DOI 10.58351/2949-2041.2025.28.11.004

Гантуяа Гантумур,
Аспирант, Начальник отдела по предотвращению кибератак,
Институт открытого образования Монгольского университета науки и технологии;
Центр по борьбе с кибератаками и инцидентами Монголии
Gantuya Gantumur, Ph.D. Candidate, Head of the Cyberattack Prevention Department
Institute of Open Education, Mongolian University of Science and Technology;
Public CSIRT/CC of Mongolia

Урангоо Хаш-Эрдэнэ,
доктор (Ph.D), Старший научный сотрудник,
Институт Исследования Проблем Безопасности Монголии
Urangoo Khash-Erdene, Ph.D., Senior Research Fellow,
National Institute for Security Studies of Mongolia

Дугэрсурэн Даваадаш,
Старший научный сотрудник,
Институт Исследования Проблем Безопасности Монголии
Dugersuren Davaadash, Senior Research Fellow,
National Institute for Security Studies of Mongolia

КИБЕРДИПЛОМАТИЯ: РАЗВИТИЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ В ЭПОХУ ЦИФРОВИЗАЦИИ, ЕЁ ВЫЗОВЫ И ВОЗМОЖНОСТИ
CYBER DIPLOMACY: THE DEVELOPMENT OF INTERNATIONAL RELATIONS IN THE DIGITALIZATION ERA: CHALLENGES AND OPPORTUNITIES

Аннотация: В статье исследуются теоретико-прикладные аспекты становления и развития кибердипломатии как новой формы международных отношений в условиях цифровой трансформации. Проанализированы ключевые направления кибердипломатии, включающие обеспечение международной кибербезопасности, разработку международно-правовых норм и укрепление национального потенциала государств в цифровой сфере. Особое внимание уделяется роли Организации Объединенных Наций (ООН), Будапештской конвенции о киберпреступности и региональных инициатив в институционализации кибердипломатии.

На примере Монголии проведено исследование современного состояния национальной кибербезопасности, нормативно-правовой базы, деятельности центров реагирования на компьютерные инциденты (CERT/CSIRT), а также уровня вовлеченности в международное сотрудничество. Представлен анализ отчетов Международного союза электросвязи (МСЭ) и Глобального центра по развитию потенциала в области кибербезопасности Оксфордского университета, демонстрирующих прогресс Монголии в развитии законодательства и организационных структур, но указывающих на сохраняющиеся проблемы в техническом оснащении и расширении международного сотрудничества.

Сделан вывод о возрастающей роли кибердипломатии как инструмента поддержания глобальной стабильности и формирования ответственного поведения государств в киберпространстве. Определены приоритетные направления развития кибердипломатии

для Монголии, включающие развитие кадрового потенциала, модернизацию технологической инфраструктуры и активизацию участия в международных правовых инициативах.

Abstract: This article explores the theoretical and practical aspects of the formation and development of cyber diplomacy as a new form of international relations in the era of digitalization. The authors analyze the key areas of cyber diplomacy — ensuring international cybersecurity, developing legal norms, and strengthening the capacity of states in the digital space. Particular attention is paid to the role of the UN, the Budapest Convention, and regional initiatives in the institutionalization of cyber diplomacy.

Using Mongolia as a case study, the article examines the current state of national cybersecurity, the legal framework, the activities of incident response centers (CERT/CSIRT), and the level of international cooperation. It also analyzes the findings of reports by the International Telecommunication Union (ITU) and the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford, which demonstrate Mongolia's progress in legal and organizational aspects but highlight continuing challenges in technical capacity and international collaboration.

The authors conclude that cyber diplomacy is becoming an essential instrument for strengthening global stability and fostering responsible state policies in cyberspace. For Mongolia, key priorities include the development of human resources, improvement of technological infrastructure, and active participation in international legal initiatives.

Ключевые слова: кибердипломатия, кибербезопасность, международные отношения, цифровизация, Монголия, международное сотрудничество.

Keywords: cyber diplomacy, cybersecurity, international relations, digitalization, Mongolia, international cooperation.

ВВЕДЕНИЕ

В условиях возрастающей значимости цифровых технологий, кибердипломатия играет ключевую роль во внешней политике государств. Монголия, стремясь к интеграции в глобальное информационное пространство и защите национальных интересов, уделяет приоритетное внимание развитию данного направления. При этом понимание, принятие той или иной сферы развития в киберпространстве и переход в цифровизацию требует общественного признания и поддержки.

В связи с этим, целью данной работы является анализ состояния и перспектив развития кибердипломатии в Монголии, что позволит выявить ключевые проблемы и вызовы, стоящие перед страной в цифровом пространстве, а также предложить практические рекомендации по совершенствованию кибердипломатической деятельности. В результате чего кибердипломатия должно внести реальный вклад в формировании и применении соответствующих норм в киберпространстве, обеспечивая тем самым глобальный мир и стабильность. Актуальность исследования кибердипломатии в контексте Монголии обусловлена ростом киберугроз, необходимостью укрепления позиций на международной арене и модернизацией экономики. (Вклад и новизна исследования: определение направлений, оценка роли, выявление проблем, разработка рекомендаций, имеющих практическую значимость для государственных органов и научно-исследовательских организаций Монголии). В методологии исследовании использованы общенаучные методы исследования, включая анализ, синтез, сравнение, обобщение, а также методы системного и институционального анализа.

КОНЦЕПЦИЯ И РАЗВИТИЕ КИБЕРДИПЛОМАТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Определение и сущность: Что такое кибердипломатия?

Кибердипломатия –это комплекс мер, реализуемых государствами и организациями в цифровом пространстве для достижения внешнеполитических целей, включая ведение переговоров, предотвращение конфликтов, защиту национальных интересов и продвижение ценностей. (по Йоргену Эстергорду)

ОСОБЕННОСТИ И ФУНКЦИИ

Кибердипломатия осуществляется в виртуальной среде, характеризуется высокой скоростью распространения информации и требует привлечения экспертов в IT и кибербезопасности. Функции кибердипломатии:

Информационная: сбор и анализ информации о событиях и тенденциях в киберпространстве. (Пример: мониторинг социальных сетей для выявления угроз)

Коммуникационная: установление и поддержание контактов с другими государствами и организациями в киберпространстве. (Пример: участие в международных конференциях и форумах по кибербезопасности)

Защитная: защита национальных интересов в киберпространстве. (Пример: отражение кибератак на критическую инфраструктуру)

Наступательная: проведение операций в киберпространстве для достижения внешнеполитических целей. (Пример: проведение кибероперациий против террористических организаций)

В работе Д. Т. Кюля (2009). «От киберпространства к кибервласти: Выявление проблемы» киберпространство определяется как «публичная сфера в информационном пространстве», требующая конкретных дипломатических усилий для урегулирования конфликтов и взаимодействия между государственными и негосударственными субъектами. Кибердипломатия включает в себя следующие основные направления:

РОЛЬ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

Международные организации играют важную роль в развитии кибердипломатии, обеспечивая платформу для обсуждения вопросов кибербезопасности, разработки норм и координации усилий государств в противодействии киберугрозам. (Примеры: деятельность ООН в сфере кибербезопасности, разработка норм поведения государств в киберпространстве под эгидой ОБСЕ, работа Совета Европы по защите персональных данных)

К примеру:

Будапештская конвенция 2001 года: первый международно-правовой документ по борьбе с киберпреступностью, заложивший основу для совместного решения государствами-членами вызовов и препятствий, возникающих в сфере информационно-коммуникационных технологий. Конвенция является моделью для последующих международных договоров и соглашений.

Группа правительственных экспертов Организации Объединенных Наций (ГПЭ ООН): с 2004 года ГПЭ ООН работает над укреплением доверия между государствами-участниками, изучает возможности и ограничения международно-правовых норм в киберпространстве и разрабатывает соответствующие рекомендации. Разработки и

рекомендации группы положили основу для формирования политики международно-правовых документов.

Региональные стратегии и соглашения: Стратегия кибербезопасности Европейского Союза 2013 года и Соглашение о сотрудничестве в области кибербезопасности Ассоциации государств Юго-Восточной Азии (АСЕАН) являются существенным достижением, повлиявшим систематическому развитию кибердипломатии на региональном уровне.

Согласно исследованию «Кибердипломатия: Формирование международного общества в цифровую эпоху» (2021) вышеперечисленные достижения свидетельствуют о формировании института управления киберпространством в международном сообществе. Кибердипломатии присвоена ключевая роль в решении проблем киберсуверенитета, цифрового неравенства и отсутствия всеобщего доверия.

Кроме того, одним из наиболее значимых событий последних лет можно назвать принятие резолюции 74/247 Генеральной Ассамблеи Организации Объединенных Наций об учреждении межправительственного специального комитета для разработки конвенции о “Противодействии использованию информационно-коммуникационных технологий в преступных целях”, основной задачей которой является решение глобальных проблем и вызовов в области технологии посредством коллективных усилий и созданию общеприемлемой и обязательной правовой базы.

Спецкомитет в рамках своей деятельности 2021-2024 гг. занимался разработкой всеобъемлющего правового инструмента, принимая в расчёт национальные, региональные и многосторонние усилия, передовую практику о противодействии использованию информационно-коммуникационных технологий в преступных целях, в итоге чего в декабре 2024 года Генеральная Ассамблея ООН приняла Конвенцию против киберпреступности.

1.2 Кибердипломатия: новые вызовы

Несмотря на достигнутый прогресс в кибердипломатии существуют новые вызовы, решение которых вызывает некоторые затруднения:

Выявление киберпреступления /кибератаки/ и привлечение к ответственности: Установить, выявить кибератаку или киберагрессию /нарушение/ является весьма затруднительным что создаёт проблемы привлечения за содеянное к ответственности. Использование хакерами передовых методов APT (Advanced Persistent Threats), а также ипользование специальных технологий, поддерживаемых государствами, покрывает происхождение атак, то есть выявить нарушителя. Эта неопределенность усиливает недоверие между странами и продолжает препятствовать внесению правовых аспектов и координирующих изменений в сфере кибербезопасности.

Правовые нормы и их имплементация: Процесс разработки общепризнанных и обязательных международно-правовых норм продолжает осуществляться медленными темпами из-за конфликта интересов между государствами. Несмотря на принятие первой международной конвенции о борьбе с киберпреступностью, её имплементация во многом зависит от геополитического соперничества и стратегических интересов крупных держав. Некоторые государства отказываются от присоединения к этим документам или склонны толковать их имплементацию исходя от своих собственных интересов.

Негосударственные субъекты: Растущее влияние негосударственных субъектов, таких как киберпреступные группировки, международные корпорации и правозащитные организации, бросая вызов традиционной «государственно-центричной» дипломатической парадигме препятствуют формированию правовых норм и политики в киберпространстве.

Кроме вышеперечисленных факторов, эксперты сходятся во мнении, что основная проблема, возникающая при противодействии преступлений с использованием информационных технологий и борьбы с киберпреступностью, заключается в том, что развитие международной и национальной правовой системы и нормативные акты значительно отстают от технологического прогресса. Когда поднимается вопрос об устранении некопетентности или пробелов действующей правовой системы, государства разделяются во мнении относительно применимости международных правовых норм и других соответствующих документов, Устава ООН касающихся киберпространства. Мнения расходятся в следующих вопросах:

Применяются ли /в какой степени/ действующие международные правовые нормы в киберпространстве той или иной страны;

Большинство стран согласны с тем, что международно-правовые нормы, соответствующие статьи Устава ООН и резолюции Генеральной Ассамблеи ООН в определённой степени регулируют обязанности государств-членов в киберпространстве.

1.3 Соблюдение Устава ООН в киберпространстве:

Среди государств-членов существует широкий консенсус относительно того, что Устав ООН должен применяться в киберпространстве в полном объеме, что подтверждается докладами Группы правительственных экспертов, Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и соответствующими резолюциями Генеральной Ассамблеи ООН.

Однако некоторые положения Устава ООН и их толкование создают определенные недопонимания. Например:

Как определяется государственный суверенитет в киберпространстве:

Статья 2 Устава регламентирует один из основных принципов Устава ООН, а именно самоопределение и равенство государств-участников. Согласно Уставу, каждое государство-участник обязуется уважать независимость другого и в этом контексте соглашается не участвовать в кибердеятельности, подвергающей нарушению суверенитета другого государства. В то время как трансграничные кибератаки, направленные на «базы данных», часто используют такие инструменты, как VPN и прокси-серверы, для сокрытия атак, что существенно затрудняет идентификацию злоумышленников. Это приводит к затруднению доказательства трансграничной операции или киберпреступной деятельности, способной поставить под угрозу суверенитет атакованного государства.

Как принцип невмешательства во внутренние дела регулируется в киберпространстве:

Принцип невмешательства во внутренние дела, исходящий из принципа государственного суверенитета, запрещает одному государству-участнику вмешиваться во внутренние или внешние дела другого с целью оказания давления. Однако эксперты считают, что информационно-коммуникационные технологии создают возможности для вмешательства во внутренние и внешние дела страны, несмотря на этот принцип. В связи с этим возникает следующий вопрос.

Согласно традиционным понятиям, кибератаку без применения оружия можно ли отнести к таким категориям преступления как – принуждение, применение силы или военная агрессия?

Страны-участники Рабочей группы открытого состава по вопросам безопасности в сфере информационно-коммуникационных технологий считают, что кибератаки и повлекшие за ними последствия следует ассоциировать с традиционным нарушением и

преступлением, исходя из масштаба атаки, причиненного ущерба и последствий. Например, если кибератака нанесла серьезный финансовый и экономический ущерб, некоторые страны могут расценивать ее как форму «применения силы».

В результате страны-участники объединились во мнении о необходимости запрета применения силы что стало основной дилемой рабочей группы. Однако, вопрос касающийся осуществления права на самооборону в случае совершения кибератаки в контексте военной агрессии, Рабочая группа открытого состава не смогла достичь консенсуса, так как государство может применить самооборону только если военная агрессия была совершена традиционным способом, то есть с использованием вооруженных сил.

Статья 51 Устава ООН об осуществлении права на самооборону в ответ на кибератаку:

Статья 51 Устава ООН регулирует осуществление права государства-участника на самооборону индивидуально или коллективными силами, в случае вооруженного нападения со стороны другого государства. Естественно возникает вопрос о том, насколько это регулирование совместимо с киберсредой и кибератаками, и определяется ли критериями военной агрессии включая только физический ущерб или же он рассматривает кибератаки, наносящие финансовый, экономический, экологический или политический ущерб? Помимо этого вопрос о необходимости учитывать факторы о содержании, цели и ущерба кибернападения, предложеные в Таллинском руководстве остаётся спорным. Вопрос о применении самообороны, как средство реагирования на кибернападение сталкивается с противоречием, и следовательно может ли страна, ставшая жертвой кибератаки использовать традиционный подход с вовлечением военных или вооруженных сил. Именно из-за расхождения мнений по этому вопросу Группа правительственных экспертов не смогла принять свой доклад на основе общественного консенсуса в 2017 году.

В заключении доклада Рабочей группы открытого состава 2021 года указано что меры, принимаемые государством, пострадавшим от кибератаки, в ответ на кибератаку со стороны другого государства, которое, по его мнению, могло совершить кибератаку, должны соответствовать Уставу ООН и международному праву, а также его обязательствам по разрешению конфликтов мирными путём и предотвращению международно-противоправных деяний.

2. КИБЕРБЕЗОПАСНОСТЬ В МОНГОЛИИ И ДИПЛОМАТИЯ КИБЕРДИПЛОМАТИЯ В МОНГОЛИИ ОСНОВНЫЕ НАПРАВЛЕНИЯ

Развитие кибердипломатии в Монголии осуществляется по следующим направлениям:

Защита критической информационной инфраструктуры: принятие мер по защите государственных информационных систем, энергетической инфраструктуры, транспортных сетей и других объектов от кибератак.

Борьба с киберпреступностью: сотрудничество с другими государствами и международными организациями в борьбе с киберпреступностью.

Участие в международном сотрудничестве: участие в международных конференциях, форумах и проектах в области кибербезопасности.

Продвижение национальных интересов в цифровой среде: использование цифровых технологий для продвижения монгольской культуры, туризма и бизнеса на международной арене.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Вопросы кибербезопасности и кибердипломатии регулируются рядом законодательных и нормативных актов Монголии, включая:

Закон о кибербезопасности: устанавливает основные принципы и меры по обеспечению кибербезопасности в Монголии.

Закон об электронной подписи: регулирует использование электронной подписи в электронном документообороте.

Закон об информации и защите персональных данных: устанавливает правила сбора, обработки и защиты персональных данных.

УЧАСТИЕ В МЕЖДУНАРОДНОМ СОТРУДНИЧЕСТВЕ

Монголия активно участвует в международном сотрудничестве в области кибербезопасности, являясь членом ряда международных организаций и партнером многих государств. (Примеры: участие Монголии в деятельности ООН, ОБСЕ, Совета Европы, ШОС в сфере кибербезопасности)

ПРОБЛЕМЫ И ВЫЗОВЫ

По уровню международного индекса кибербезопасности Монголия по 26.2 процентной защищенности из 194 стран находится в 128 по с

Развитие кибердипломатии в Монголии осложняется следующими факторами:

Недостаточный уровень развития инфраструктуры и технологий: ограниченный доступ к высокоскоростному интернету в сельских районах, устаревшее оборудование и программное обеспечение.

Нехватка квалифицированных кадров: недостаток специалистов в области кибербезопасности, кибердипломатии и IT.

Ограниченность финансовых ресурсов: недостаточное финансирование мероприятий по обеспечению кибербезопасности и развитию кибердипломатии.

Недостаточная координация между ведомствами: отсутствие единого центра координации деятельности различных государственных органов в сфере кибербезопасности.
https://nonews.co/directory/lists/countries/cybersecurity-index

1. Политика и стратегия кибербезопасности

В Монголии на национальном уровне действуют четыре центра реагирования на чрезвычайные ситуации и инциденты в киберпространстве (CERT/CSIRT). Закон о кибербезопасности, принятый в 2021 году, заложил правовую основу для создания центров реагирования нарушений в киберпространстве и определил их функции. В соответствии с законом были созданы следующие центры:

- Национальный центр по борьбе с кибератаками и нарушениями в киберпространстве при Главном разведывательном управлении
- Общественный центр по борьбе с кибератаками и нарушениями в киберпространстве при Министерстве цифрового развития, инноваций и телекоммуникаций

• Центр Вооруженных сил по борьбе с кибератаками и нарушениями при Киберкомандовании Вооруженных сил Монголии

Эти центры официально начали свою деятельность с 2023 года и выполняют свои функции в законодательном порядке. Кроме того, Национальный центр обработки данных, занимаясь развертыванием и эксплуатацией информационных систем государственных органов, продолжает играть важную роль в идентификации, выявлении нарушений в киберпространстве и реагировании на них.

Результаты исследования подчеркивают, что Закон о кибербезопасности и прилагающиеся к нему нормативные акты и постановления обеспечивают правовую основу для достижения значительного прогресса в защите критически важной информационной инфраструктуры страны.

Кроме того, показатели критерии, внесённые в Национальную стратегию кибербезопасности, служат важным инструментом для определения фактического состояния практического применения мер и текущего уровня кибербезопасности организаций с критически важной информационной инфраструктурой, которое выражено в следующих дотижениях :

• Рост числа организаций, внедривших конкретные меры, основанные на оценке рисков кибербезопасности;

• Рост числа организаций, внедривших системы восстановления и стабильного управления бизнесом.

Эти показатели служат основой для анализа, мониторинга и повышения эффективности государственной политики и реализации правовых норм, а также для оценки способности реагирования на киберриски и даёт возможность определить существенный прогресс. В исследовании также подчеркивается необходимость постоянного анализа и повышения эффективности координирующих, организационных мер, предусмотренных в соответствии критерий, в ходе исполнения законодательства.

В рамках реализации политики в области кибербезопасности Монголии представители Министерства цифрового развития, инноваций и телекоммуникаций и Главного разведывательного управления принимают активное участие в дискуссиях и мероприятиях международного характера. Например, дискуссии, о “Конвенцией о киберпреступности” ООН и об обменне разведывательной информацией о киберпреступности (CTI), а также такие международные платформы, как Организация по безопасности и сотрудничеству в Европе (ОБСЕ) и “Альянса по кибербезопасности для взаимного прогресса”, с позициям Монголии по вопросам международной политики в области кибербезопасности, способствуя взаимопониманию и обмену опытом.

Монголия расширяет сотрудничество с зарубежными странами посредством двусторонних соглашений и договоров. Примером этого является меморандум о взаимопонимании, подписанный с Национальным агентством кибербезопасности Израиля. Меморандум предусматривает сотрудничество в области политики, атак и нарушений, обмена передовым опытом и наращивания потенциала. Кроме того, в рамках соглашения о сотрудничестве, подписанного между США и Монголией в 2019 году, с организацией MITRE осуществляется проект по развитию Центра вооруженных сил, предоставлению обучения организациям с критически важной информационной инфраструктурой и дальнейшему укреплению киберпотенциала по всей стране.

Кроме того, международные организации, такие как японское Агентство международного сотрудничества (JICA), Программа развития Организации Объединенных

Наций (ПРООН) и Всемирный банк, оказывают Монголии ощутимую поддержку в повышении ее потенциала кибербезопасности, и несколько учебных программ, реализуемых совместно с Индией, также имеют особое значение в этом контексте. Однако нехватка кадров в сфере кибербезопасности остается актуальной проблемой, поэтому непрерывная подготовка профессиональных кадров в рамках поэтапных проектов обучения со странами-партнерами, как США, Республика Корея и Япония, а также в рамках партнерств НАТО.

2. Культура в области кибербезопасности и социальное участие

Несмотря на то, что Монголия стремительно внедряет цифровую трансформацию в среде с высоким уровнем использования интернета и надежной сетевой инфраструктурой, базовые методы кибербезопасности по-прежнему не получили широкого распространения среди населения. Например, по-прежнему распространены такие рискованные практики, как передача государственными органами официальной информации с использованием личных адресов электронной почты и приложений общего назначения, отказ от двухфакторной аутентификации (2FA) и недостаточная защита паролей. Результаты опроса также показывают, что население слабо различает легитимные веб-сайты и поддельные сайты, предназначенные для фишинга.

Хотя Закон о защите персональных данных, принятый в 2021 году, создал правовую основу для защиты персональных данных, осведомленность граждан о ценности и защите персональных данных в онлайн-среде остается недостаточной. Кроме того, в обществе наблюдается ограниченное понимание кибербезопасности, и, несмотря на создание механизмов для предоставления гражданам и организациям информации о киберпреступлениях и атаках, а также механизм обратного отсчёта, координация и сотрудничество между ними остаются слабыми. Это свидетельствует о том, что кибербезопасность остается серьезной проблемой для общества в целом.

3. Укрепление потенциала в области кибербезопасности

Острая нехватка высококвалифицированных специалистов в области кибербезопасности в Монголии препятствует развитию сектора и негативно сказывается на устойчивости национальной кибербезопасности. Если эта проблема не будет решена комплексно, эффективность борьбы киберугрозами и наращивание внутреннего потенциала останется ограниченной в дальнейшем.

В Монголии реализуется ряд образовательных программ в области кибербезопасности, однако они не имеют централизованной политики и координации, систематической взаимосвязи. Несмотря на то, что Национальной стратегии кибербезопасности 2022 года является киберобразование населения, исследование показывает отсутствие устойчивых и систематических мер для достижения этой цели, особенно программ подготовки административного и управленческого персонала. Хотя некоторые университеты предлагают профессиональные программы в области кибербезопасности, нехватка учебной среды, оборудования и преподавательского состава тоже продолжает оставать реальной проблемой.

В связи с этим международные организации оказывают поддержку Монголии в наращивании потенциала в области киберобразования, при этом ключевую роль играют японское Агентство международного сотрудничества (JICA), ЮНЕСКО и Управление ООН по наркотикам и преступности (УНП ООН). Например, «Проект развития кадровых ресурсов в сфере кибербезопасности», реализуемый JICA, является особо важной

инициативой в сфере образования. Проект, запущенный в 2023 году, преследует три основные цели:

• Создание сети сотрудничества между промышленностью, государственными учреждениями и университетами для развития кадровых ресурсов в сфере кибербезопасности;

• Разработка и реализация образовательных программ для студентов и граждан с уже имеющим образование;

• Разработка и внедрение программ профессиональной подготовки государственных служащих.

В рамках этих усилий JICA работает над выявлением наиболее востребованных в Монголии сегодня навыков, обновлением учебных программ по кибербезопасности в высших учебных заведениях и созданием системы подготовки преподавателей-инструкторов.

Данный проект демонстрирует развитие образования в области кибербезопасности как важного направления международных отношений и подчёркивает значимость одействия партнёров в образовательной сфере в рамках кибердипломатии, основанной на международном сотрудничестве. В дальнейшем существует необходимость систематически включать подобные программы, проекты и инициативы в стратегическую политику высшего образования.

4. Правовая и нормативная среда

В последние годы Монголия предприняла конкретные шаги по созданию правовой и нормативной среды для обеспечения кибербезопасности. Например, в Уголовном кодексе, пересмотренном в 2015 году, киберпреступность определяется как незаконное вторжение, приводящее к неработоспособности информационных систем и сетей, нарушающее их нормальное функционирование или ограничивающее доступ к ним, привлекается к уголовной ответственности. Он также включает положения, несущие ответственность за ипользование интернета для вовлечения несовершеннолетних для преступлений, что является важнейшим достижением в создании правовой основы защиты детей в онлайн-среде.

Несмотря на базовые возможности для расследований киберпреступлений правоохранительные органы, прокуратура и судебные органам власти Монголии, не хватает технических, кадровых и финансовых ресурсов, что влечёт реальные препятствия для создания комплексного и эффективного потенциала. В результате число инцидентов, связанных с киберпреступностью, растет с каждым годом, но система и возможности реагирования на них еще не полностью развиты.

5. Стандарты и технологический потенциал

Монголия старается и прикладывает усилия по применению международных и региональных стандартов кибербезопасности в отечественной практике с учетом национальных особенностей, но существует реальная потребность в обновлении и совершенствовании этих стандартов в соответствие с мировыми тенденциями. В финансовом секторе был достигнут определенный прогресс, но внедрение стандартов в других отраслях остается неравномерным и непоследовательным. Но несмотря на это, некоторых секторах, особенно в государственных учреждениях и финансовом секторе, меры контроля в киберсреде относительно хорошо налажены, за исключением нехватки бюджета, кадровых ресурсов и опыта, что ограничивает эффективность этих мер. Это особенно актуально для сектора здравоохранения.

Некоторые организации проводят аудит безопасности программного обеспечения для улучшения мер контроля в киберсреде, но использование нелицензионного программного обеспечения создает дополнительные риски. Несмотря на надежность инфраструктуры интернет-услуг, реализация требований по защите от DDoS-атак и готовности к ним со стороны интернет-провайдеров остается недостаточной.

Телекоммуникационные компании считаются организациями критически важной информационной инфраструктуры и обязаны проводить мониторинг кибербезопасности, оценку рисков и разрабатывать планы действий в чрезвычайных ситуациях. Однако уровень регулирования остается слабым, а степень реализации – недостаточной. В то же время локальный рынок услуг кибербезопасности расширяется, но их доступность и качество остаются неудовлетворительными.

Некоторые организации также выполняют ИТ-услуги через аутсорсинг, иностранные организации, что может создавать дополнительные риски, а способность оценивать риски таких услуг напрямую связана с уровнем развития и ресурсами организации. Несмотря на то, что в финансовом секторе уже налажены каналы обмена информацией, создание более широкой межсекторальной сети обмена информацией имеет решающее значение для повышения эффективности и устойчивости системы кибербезопасности.

ПЕРСПЕКТИВЫ РАЗВИТИЯ

Кибердипломатия в Монголии имеет хорошие перспективы развития, подкрепленные политической волей и стремлением к укреплению кибербезопасности и расширению участия в международном сотрудничестве. Для реализации этих перспектив необходимо:

Разработать и принять комплексную стратегию кибербезопасности Монголии.

Увеличить инвестиции в развитие инфраструктуры и технологий.

Обеспечить подготовку квалифицированных кадров в области кибербезопасности и кибердипломатии.

Усилить координацию между ведомствами.

Расширять международное сотрудничество в области кибербезопасности.

РЕКОМЕНДАЦИИ

Для совершенствования кибердипломатической деятельности Монголии целесообразно: 1) разработать комплексную стратегию кибербезопасности; 2) увеличить инвестиции в развитие инфраструктуры и технологий; 3) обеспечить подготовку квалифицированных кадров; 4) усилить координацию между ведомствами; 5) расширять международное сотрудничество.

ЗАКЛЮЧЕНИЕ

Кибердипломатия – важный инструмент внешней политики Монголии, позволяющий стране защищать национальные интересы и укреплять позиции на международной арене. Для успешного развития кибердипломатии в Монголии необходимо решение существующих проблем, разработка комплексной стратегии и усиление координации.

Кибердипломатия становится новым дипломатическим механизмом, инструментом формирования долгосрочных и устойчивых урегулирований на международном уровне в ответ на растущие вызовы безопасности цифровой эпохи. Исследования показывают, что

стремительное развитие информационно-коммуникационных технологий вносит фундаментальные изменения в структуру, организацию и политику безопасности международных отношений, и кибердипломатия является областью политики, требующей развития.

Несмотря на определённые достижения Монголии в области правовой базы, институциональной структуры и наращивания потенциала для обеспечения кибербезопасности, существенного прогресса в области технологического развития и международного сотрудничества пока не наблюдается. Согласно докладу Международного союза электросвязи (МСЭ) за 2024 год усилия Монголии в области кибербезопасности были оценены как «укрепляющиеся». Это свидетельствует о том что, несмотря на относительно высокую правовую и организационную оценку, показатели технико-технологической и кооперационной деятельности остаются слабыми.

Монголия старается расширять свои гарницы в области кибердипломатии, но результаты исследования показывают, стране необходимо более активное, смелое участие в двусторонних и многосторонних соглашениях и сотрудничестве, опираясь на стратегическое планирование. Для нашей страны возрастает необходимость активного участия в разработке международных документов, регламентирующих ответственность государств в киберпространстве, а также последовательной защиты национальной безопасности, интересов и позиций на международной арене.

Список литературы:

1. Cornish, P., Hughes, R., & Livingstone, D. (2021). Cyber-Diplomacy: The Making of International Society in the Digital Age. Chatham House.

2. Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer et al. (Eds.), Cyberpower and National Security. National Defense University Press.

3. Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace. Polity Press.

4. Nye, J. S. (2011). The Future of Power. PublicAffairs.

5. Röttger, P., & Gasser, U. (2018). Cyber Diplomacy: A Systematic Literature Review. Berkman Klein Center for Internet & Society.

6. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4-37.

7. United Nations Group of Governmental Experts (UNGGE). Reports (2004-2021).

8. Кибер гэмт хэргийн зохицуулалтын талаарх харьцуулсан судалгаа. Нээлттэй Нийгэм Форум, 2022. х. 86, эх сурвалж: https://forum.mn/product/257219?page=14

9. Cung Vu S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) November 2016 From: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/RSIS cybersecurity%20in%20Singapore

10. Global Cybersecurity Index 2020, 2024. From: www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index

11. ByBenjamin Ang A leading actor in ASEAN cybersecurity. First Published2021, ImprintRoutledge, pages11

12. U.S. Department of State. (2020). The United States Cybersecurity Strategy. (Официальная стратегия США по кибербезопасности, определяющая цели и приоритеты в этой области).

13. European External Action Service (EEAS). (2016). Global Strategy for the European Union's Foreign and Security Policy. European Union.

14. Монгол Улсын Кибер Аюулгүй байдлын тухай хууль, 2021.

15. CCDCOE. (2020) Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action. https://ccdcoe.org/incyder-articles/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/ [Accessed 10 January 2023].

16. ENISA (European Network and Information Security Agency). (2020). Cybersecurity in the EU: Policies and Challenges. European Union.

17. National Cybersecurity Strategy. (2018). Cybersecurity and Infrastructure Security Agency. U.S. Government.

18.https://www.researchgate.net/publication/371101937_Comparative_Analysis_on_Cyber_Diplomacy_in_EU_and_US

19. 117th Congress (2021) H.R.1251: Cyber Diplomacy Act of 2021. https://www.congress.gov/bill/117th-congress/house-bill/1251/text [Accessed 12 December 2022].

20. Attatfa A., Renaud K. & De Paoli S. (2020) Cyber Diplomacy: A Systematic Literature Review, Procedia Computer Science. 176, 60-69. doi: 10.1016/j.procs.2020.08.007 [Accessed 15 November 2022].

21. Barrinha, A. & Renard, T. (2017) Cyber-diplomacy: the making of an International Society in the digital age. Global Affairs. 3, 353–364. https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924 [Accessed 12 November 2022].

22. Bendiek A. (2018) The European Union's Foreign Policy Toolbox in International Cyber Diplomacy, Cyber, Intelligence, and Security. 2 (3), December 2018. https://www.inss.org.il/wp-content/uploads/2019/01/Bendiek.pdf [Accessed 12 ovember 2022]

23. Buchan, R.J. (2016) Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm, Journal of Conflict & Security Law 21 (3), 429-453. doi: 10.1093/jcsl/krw011 [Accessed 16 November 2022].

24. CCDCOE. (2020) Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action. https://ccdcoe.org/incyder-articles/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/ [Accessed 10 January 2023].

25. Cîrnu, C.E., (2017) Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy. The Market for Ideas. 7-8. https://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/ [Accessed 24 November 2022].

26. Cybersecurity Capacity Review. Mongolia, 2024

27. "Цахим орчин дахь хүүхэд хамгааллын талаар бодлого боловсруулагчдад зориулсан удирдамж", 2020 он

28. Засгийн газрын 2023 оны 08 дугаар сарын 30-ны өдрийн 319 дүгээр тогтоолын 1 дүгээр хавсралт "Кибер Халдлага, Зөрчилтэй Тэмцэх Нийтийн Төв" УТҮГ-ын дүрэм. https://legalinfo.mn/mn/detail?lawId=16760334044401&showType=1