УДК 327.7

Коростелев Дмитрий Александрович,
магистрант 1-го курса
Уральского гуманитарного института
Уральского федерального университета

ОТВЕТ ООН НА КИБЕРУГРОЗЫ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Аннотация. Статья посвящена проблеме киберугроз в современных международных отношениях, освещенности данного вопроса в ООН, а также проблемам, которые не позволяют разрешить данный вопрос и корректно бороться с киберпреступностью.

Ключевые слова: киберугрозы, кибербезопасность, киберпреступность, международное право, ООН.

Korostelev Dmitry,
Master's student of the 1st year
Ural Institute of Humanities
Ural Federal University

RESPONSE OF THE UN TO THE CYBER THREATS IN CONTEMPORARY INTERNATIONAL RELATIONS

Abstract. This article considers the problem of cyber threats in contemporary international relations, the prevalence of this topic in the UN, and also the problems which stand in the way of solving this task and do not let fight cyber crime properly.

Key words: cyber threats, cybersecurity, cybercrimes, international law, UN.

За последнее десятилетие цифровая безопасность стала одним из главных вопросов в повестках дня как внутренней, так и внешней политики стран мира. Все большая вовлеченность цифровых технологий в жизнь людей, политику и международные отношения делает проблему цифровой безопасности особенно острой. Цифровая

безопасность — это «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, искажения, изменения или уничтожения информации» [1]. В связи с этим киберугрозы — одни из самых опасных нетрадиционных угроз для государства, которые можно приравнять к безопасности государственных границ [2]. Пропорционально вовлеченности цифровых технологий растет и киберпреступность. Борьба с данным видом преступлений производится не только на национальном уровне, а также на наднациональном. Государства кооперируются в рамках двусторонних и многосторонних коалиций, в том числе и на базе ООН.

В РФ и США проблемы кибербезопасности занимают особое место. Как в случае с традиционными угрозами, у обеих стран свое видение, поэтому они выступают со своими проектами в рамках ООН [3]. С 1998 г. по инициативе РФ в рамках ООН функционирует группа правительственных экспертов (ГПЭ), которая занимается обсуждением данных вопросов в закрытом формате [3]. В 2018 г. РФ выступила с новой инициативой создания рабочей группы открытого состава (РГОС) [4]. Данный формат не был поддержан американской стороной. Тем не менее обе страны репрезентированы в обеих группах и кооперируются в вопросах кибербезопасности [5], единственное отличие в том, что в РГОС могут участвовать страны, которые ранее не приглашались в ГПЭ, что дает им возможность быть услышанными. Это очень большой шаг в борьбе с киберугрозами, поскольку все больше стран начинают полагаться на цифровые технологии, вследствие чего у них также должна быть возможность учувствовать в обсуждении проблем. Также в РГОС могут принимать участие ТНК и НГО. Данные акторы тоже вовлечены в цифровую среду, работают в ней и занимаются ее развитием, в связи с этим учет их мнения — большой шаг для ООН. На данном этапе существует ряд проблем, которые мешают борьбе с киберпреступностью. Нормы международного права (МП) имплементируются некорректно, поскольку не ясно, как они должны работать в киберпространстве. Так, например, устав ООН применим в киберпространстве, но в киберпространстве урон исходит не от «угрозы силой или ее применения» [6]. В на-

стоящий момент в РГОС ведутся дискуссии, как можно было бы применить МП в киберпространстве и что нужно сделать, чтобы оно работало [7].

Акторы вынуждены руководствоваться своим законодательством в данных вопросах, что затруднительно, поскольку преступление зачастую происходит не на их территории. С этим помогают бороться двусторонние и многосторонние соглашения, но этого недостаточно. Тем не менее стоит отметить, что в последние годы наблюдается тенденция установить общие правила и нормы в сфере киберпространства, чему свидетельствует создание РГОС. Необходимо достичь консенсуса в рамках норм МП и решить, как ограничить деятельность в киберпространстве, чтобы при этом не был затронут суверенитет и права человека, поскольку нельзя просто взять и ограничить доступ или каждому создать множество локализованных, отделенных друг от друга сетей, как, например, в Китае. На практике получается, что не все страны сами заинтересованы в этом, поскольку они и их компании не смогут использовать данные лазейки, чтобы тайно добывать информацию, раскрывать секреты других стран или людей, а совершать другие незаконные действия.

Литература

1. Glossary of Key Information Security Terms // NIST Interagency or Internal Report (NISTIR) 7298 Rev. 2. 03.07.2019. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (дата обращения: 26.02.2020).

2. *Ebert H., Maurer T.* The impact of cybersecurity on international relations // Oxford University Press Academic Insights for the Thinking World. 12.02.2017. URL: https://blog.oup.com/2017/02/impact-cyber-security-international-relations/ (дата обращения: 23.02.2020).

3. *Шакиров О.* Кибердипломатия открытого состава // Российский совет по международным делам. 20.12.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberdiplomatiya-otkrytogo-sostava/?sphrase_id=34557237 (дата обращения: 24.02.2020).

4. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Организация Объединенных Наций.

11.12.2018. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R (дата обращения: 24.02.2020).

5. *Hakmeh J., Peters A.* A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet // Council on Foreign Relations. 13.01.2020. URL: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet (дата обращения: 24.02.2020).

6. Устав ООН // Организация Объединенных Наций. 24.10.1945. URL: https://www.un.org/ru/charter-united-nations/ (дата обращения: 26.02.2020).

7. *Stadnik I.* 5th Meeting of the first substantive session of the Open-Ended Working Group (OEWG) // GIP Digital Watch observatory. 11.09.2019. URL: https://dig.watch/resources/5th-meeting-first-substantive-session-open-ended-working-group-oewg (дата обращения: 26.02.2020).

УДК 327.37+341.67+355.019.1

Ларионов Константин Олегович,
бакалавр 4-го курса
Уральского гуманитарного института
Уральского федерального университета

АНАЛИЗ РОССИЙСКОЙ КОНЦЕПЦИИ ПРИМЕНЕНИЯ ЯДЕРНОГО ОРУЖИЯ

Аннотация. В данной статье проведен подробный анализ российской концепции применения ядерного оружия. Рассмотрены основные вызовы и угрозы, нарушающие стабильность концепции ответно-встречного удара, а также ее дальнейшее будущее.

Ключевые слова: упреждающий ядерный удар, ответный ядерный удар, концепция применения ядерного оружия, ДРСМД, ракетное оружие.