***Кибердипломатия как способ обеспечения кибербезопасности***

***Данилова Е.В.***

*Воронежский государственный университет, Студент (бакалавр), 2025*

*E–mail: jane.dan02@mail.ru*

По мере развития информационно-коммуникационных технологий менялось и их значение в международной политике. Цифровое пространство стало милитаризироваться: государственные и негосударственные акторы все чаще используют киберпространство и Интернет для манипуляций, мошенничества, кражи данных, вымогательства и отмывания денег. Для того, чтобы этому противостоять появилась кибердипломатия, которая отчасти диктует внешнеполитический курс лидеров мировой арены.

Данная модель дипломатии должна минимизировать последствия кибертерроризма, кибератак на критически важную инфраструктуру, киберагрессии, утечки данных, кибершпионажа, проводимых как государственными, так и негосударственными акторами международных отношений [4]. Природа киберпространства диктует свои условия: в силу ее особенностей важно заниматься кибердипломатией, а не полагаться исключительно на киберзащиту.

Инициатором международных переговоров и заключения многосторонних переговоров по вопросам информационной безопасности является Российская Федерация. С самого начала ее целью было предотвращение конфликтов и гонки кибервооружений между государствами.

Ряд соглашений был подписан с государствами-членами ОДКБ [1]. Президент Путин в официальном заявлении от сентября 2020 года предложил США восстановить двустороннее сотрудничество в области кибербезопасности, которое осталось без ответа [3].

Однако на данном этапе так и не удалось прийти к конкретным обязательствам государств в области кибербезопасности. Коллективный Запад и США хотят использовать безграничное киберпространство в качестве нового театра военных действий для противостояния усилению Китая, России и других своих оппонентов. Они стараются обеспечить себе свободу рук, для совершения преступлений против информационной безопасности других стран.

Надежная кибербезопасность является ключом к использованию огромных возможностей новых технологий, что служит трамплином для обеспечения экономического роста и общего процветания при минимизации потенциальных рисков. В связи с этим, в марте 2023 года Белый Дом опубликовал Национальную стратегию кибербезопасности [2]. В ней содержался ряд стратегий для обеспечения защиты критически важной инфраструктуры. Также Белый Дом сотрудничает с ЕС в данной сфере.

Подход Китая к кибердипломатии обусловлен всеобъемлющей целью стать «киберсверхдержавой» в экономической, нормативной, военной и коммерческой сферах, которая использует силу цифровых технологий и инноваций для достижения глобального технологического лидерства и модернизации экономического развития. Однако такого понятия, как кибердипломатия китайские источники не употребляют, вместо этого развивается сетевая онлайн дипломатия. Можно сделать вывод, что дипломатия, направленная на предотвращение кибертерроризма, в КНР либо не применяется, либо является государственной тайной.

В то же время Китай признает, что необходимо правовое регулирование киберпространства для защиты суверенитета государств [5].

Список литературы:

1. Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 года // Официальный интернет-портал правовой информации.: http://publication.pravo.gov.ru/Document/View/0001201904260001
2. National Cybersecurity Strategy // The White House, 01.03.2023: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
3. US-Russia Cybersecurity Cooperation: Future Paths and Historical Perspective // geohistory, 04.12.2021: https://geohistory.today/us-russia-cybersecurity-cooperation/
4. What is cyber diplomacy? // Cyber dimlomacy toolbox: https://www.cyber-diplomacy-toolbox.com/Cyber\_Diplomacy.html
5. 中国关于网络空间国际规则的立场 // Ministry of Foreign Affair of PRC, 01.01.2024: https://www.mfa.gov.cn/web/wjb\_673085/zzjg\_673183/jks\_674633/zclc\_674645/qt\_674659/202110/t20211012\_9552671.shtml