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

Конфликты в цифровом обществе, природа, специфика, механизмы решения

Научный руководитель – Курылев Константин Петрович

Месхия Натия

Аспирант

Российский университет дружбы народов, Факультет гуманитарных и социальных наук, Москва, Россия

E-mail: natia.meskhia.1@iliauni.edu.ge

Конференция «Ломоносов 2021»

Секция _ Политические науки.

Конфликты в цифровом обществе, природа, специфика, механизмы решения

Научный руководитель - Константин Курылев Петрович

Месхия Натия

Аспирант

Российский университет дружбы народов, факультет гуманитарных и социальных наук, Москва, Россия.

E-mail: natia.meskhia.1@iliauni.edu.ge

Постиндустриальные общества характеризуются быстрыми технологическими изменениями, которые имеют влияние на вооруженные силы. В начале 1990-х гг., после окончания холодной войны, революция в военных делах усиливает технологическое применение в армии, применяется так называемое «интеллектуальное оружие», дающего новые измерения в искусстве войны. Интернет стал основным инструментом информационного общества, возникший в результате ряда военных исследования.

Появление Интернета обязано Агентству исследовательских проектов (ARPA) (США), желавшее иметь систему связи, способную противостоять ядерной войне с советскими Союзом. Эта инициатива сыграла жизненно важную роль в создании Arpanet, основа для нынешней формы Интернета. По статистике, за 2019 год, треть населения планеты активно пользуется глобальной сетью, причем в более развитых регионах, таких как Северная Америка, Европа и Азия. Количество пользователей Интернета приближается к отметке в 75% [5].

Конфликт - это противостояние двух разных позиций, имеющих совершенно неоднозначные взгляды по решению того или иного вопроса. Рассмотрим конфликт в информационной среде

Конфликты в «цифровом обществе» позволяют осуществлять воздействие на массы людей, а также добиться важных результатов в ходе конфликта между государствами.

Основными элементами информационного конфликта, как и любого другого конфликта, являются:

1) объект конфликта - общественное мнение внутри страны и на международном уровне;

2) субъекты (участники) конфликта - государство, союзы, коалиции, отдельные организации, СМИ;

3) социальная среда, условия конфликта;

4) личное восприятия конфликта [2].

Доступ к технологиям нарушает геополитический баланс. Введение технологии в промышленности и взаимозависимость между сетями критических инфраструктур привело

к новым кибер-угрозам. Информационная революция приводит к росту кибератак или кибервойн вызывает намерение к разрушению информационных и коммуникационных систем противника и к определению и использованию уязвимостей, возникающих из-за взаимосвязанности компьютерных систем [3].

За последние десятилетия киберпространство изменило общество во всем мире, изменив экономику, политику, социальные вопросы и вооруженные силы. Первые кибератаки в рамках военного конфликта начались двадцать лет назад. В последнее десятилетие киберпространство стало центральным аспектом военных операций.

Экономические и военные действия стали все более зависеть от Интернета и сетевых технологий. Тем не менее, эти эволюции и взаимозависимость между сетями критической инфраструктуры привели к новым киберугрозам. Информационная революция подразумевает рост кибератак и появление новой войны- кибервойны. Кибервойна определяется как действия, направленные на кибер-системы противника. По этой причине многие государства разрабатывают оборонительные и наступательные способности, направленные на усиление и ускорение процесса секьюритизации [1].

Ряд международных организаций и частных компаний, решили заняться вопросами стабильности в киберпространстве и урегулирования киберконфликтов. Некоторые государства и негосударственные акторы предлагают принять договор об использовании информационных технологий и международной безопасности. После того, как совещания Группы правительственных экспертов ООН в 2017 г. не смогли достичь консенсуса относительно того, что является ответственным поведением государств в киберпространстве, ООН инициировала два новых переговорных процесса, приняв соответствующие резолюции. Первая - это резолюция, инициируемая Соединенными Штатами и европейскими странами, для создания новой группы правительственных экспертов.

Другая резолюция, выдвинутая Россией и Китаем, говорит о создании рабочей группы открытого состава с целью проведения консультативных совещаний.

Результаты их работы и выработка кодексов поведения в киберконфликте, которые они смогут предложить, послужат руководством для того, как все страны, должны вести себя в будущем в киберпространстве и в отношении кибероперациий.

Именно правовые меры обеспечивают согласованные рамки с целью соблюдать общие нормативные требования и уменьшить количество киберугроз. Наконец, для лучшего диалога и координации, сотрудничество является наилучшим условием в разрешении и недопущении киберконфликтов.

Таким образом, улучшение секьюритизации киберпространства требуют правительственного участия и регулирования. Ожидается, что спрос на кибербезопасность будет расти в последующие годы, и устойчивость этого спроса связана со стратегическим, политическим и экономическим значением кибербезопасности. Главной целью является защита интересов предпрятий, инфраструктур и военных объектов, и проблемы кибербезопасности поднимают вопросы управления киберпространством и цифрового суверенитета.

Разработка киберстратегий должна быть направлена на регулирование отношений между частными лицами, организациями, компаниями и государствами. По этим причинам кибербезопасность должна стать стратегическим национальным приоритетом и для России. Политика кибербезопасности зависит как от государственного, так и частного партнерства, а текущие меры кибербезопасности должны быть основаны на частных и международных инициативах на основе международного сотрудничества и регулирования [4].

Таким образом, появление кибер-войн является кульминацией широкого использования технологий, результатом конфликтов в цифровом обществе. Кибер-война состоит из действий через Интернет, которые представляют новый тип атаки. Кибервойна опреде-

ляется как действия, направленные на нацеливание на любой аспект противника. кибер-системы, такие как связь, логистика или разведка.

Список источников и литературы

1. Богомазова Н.Л., Валеева Г.В., Слобожанин А.В. Современные медиа-этические конфликты ценностей // Наука и современное общество: актуальные вопросы, достижения и инновации. - 2020. - № 7. - С. 137-140.

2. Наумова Е.И. Конфликты в цифровом обществе // Конфликтология XXI века. Пути и средства укрепления мира. - 2019. - № 4. - С. 252-253.

3. Строков А.А. Социальные проявления цифровой культуры // Гуманитарный вектор . - 2020. - № 4. - С. 46-52.