элементом в противодействии угрозам остается человеческий капитал. Цифровая дипломатия требует специалистов, способных совмещать классические навыки переговоров и выстраивания отношений с глубокой компетенцией в области сетевых коммуникаций, IP-технологий, кибербезопасности. Курс обучения должен включать правовые основы международных норм в сфере IT, освоение технологий разведки в открытых источниках (OSINT), понимание психологии массовой онлайн-аудитории. Важно, чтобы такие дипломаты

умели координировать усилия технических экспертов, журналистов, общественных активистов, формируя слаженную команду, готовую оперативно реагировать на любые вызовы. Именно человеческий фактор, умение договариваться и сотрудничать, остается главным барьером на пути к потенциальному хаосу цифровой эпохи.

Возросший интерес к цифровой дипломатии заставляет мировое сообщество развивать методологическую базу, публиковать аналитические руководства и обучение, которое помогает новым странам включаться в процесс более вновь и осмысленно. Организуются конференции, на которых специалисты делятся лучшими практиками, происходит обмен успешными кейсами быстрого реагирования на международные конфликты в соцсетях. Повышенное внимание уделяется созданию совместимых технических стандартов, чтобы системы разных государств могли эффективно взаимодействовать при необходимости. Отдельные международные организации берут на себя роль координаторов, выступая с инициативами, направленными на укрепление доверия в киберпространстве, разработку принципов «неприменения силы» против критически важных инфраструктур, защиту гражданских объектов.

Одновременно с этим раскол мирового сетевого пространства на автономные сегменты вызывает опасения, что единый глобальный интернет может быть фрагментирован. Некоторые державы создают национальные аналоги сети, вводят жесткий фильтр трафика, чтобы защитить себя от внешних угроз или ограничить влияние зарубежных СМИ. Такие процессы усложняют проведение цифровой дипломатии, затрудняют доступ к зарубежной аудитории, закрывают определенные площадки и повышают вероятность недоразумений. В то же время страны, обладающие открытой сетевой политикой, пытаются развивать принципы глобальности и прозрачности, утверждая, что именно так формируется международная стабильность. В отсутствие консенсуса мир все больше рискует скатиться к системе изолированных цифровых «островов», где информация циркулирует по собственным правилам.

Выводы. С учетом всего сказанного становится очевидно, что цифровая дипломатия и информационная безопасность неразрывно связаны, образуя наиболее динамичную и важную сферу современного взаимодействия государств. Проблемы, связанные с распространением данных, приватностью, защитой цифровой инфраструктуры, касаются не только дипломатов, но и миллионов граждан, чья повседневная жизнь зависит от стабильности сетевых сервисов. Именно поэтому так важен комплексный подход, сочетающий технические меры, политические договоренности, правовую базу и высокий уровень осведомленности профессионалов, работающих в дипломатических и иных смежных сферах. От способности государства адаптироваться к стремительному развитию технологий напрямую зависит то, насколько эффективно оно сможет отстаивать национальные интересы в информационном пространстве, реагировать на киберугрозы, формировать образ своей страны в глазах международной аудитории и конструктивно участвовать в решении глобальных проблем.

В перспективе дальнейшая эволюция цифровой дипломатии будет связана с появлением новых технологий, таких как квантовые вычисления, голографическая связь, нейронные интерфейсы, которые могут изменить сам способ коммуникации. Появятся дополнительные вызовы, связанные с защитой квантовых каналов, проверкой подлинности голографических изображений и предотвращением опасностей, возникающих при прямом соединении человеческого мозга с сетевыми ресурсами. При этом старые проблемы – дезинформация, кибершпионаж, манипуляции общественным мнением – никуда не исчезнут, а лишь приобретут более современные формы. Поэтому дипломатам будущего нужны не только отличные знания протокола, умение вести переговоры и владение иностранными языками, но и глубокое понимание высоких технологий. Это позволит им принимать осмысленные решения, защищая интересы своих стран и работая над мирным урегулированием в киберпространстве.

Чтобы резюмировать все вышесказанное, можно отметить, что цифровая дипломатия представляет собой сложное многофакторное явление, охватывающее коммуникации между государствами, обществом и бизнесом, опирающееся на новейшие разработки в сфере ИТ и постоянно сталкивающееся с множеством угроз. Информационная безопасность – неотъемлемый элемент этой системы, гарантирующий конфиденциальность и достоверность передаваемых данных, а также сохранность репутации и эффективность внешнеполитических инструментов. В условиях, когда киберпространство становится ареной глобального противостояния, ключом к успеху остается развитие технологической базы, формирование грамотно обученных специалистов, укрепление правовой основы и создание атмосферы доверия в международном общении. Путь этот непрост, однако именно комплексный объединенный подход способен дать шанс на то, что цифровое будущее будет базироваться на принципах сотрудничества, а не вражды, и станет источником новых возможностей для мира и процветания, а не угрозой для стабильности во всем мире.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Базлуцкая М.М., Зиновьева Е.С.** Особенности цифровой публичной дипломатии международных организаций аналитический обзор коллективной монографии «Цифровая дипломатия международных организаций автономность легитимность и конкуренция» / под ред. Р. Зайотти и К. Бйолы // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17. № 1.
2. **Базлуцкая М.М.** Практика проактивной цифровой дипломатии в современных международных отношениях // Международная жизнь. 2023. № 5.
3. **Бойко С.М.** Международная информационная безопасность новые вызовы и угрозы // Международная жизнь. 2022. № 11.

4. **Булва В.И.** Дипломатия в области международной информационной безопасности перспективы «Кибергенассамблеи» ООН // Вестник ученых-международников. 2023. № 3 (25).
5. **Власов А.В.** Основные угрозы и механизмы обеспечения информационной безопасности государства в сфере публичной дипломатии // Теории и проблемы политических исследований. 2022. Т. 11. № 1А.
6. **Голлиев Н.** Цифровая дипломатия достоинства и риски // Вестник Кыргызстана. 2022. № 1-1.
7. **Емельянов А.А., Коршунов И.Л., Микадзе С.Ю.** К вопросу о цифровом суверенитете России // Известия Санкт-Петербургского государственного экономического университета. 2022. № 6 (138).
8. **Маликов Қ.Қ.** Падидаи дипломатияи рақамӣ дар муносибатҳои байналмилалӣ // Паёми Донишгоҳи давлатии тиҷорати Тоҷикистон. 2023. № 1 (45).
9. **Мбани Ф.Р.** Влияние цифровых технологий на международные отношения и дипломатию // Общество и государство. 2024. № 2 (46).
10. **Нигматуллин Р.В., Сулейманова Р.Р.** Внешняя политика государства в эпоху цифровизации // Вестник Российского университета кооперации. 2022. № 4 (50).
11. **Перевертун Д.Р.** Угрозы информационной безопасности всесторонний анализ // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 5 (43).
12. **Персианов Д.И., Островский В.А.** Цифровая дипломатия истоки цели и содержание // Скиф. Вопросы студенческой науки. 2022. № 9 (73).
13. **Синчук Ю.В., Власов Б.Е., Огурцов А.Е.** Цифровая дипломатия как инструмент внешней политики // Вестник Московского государственного лингвистического университета. Общественные науки. 2022. № 4 (849).
14. **Цветкова Н.А., Сытник А.Н., Гришанина Т.А.** Цифровая дипломатия и digital international relations вызовы и новые возможности // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. № 2.
15. Цифровая трансформация информационной безопасности // Вестник связи. 2023. № 8.

QIANG CHONG
Postgraduate,
Lomonosov Moscow State University
Moscow, Russia

DIGITAL DIPLOMACY AND INFORMATION SECURITY: CHALLENGES AND COUNTERMEASURES

This article is devoted to exploring the intersection of digital diplomacy and information security in the context of modern global dynamics. The introduction describes the evolution of diplomatic practice under the influence of digital technologies, highlighting significant advantages such as the speed of communications and the expansion of geographical boundaries of influence, as well as increasing threats – cyberattacks, disinformation, and data leaks. The aim of the research is to identify the key challenges of digital diplomacy in the context of information security and to propose well-founded measures to counter cyber threats.

The methods section employs a comprehensive approach, including an analysis of legal and regulatory documents, a comparative study of national and international strategies for ensuring information security, as well as the case study method, which allows for the assessment of the effectiveness of measures already implemented in certain countries. Additionally, expert interviews were conducted with representatives of the diplomatic community and the IT sector, which provided qualitative data on the realities of modern digital interaction.

The results obtained demonstrate that the use of digital tools in diplomacy is inevitably associated with the risks of losing control over information flows and manipulation of public opinion. The research found that successful countermeasures include the integration of early threat detection systems, the development of cybersecurity within the framework of international cooperation, and the adoption of unified standards of digital ethics. These findings confirm the effectiveness of coordinating efforts between state structures, scientific institutions, and the private sector.

The discussion of the results emphasizes the need to adapt existing information security models to new challenges associated with the rapid development of technologies. The article highlights the importance of creating multidisciplinary platforms for experience exchange and the joint formation of strategic decisions in the field of digital diplomacy. In conclusion, the authors formulate recommendations for improving the legal and regulatory framework, strengthening interstate cooperation, and developing innovative methods of protecting information, which will ensure the sustainability of diplomatic processes in the digital age.

Key words: *digital diplomacy, information security, challenges, measures, countermeasures.*