КИБЕРБЕЗОПАСНОСТЬ КАК ЯДРО ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ДИПЛОМАТИИ

Мамашарифов М.Б.
Университет мировой экономики и дипломатии, кафедра «Международное право и публично-правовые дисциплины», г. Ташкент, e-mail: mamasharifov.mb@uwed.uz
https://doi.org/10.5281/zenodo.21927963

Актуальность темы определяется тем, что цифровизация внешнеполитической деятельности государств сопровождается стремительным ростом угроз информационно-коммуникационной инфраструктуре дипломатических ведомств. Классическая дипломатия, столетиями опиравшаяся на модель Венской конвенции о дипломатических сношениях 1961 года (ВКДС), приобрела цифровое измерение: электронный документооборот посольств, зашифрованная дипломатическая переписка («цифровая вализа»), официальные аккаунты министерств иностранных дел в социальных сетях и консульские онлайн-сервисы стали неотъемлемой частью внешних сношений государств. Одновременно возрастает число зафиксированных кибератак на инфраструктуру дипломатических представительств, что переводит вопрос правового регулирования цифровой дипломатии из плоскости преимущественно коммуникационной в плоскость обеспечения национальной и коллективной безопасности. Целью настоящей работы является обоснование тезиса о том, что именно кибербезопасность образует функциональное ядро формирующегося международно-правового режима цифровой дипломатии, вокруг которого выстраиваются остальные элементы регулирования — от статуса цифровых архивов до атрибуции противоправных деяний.

Международно-правовая база регулирования. При отсутствии специализированной всемирной конвенции о цифровой дипломатии деятельность дипломатических ведомств в сети регулируется универсальными договорами середины XX века на основе доктрины технологической нейтральности. Особое значение в контексте кибербезопасности приобретают статья 24 ВКДС (неприкосновенность архивов и документов независимо от их местонахождения и формы) и статья 27 ВКДС (неприкосновенность официальной корреспонденции): правовой статус и иммунитеты дипломатических документов не зависят от материального носителя, а зашифрованный трафик посольства юридически приравнивается к классической дипломатической почте. Статья 22 ВКДС возлагает на государство пребывания обязанность принимать надлежащие меры для защиты представительства от вторжения или ущерба, что при эволюционном толковании охватывает и киберугрозы системам жизнеобеспечения посольства. Статья 34 Устава Международного союза электросвязи предоставляет государствам право прекращать электросвязь, угрожающую их безопасности, — норма, используемая для обоснования ограничения деструктивного трансграничного информационного воздействия.

Ядром нормативного регулирования на современном этапе выступают источники «мягкого права» — резолюции Генеральной Ассамблеи ООН и доклады переговорных треков Первого комитета: Группы правительственных экспертов (ГПЭ) и Рабочей группы открытого состава (РГОС). Доклады ГПЭ 2013 и 2015 годов закрепили

применимость Устава ООН, включая принципы суверенного равенства, невмешательства и неприменения силы, к киберпространству; суверенитет государств над ИКТ-инфраструктурой на их территории; и принцип должной осмотрительности (due diligence), согласно которому государство не должно сознательно допускать использование своей территории для кибератак против других государств. РГОС переводит эти политические обязательства в предмет обсуждения об их будущей юридической обязательности. Субсидиарно применяются статья 19 Международного пакта о гражданских и политических правах 1966 года (свобода поиска и распространения информации) и Статьи об ответственности государств за международно-противоправные деяния 2001 года, образующие базу для анализа атрибуции кибератак.

Три группы киберугроз дипломатической деятельности. Во-первых, кибершпионаж и несанкционированный доступ к государственным сетям министерств иностранных дел, формально не запрещённый общим международным правом как таковой, но нарушающий национальное законодательство о киберпреступности и принцип информационного суверенитета государства. Во-вторых, кибератаки на критическую инфраструктуру дипломатических представительств — блокирование серверов, систем связи и безопасности, — которые могут квалифицироваться как нарушение обязанности государства пребывания по статье 22 ВКДС. В-третьих, использование ИКТ для дезинформационных кампаний: создание фейковых аккаунтов от имени посольств и применение технологии «дипфейк» для имитации заявлений официальных лиц, что создаёт угрозу международной безопасности и нарушает принцип добросовестности. Региональным ориентиром криминализации таких деяний служит Будапештская конвенция о киберпреступности 2001 года, а под эгидой ООН, при активном участии Республики Узбекистан, разрабатывается всеобъемлющая конвенция о противодействии использованию ИКТ в преступных целях.

Ключевая правовая коллизия — атрибуция кибератак. Существенным препятствием для применения норм об ответственности государств остаётся техническая и юридическая сложность атрибуции: кибероперация против дипломатического объекта может быть проведена через инфраструктуру третьих государств, с использованием анонимизирующих технологий и формально частных групп, действующих в интересах государства без прямого подтверждения такой связи. Статьи об ответственности государств КМП ООН требуют для присвоения поведения государству высокого порога доказывания — эффективного контроля либо однозначного указания на использование его территории, что на практике редко достижимо. В результате государства фактически лишены эффективного правового средства защиты и вынуждены прибегать не к правовым, а к политическим формам реагирования — демаршам и односторонним санкциям. Эта асимметрия особенно значима для государств с ограниченными технологическими ресурсами, включая государства Центральной Азии, чьё формально равное суверенное положение не подкрепляется равными возможностями защиты.

Национальный опыт Республики Узбекистан. Административно-правовой режим кибербезопасности дипломатической деятельности Узбекистана опирается на

Закон «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764, Закон «Об электронной цифровой подписи», Закон «Об информатизации» и Закон «О персональных данных», а также на Стратегию «Цифровой Узбекистан — 2030» (Указ Президента № УП-6079 от 5 октября 2020 года). Координация защиты дипломатической ИКТ-инфраструктуры выстроена как четырёхуровневая институциональная система: Служба государственной безопасности отвечает за отражение комплексных кибератак на высшем уровне; Министерство цифровых технологий обеспечивает защиту национальной ИКТ-инфраструктуры в целом; центральный аппарат Министерства иностранных дел осуществляет ведомственный контроль через управление информационных технологий и связи; загранучреждения и консульства защищают периметр сети и персональные данные на местах. Практическая сложность связана с тем, что серверное и кабельное оборудование, обслуживающее посольства Узбекистана за рубежом, физически находится под технической юрисдикцией страны пребывания, несмотря на иммунитет территории представительства по статье 22 ВКДС; действующий подход основан на применении сквозного шифрования с ключами, генерируемыми уполномоченными органами на территории Узбекистана.

Проведённый анализ выявил, что действующее законодательство о кибербезопасности не содержит специальных требований к защите ИТ-периметра загранучреждений, а ведомственные регламенты МИД не исключают использования коммерческих иностранных облачных сервисов для хранения служебных документов, что создаёт риски утечки данных. В этой связи предлагается: утвердить постановление Кабинета Министров о регламенте информационной безопасности и защиты персональных данных в загранучреждениях, вводящее режим минимизации доверия (Zero Trust) к сетям стран пребывания; включить в Стратегию «Цифровой Узбекистан — 2030» проект суверенного «дипломатического облака» с локализацией серверов на территории страны; ввести в штатные расписания посольств категорий «А» и «Б» должность атташе по цифровым технологиям и кибербезопасности; а на международном уровне — поддержать разработку факультативного протокола к ВКДС 1961 года, специализированно регулирующего статус цифровых архивов, электронной переписки и атрибуции кибератак на дипломатические объекты, в том числе в рамках профильных инициатив Шанхайской организации сотрудничества по международной информационной безопасности.

Заключение. Проведённое исследование подтверждает, что кибербезопасность выступает не периферийным, а системообразующим элементом правового регулирования цифровой дипломатии: именно вокруг задачи защиты дипломатической ИКТ-инфраструктуры и информации выстраиваются как применение классических норм ВКДС и ВККС в силу принципа технологической нейтральности, так и развитие источников «мягкого права» ООН, и национальное регулирование государств. Отсутствие специализированной международной конвенции и нерешённость проблемы атрибуции кибератак сохраняют высокую степень правовой неопределённости, компенсировать которую на нынешнем этапе способны прежде всего национальные меры — институциональные, нормативные и кадровые, — предложенные в настоящей работе применительно к практике Республики Узбекистан.

Adabiyotlar, References, Литературы:

1. Венская конвенция о дипломатических сношениях. — Вена, 1961.
2. Устав Международного союза электросвязи (в действ. редакции).
3. Доклады Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 2013, 2015 гг.
4. Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности».
5. Указ Президента Республики Узбекистан от 5 октября 2020 года № УП-6079 «Об утверждении Стратегии "Цифровой Узбекистан — 2030"».
6. Bjola C., Manor I. The Oxford Handbook of Digital Diplomacy. — Oxford: Oxford University Press, 2024.
7. Мамашарифов М.Б. Цифровая дипломатия в международном праве: правовые основы и перспективы развития в Узбекистане: дис. ... магистра. — Ташкент: УМЭД, 2026.