**Баутин Николай Игоревич**

курсант

ФГКВОУ «Военный учебно-научный центр

Военно-воздушных

сил Военно-воздушная академия имени профессора

Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

**КИБЕРБЕЗОПАСНОСТЬ КАК НОВЫЙ ФРОНТ ГЕОПОЛИТИЧЕСКОГО ПРОТИВОСТОЯНИЯ**

Введение

В цифровую эпоху киберпространство стало пятой сферой военных действий наряду с сушей, морем, воздухом и космосом. Кибератаки на критическую инфраструктуру, вмешательство в выборы и цифровой шпионаж превратили кибербезопасность в ключевую проблему международной безопасности. Данная статья исследует эволюцию киберугроз, стратегии ведущих государств в киберпространстве и перспективы международного регулирования этой сферы.

1. Эволюция киберугроз в XXI веке

1.1. Основные типы киберугроз

Современные киберугрозы можно классифицировать по трем уровням:

1. Государственные (кибератаки между странами)

2. Криминальные (финансовые махинации, ransomware)

3. Террористические (дестабилизация инфраструктуры)

1.2. Знаковые киберинциденты

- 2010: Stuxnet - первая кибероружие против иранских ядерных объектов

- 2014: Sony Pictures Hack - атака, связанная с КНДР

- 2017: WannaCry - глобальная эпидемия ransomware

- 2020: SolarWinds - масштабная киберразведка

2. Стратегии ведущих держав в киберпространстве

2.1. США: Оборона через силу

- Создание Киберкомандования (USCYBERCOM) в 2010

- Доктрина "Defend Forward" (2018)

- Партнерство с IT-корпорациями

2.2. Россия: Асимметричный подход

- Акцент на информационные операции

- Развитие автономных хакерских групп

- Концепция "суверенного интернета"

2.3. Китай: Системная кибермощь

- Программа "Великий киберфайрвол"

- Интеграция гражданских IT-компаний в оборону

- Стратегия "Civil-Military Fusion"

3. Проблемы международного регулирования

3.1. Провал существующих инициатив

- Неэффективность Будапештской конвенции

- Отсутствие консенсуса в ООН

- Проблема атрибуции атак

3.2. Перспективные направления

- Создание "Красных линий" в киберпространстве

- Развитие норм ответственного поведения

- Международные киберучения

Заключение

Киберпространство стало ареной нового типа холодной войны. В ближайшее десятилетие мы увидим ужесточение конкуренции за цифровой суверенитет, рост инвестиций в кибервооружения и попытки выработки новых правил игры. Успех в этой гонке будет зависеть от способности государств сочетать технологическое развитие с эффективной стратегией безопасности.

Список литературы

1. Кларк Р., Кнаке Р. Кибервойна. — М.: Альпина Паблишер, 2019.

2. Гусев А.В. Геополитика киберпространства. — М.: Аспект Пресс, 2021.

3. Nye J.S. The Future of Power in the Cyber Age. — Foreign Affairs, 2022.

4. Rid T. Cyber War Will Not Take Place. — Oxford Press, 2020.

5. Министерство обороны РФ Концепция кибербезопасности. — 2021.

Электронные ресурсы

6. CSIS Critical Threats Project — URL: https://www.csis.org/programs/cybersecurity

7. MIT Technology Review: Кибербезопасность — URL: https://www.technologyreview.com/cybersecurity/