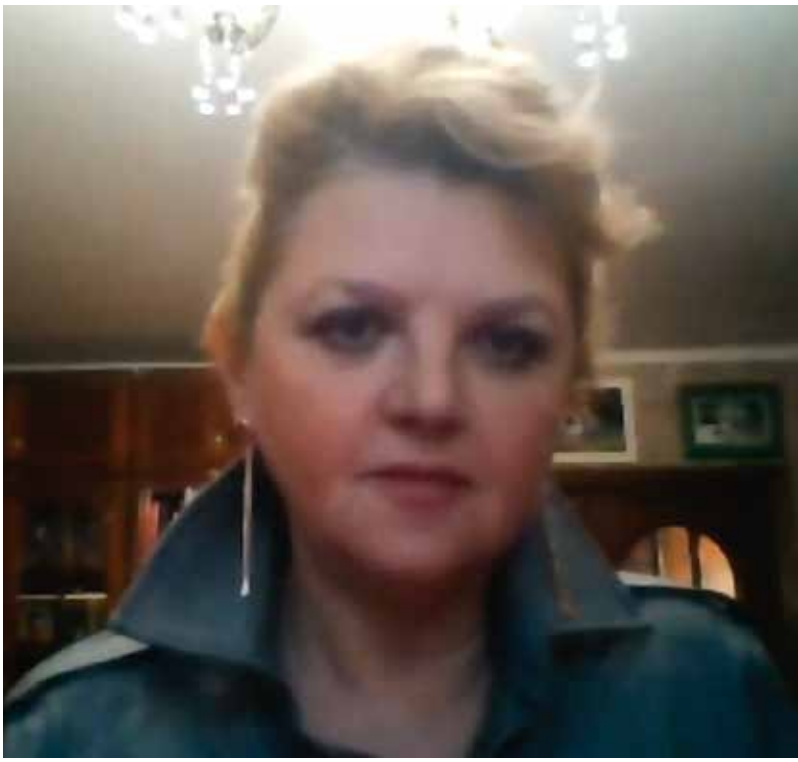
СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
XVI МЕЖДУНАРОДНОГО ФОРУМА

ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ • NATIONAL ASSOCIATION OF THE INTERNATIONAL INFORMATION SECURITY • NAIIS • НАМИБ

19–21 СЕНТЯБРЯ 2022 г.,
МОСКВА, РОССИЯ

Н.П. Ромашкина
к.п.н., профессор, Центр международной безопасности Института мировой экономики и международных отношений имени Е.М. Примакова (ИМЭМО) РАН



ФОРМИРОВАНИЕ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: НОВЫЙ ФОРМАТ

Текущая кризисная ситуация обозначила большое количество проблем в глобальной среде информационно-коммуникационных технологий (ИКТ), в том числе, юридического обеспечения действий в киберпространстве. Еще недавно о многих этих проблемах эксперты из разных стран говорили чисто теоретически, но сейчас речь идет о практическом применении кибернетического оружия, других информационных и киберсредств в условиях кризиса. И сегодня, как никогда ранее, максимально актуально говорить о новом формате, требующем активных действий по предотвращению конфликтов в глобальном информационном пространстве. А для этого необходимо формирование международно-правового режима[1].

Характеристики современного международного пространства даны Президентом России В.В. Путиным в Обращении к участникам и гостям X Московской конференции по международной безопасности 16 августа 2022 г: «Ситуация в мире динамично меняется, формируются контуры многополярного мироустройства. Всё больше стран и народов выбирают путь свободного, суверенного развития с опорой на свою самобытность, традиции, ценности… Этим объективным процессам противодействуют западные глобалистские элиты, провоцируя хаос, разжигая застарелые и новые конфликты, реализуя политику так называемого сдерживания, а по сути — подрыва любых альтернативных, суверенных путей развития… США и их вассалы грубо вмешиваются во внутренние дела суверенных государств: организуют провокации, государственные перевороты, гражданские войны. Угрозами, шантажом и давлением пытаются заставить независимые государства подчиниться своей воле, жить по чужим для них правилам»[2].

Таким образом, процесс противодействия современным угрозам, в число которых входят все более широкое использование ИКТ во враждебных военно-политических целях и киберпреступность, напрямую связан сегодня с процессом построения многополярного мира, основанного на принципах международного права. И это в полной мере отвечает заявленной теме нашего Форума «Многополярный мир в глобальной ИКТ-среде».

Очень опасной современной тенденцией, характеризующей новый формат процесса предотвращения конфликтов в глобальном информационном пространстве, является существенный рост фактов применения различных ИКТ-возможностей во враждебных военно-политических целях в условиях кризиса. В условиях военных действий. И это происходит на фоне роста количества вооруженных конфликтов в различных точках Земного шара, в том числе, на границах России,

1 Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с. https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s.

2 Обращение к участникам и гостям X Московской конференции по международной безопасности. 16 августа 2022 года. http://www.kremlin.ru/events/president/transcripts/69166.

что, безусловно, подрывает ее безопасность. Так называемый, коллективный Запад уже не только на доктринальном уровне, на уровне заявлений и документов, а уже на деле, открыто демонстрирует свою позицию по использованию киберпространства как сферы военных действий[3].

На фоне таких тенденций 24 февраля 2022 г. Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупредил об угрозе увеличения интенсивности компьютерных атак на российские информационные ресурсы, в том числе, объекты критической информационной инфраструктуры (КИИ) в период проводимой военной операции на Украине.

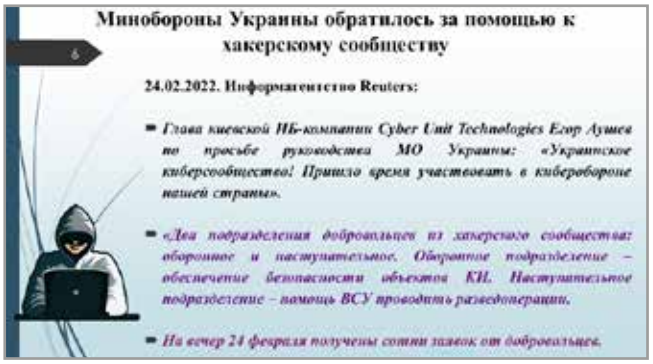
Специалисты НКЦКИ рекомендуют российским организациям усилить бдительность при мониторинге вредоносной активности, направленной на объекты, находящиеся в зоне их ответственности, организовать процесс приоритетной обработки информации об аномалиях, обнаруживаемых в работе объектов КИИ. *«Любой сбой в работе объектов КИИ по причине, не установленной достоверно, в первую очередь необходимо рассматривать как результат компьютерной атаки… В случае выявления признаков целенаправленных компьютерных атак незамедлительно информировать НКЦКИ для своевременной выработки мер противодействия»*[4]. Кроме того, координационный центр обратил внимание на рост угроз как из информационного пространства недружественных России стран, так и из российского информационного пространства. Мы видим, что эти прогнозы, к сожалению, оказались верными.

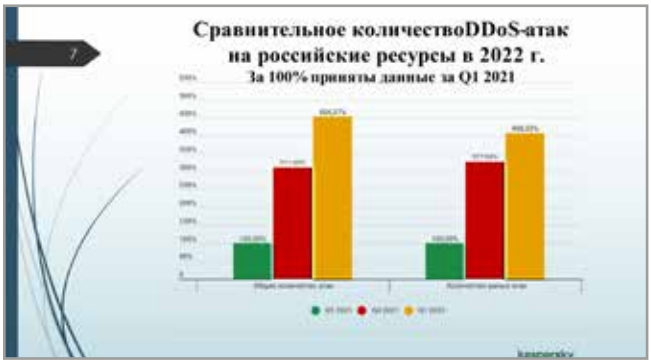
Но сегодня речь идет не только о росте угроз кибератак на информационное пространство России, но и на другие структуры критически важной государственной инфраструктуры.

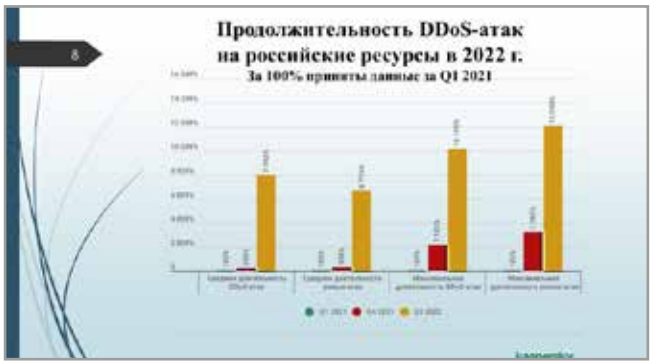
Так, 24 февраля 2022 г. по сообщению телеканала NBC Президенту США Джозефу Байдену был представлен ряд вариантов проведения Соединенными Штатами массированных кибератак, направленных на то, чтобы подорвать способность России поддерживать

3 Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы / Н. П. Ромашкина // Вопросы кибербезопасности. – 2019. – № 1 (29). – С. 2–9. DOI: 10.21681/2311–3456-2019-1-2-9. https://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf.

4 НКЦКИ: существует угроза кибератак на российские информационные ресурсы. 24.02.2022. https://safe-surf.ru/specialists/news/675925/?sphrase_id=45691. https://safe-surf.ru/upload/ALRT/ALRT-20220224.1.pdf.
Центр кибербезопасности РФ предупреждает об угрозе роста интенсивности кибератак. 24 февраля 2022. https://tass.ru/obschestvo/13846783.







свои военные операции на Украине[5]. По данным телеканала, специалисты из разведывательных и военных ведомств предлагают «использовать американское кибероружие» в невиданных ранее масштабах. Среди предлагаемых вариантов — «нарушение интернет-соединения по всей России, отключение электроэнергии и вмешательство в железнодорожное сообщение, чтобы помешать России пополнить запасы своих сил». Кроме того, сообщалось, что киберкомандование США, Агентство национальной безопасности, ЦРУ и другие агентства должны будут сыграть свою роль в этих операциях.

США годами закладывали основу для таких возможных кибероперaций против России, Китая и других противников. Однако такой масштаб атак ранее если и оценивался специалистами как теоретически возможный, но точно не озвучивался официальными лицами США. При этом речь идет о превентивных кибератаках, независимо от того, предпримет ли Россия кибератаки на Соединенные Штаты.

С конца февраля и по сей день российские интернет-ресурсы подвергаются лавинообразным, очень мощным по силе и продолжительности компьютерным DDoS-атакам. ИТ-специалисты говорят о ситуации как об эпидемии. Охват и интенсивность атак огромны. В качестве целей атак выступают сайты госорганов и государственных информационных систем, банков и коммерческих предприятий, Роскосмоса, РЖД, Госуслуг, телеком-провайдеров, СМИ, спортивных и общественных организаций, образовательных и медицинских учреждений и так далее.

«Лаборатория Касперского» сообщает, что по косвенным признакам видно, что в начале всплеска DDoS-атак в них принимало участие большое количество так называемых хактивистов, непрофессиональных хакеров. Со временем их доля в общем числе атакующих снизилась. При этом сами атаки стали более мощными, подготовленными и длительными»[6].

Крайне опасными в настоящее время являются угрозы, связанные с применением космических информационных технологий, спутников стран НАТО и их партнеров во враждебных военно-политических целях. Речь идет о передаче со спутников, в том числе, спутников военного назначения, разведывательной информации формально нейтральным государством для поддержки военных действий одной из сторон военного конфликта и для

5 Biden has been presented with options for massive cyberattacks against Russia. https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.
NBC: спецслужбы предложили Байдену варианты кибератак против России. 24 февраля 2022. https://tass.ru/mezhdunarodnaya-panorama/13846677.

6 Отчеты о DDoS-атаках. https://securelist.ru/category/ddos-reports/.

уничтожения военнослужащих и военной техники другой стороны.

Так, США открыто заявляют на самых разных уровнях, включая Президента США, что они обеспечивают армию Украины разведывательной информацией со своих спутников, в том числе, спутников военного назначения. Это информация о расположении военных объектов, военной техники и военных подразделений армии России, в том числе, подразделений Донецкой народной республики и Луганской народной республики. Министерство обороны РФ подтверждает эту информацию.

Таким образом, получается, что военные спутники, которые являются частью военной инфраструктуры США, используются во время военных действий, в которых Соединенные Штаты формально не участвуют, для предоставления Украине разведданных о расположении подразделений армии России.

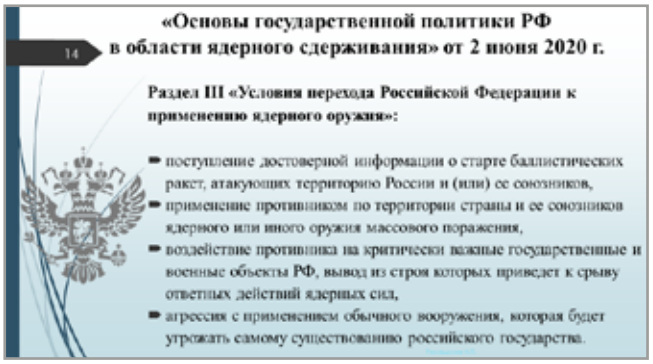
В связи с этим возникают вопросы.

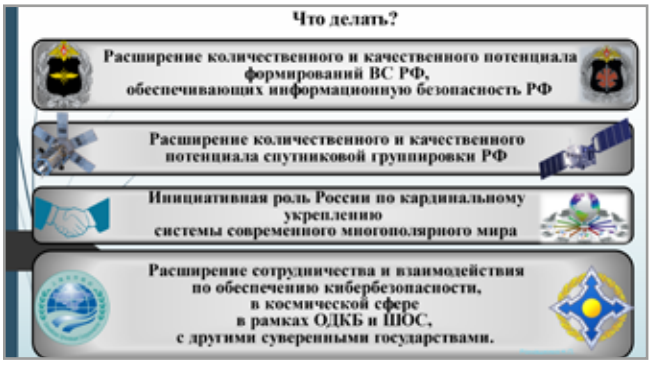
- Какие юридические обоснования подобных действий существуют в международном праве и в нормативно-правовой базе США?
- Можно ли это рассматривать как участие в военных действиях, а, следовательно, в качестве военного вмешательства?
- Можно ли это расценивать как применение силы или угрозу применения силы в соответствии с Уставом ООН?

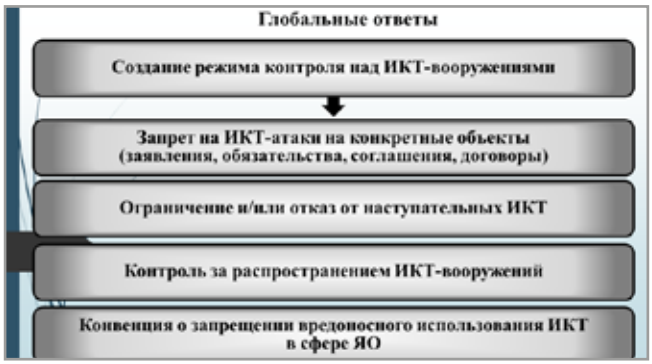
Глобальное враждебное информационное воздействие оказывается на мировое сообщество и в другой области, которую можно назвать не только политической, но и этической, моральной. Это существенно усложняет проблему психологического воздействия на граждан с применением информационно-коммуникационных технологий в период кризиса. Вот только один из примеров.

21 апреля 2022 г. на сайте Государственного Департамента США появилась информация под названием «Что такое «Специальная военная операция?»» (*What Is a «Special Military Operation?»*)[7]. После серии фото звучит, по сути, призыв к гражданам США присоединиться к антироссийской пропаганде с использованием нового предлагаемого Госдепом ИКТ-ресурса. Таким образом, гражданам США навязывается необходимость распространения информации, не подтвержденной никакими доказательствами. Следовательно, гражданам США убедительно предлагается использовать личные средства связи для ведения пропаганды в худшем смысле этого слова. При этом речь идет о рассылке сообщений даже не в средствах массовой информации, а на личные номера и адреса граждан

7 APRIL 21, 2022, What Is a "Special Military Operation?". https://stories.state.gov/what-is-a-special-military-operation/.







России без их предварительного согласия. Логично рассматривать подобные действия в качестве вмешательства в частную жизнь граждан и РФ, и США.

Возникает множество вопросов, в частности:

- Какие юридические обоснования подобных действий существуют в международном праве?
- Какие нормы законодательства США позволяют такие действия?

Все эти наряду с другими вызовами в современных условиях существенно повышают угрозу сокращения, так называемой, «лестницы» эскалации конфликта, а, следовательно, снижает уровень и кризисной, и стратегической стабильности[8]. А это может привести к таким страшным последствиям, которые не выгодны ни одной стране в мире.

При этом важно, что проблема эскалации конфликта усложняется решением НАТО о применении Статьи 5 Устава Альянса к кибернападениям.

Условия перехода Российской Федерации к применению ядерного оружия представлены в Военной доктрине и в документе «Основы государственной политики РФ в области ядерного сдерживания» от 2 июня 2020 г.

Для повышения стабильности, с целью предотвращения конфликтов, в том числе, в глобальном информационном пространстве целесообразно:

- расширение количественного и качественного потенциала формирований ВС РФ, обеспечивающих информационную безопасность РФ;
- расширение количественного и качественного потенциала спутниковой группировки РФ;
- расширение сотрудничества и взаимодействия по обеспечению кибербезопасности, в частности, в космической сфере в рамках ОДКБ и ШОС, с другими суверенными государствами;
- инициативная роль России по кардинальному укреплению системы современного многополярного мира.

Мир, безусловно, будет другим после окончания военной операции. И рано или поздно крупнейшим ядерным державам придется договариваться и о стратегической стабильности, и о формировании международно- правового режима предотвращения конфликтов в глобальном информационном пространстве. И сегодня уже совершенно ясно, что это напрямую связанные межу собой процессы. Но такие усилия требуют новой стратегии действий и новых инструментов.

8 Ромашкина Н.П. Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5. С. 77–86. DOI 10.21681/2311-3456-2020-05-77-86. https://cyberrus.com/wp-content/uploads/2020/12/77-86-539-20_7.-Romashkina.pdf.