

Секция «Конфликты в "цифровом обществе": природа, специфика, механизмы решения»

Киберсанкции в контексте современной международной информационной безопасности

Научный руководитель – Зиновьева Елена Сергеевна

Яникеева Инна Олеговна

Аспирант

Московский государственный институт международных отношений, Факультет международных отношений, Москва, Россия

E-mail: yanikeeva93@mail.ru

Одной из серьезных современных международных проблем являются вызовы в цифровой среде (киберугрозы). С одной стороны, киберпространство стало ареной конкуренции и конфликтов. С другой стороны, в цифровой среде совершается все больше преступлений - нарушаются права физических и юридических лиц, государств, нарушается национальное и международное право.

Киберугрозы включают несанкционированное вредоносное вмешательство в работу какой-либо информационной системы, кражу информации через компьютерные сети, распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и банковских реквизитов, распространение через Интернет противоправной информации, такой как клевета и материалы, возбуждающие межнациональную и межрелигиозную вражду, злонамеренное использование таких технологий как анализ больших данных и использование искусственного интеллекта, вредоносное воздействие на технологии Интернета вещей. При этом новая коронавирусная инфекция способствовала усилению киберугроз [3].

Угрозу для международной информационной безопасности (МИБ) представляет активное проникновение информационно-коммуникационных технологий (ИКТ) в жизнь современных государств. Усиливается риск того, что киберугрозы могут спровоцировать межгосударственные конфликты [1].

Кроме того, важно отметить, что киберпространство уже стало сферой межгосударственной конкуренции, что препятствует развитию международно-правовой регламентации глобального информационного пространства.

Как отмечает программный директор Российского совета по международным делам И.Тимофеев, нестабильное сдерживание, каким оно и является в киберпространстве, может обернуться серьезным мировым конфликтом «даже при наличии ядерной дубинки и угрозы взаимного уничтожения» [2]. При этом цифровая среда связана с другими измерениями безопасности, и кризисы в киберпространстве способны породить политические последствия за его пределами, что, например, демонстрируют российско-американские отношения (введение антироссийских санкций, высылка дипломатов, «визовая война»).

Государства своими силами пытаются оказывать влияние на сложившуюся международную обстановку, в том числе используя односторонние экономические санкции для того, чтобы принудить другие страны или отдельные лица к изменению своего поведения или чтобы нанести им ответный ущерб за их действия в цифровой среде (киберсанкции). В числе наиболее активных инициаторов односторонних кибермер - Европейский союз (ЕС) и Соединенные Штаты Америки (США).

Масштаб существующих киберпроблем и тот факт, что киберпространство становится ареной межгосударственной конкуренции, актуализируют вопрос глобального регулирования цифровой среды. Единым универсальным институтом является Организация Объединенных Наций (ООН). ООН обладает санкционными механизмами, соблюдение которых обязательно для всех государств-членов Организации. Ограничительные меры ООН

применяются, в частности, в таких направлениях как проблемы нераспространения и терроризма. Между тем у Организации отсутствует механизм санкций по вопросам МИБ. При том, что его наличие могло бы повысить координацию государств, усилить легитимность применяемых ограничительных мер и, возможно, снизить или смягчить растущую межгосударственную конкуренцию и конфликты в киберпространстве.

В настоящее время преобладают односторонние ограничительные кибермеры. Перспективы создания многостороннего механизма киберсанкций в качестве механизма решения конфликтов в «цифровом обществе» на уровне ООН остаются неясными, поскольку межгосударственная конкуренция в цифровой среде мешает достижению консенсуса на уровне ООН.

Киберсанкции являются своеобразным способом балансирования посредством нанесения встречного ущерба в отличной от киберсреды, чаще всего в финансовой, сфере. Так, ЕС и США, разрабатывая варианты ответов на киберинциденты, осознают, что на уровне ООН их основными оппонентами являются Китай и Россия, с которыми в настоящее время Брюссель и Вашингтон не изъявляют желания договариваться и, вероятно, не смогут это сделать в связи с внутривнутриполитическими факторами. Однако искать совместные варианты противодействия киберинцидентам на уровне ООН необходимо, поскольку проблематика обеспечения МИБ является глобальной. При этом, международное взаимодействие и механизм санкций ООН по вопросам МИБ возможны и необходимы. Несмотря на то, что такой механизм не позволит наказывать ряд государств, в отношении не относящихся к государствам киберпреступников механизм будет эффективен, подобно действию санкций по правам человека и ядерному нераспространению.

Источники и литература

- 1) Андрей Крутских рассказал о количестве кибератак на объекты критической инфраструктуры России // Журнал «Международная жизнь». 2020. <https://interaffairs.ru/news/show/26787>
- 2) Тимофеев И. Новое сдерживание: как могут развиваться отношения между Россией и НАТО. <https://www.rbc.ru/opinions/politics/28/08/2017/59a3d3a99a79478626538f50>
- 3) Черноусов И. Хакеры скомпрометировали 12 млрд. учетных записей в 2020 году. <https://rg.ru/2021/01/21/hakery-skomprometirovali-12-mlrd-uchetnyh-zapisej-v-2020-godu.html>