Б.И. Шумская
Научный руководитель — кандидат политических наук Н.Ю. Веремеев
БГЭУ (Минск)

ПОЛИТИЧЕСКИЙ КИБЕРТЕРРОРИЗМ: ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ И ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

Начало XXI в. ознаменовалось качественным сдвигом в понимании природы угроз национальной безопасности. Ранее информационные технологии воспринимались как инструменты экономического и социального прогресса. На данный момент они становятся орудиями насилия, манипуляции и подрыва государственной стабильности. Традиционные формы терроризма в виде физического насилия дополнились новыми — анонимными, бесконтактными, но не менее разрушительными по своим последствиям.

Одной из таких форм является кибертерроризм. В научной литературе его понятие остается спорным и фрагментарным из-за двух подходов. Технический подход определяет кибертерроризм как атаки, вызывающие разрушения и хаос в компьютерных системах. Мотивационный подход подчеркивает экстремистские и идеологические мотивы авторов, где кибератаки выступают средством политических целей [1, с. 30–31]. Первый подход рассматривает действие, второй — цель.

Под политическим кибертерроризмом в рамках данной работы понимается преднамеренное и систематическое применение ИКТ государственными и негосударственными акторами ради подрыва легитимности, вмешательства во внутренние дела государств и расшатывания политических процессов. Его специфика состоит в нарушении фундаментальных основ демократии посредством действий через информационное вторжение и подмену реальности.

Выбранный теоретический подход опирается на синтез трех парадигм. Реалистическая теория рассматривает киберпространство как новую арену борьбы государств за власть; кибератаки — метод достижения национальных интересов, отодвигающий мораль и право на второй план [2, с. 153]. Теория сетевых войн описывает конфликты нового типа, в которых главенствующую роль играют децентрализованные государственные (разведка, военные) и негосударственные (террористы, хакеры) сети. Политический кибертерроризм вписывается в модель идеально, используя влияние киберсреды на политику стран [3, с. 21–22]. Постструктурализм видит власть в качестве контроля над данными и дискурсом. В политическом кибертерроризме киберпространство становится полем битвы за этот контроль [4, с. 183].

Классический кибертерроризм и его политически мотивированная форма выбирают схожие методы атак; различие кроется в целях и исполнителях. Классический кибертерроризм инициирован идеологически заряженными группами

и преследует цели запугивания населения, разрушения инфраструктуры. Политический кибертерроризм реализуется в рамках геополитики. Государства и их агенты кибератаками добиваются политических изменений в интересующих странах.

Международное право отстает от темпов эволюции новой угрозы:

- отсутствует общепризнанное определение кибертерроризма;
- размытые границы между кибертерроризмом, кибершпионажем и кибервойной мешают правовой квалификации атак;
- установление авторов атак технически и политически затруднительно;
- политизация и недоверие государств тормозят выработку норм;
- технологическое неравенство малоразвитых стран;
- отсутствует единый орган по международной кибербезопасности;
- угроза правам граждан во имя оправдания цензуры и слежки.

Устранение выявленных международно-правовых проблем и борьба с политическим кибертерроризмом начинается:

- с разработки стандартизированного понятия кибертерроризма;
- создания международного юридического механизма с мандатом расследования и установления уголовной ответственности за кибератаки;
- расширения форм взаимодействия между правоохранительными и разведывательными органами на международном и региональном уровнях;
- поддержки развивающихся государств в создании центров киберзащиты и повышения цифровой грамотности гражданского общества;
- деполитизации кибердиалога — развития экспертных платформ вне рамок геополитического соперничества;
- интеграции стандартов по защите прав человека в международные нормы кибербезопасности.

Политический кибертерроризм — новый вызов суверенитету и демократии, стирающий границы войны и мира. Правовое урегулирование осуществимо при условии формирования нового международного консенсуса, в центре которого должны стоять кибербезопасность и защита цифровых прав граждан.

Источники

1. *Симонова, Э.Ю.* Сравнительный анализ основных подходов к определению кибертерроризма в современной мировой политической науке / Э.Ю. Симонова // Общество: политика, экономика, право. — 2018. — Т. 59, № 6. — С. 29–32.

2. *Кардава, Н.В.* Киберпространство как новая политическая реальность: вызовы и ответы / Н.В. Кардава // История и современность. — 2018. — Т. 28, № 2. — С. 152–166.

3. *Володенков, С.В.* Сетевые информационные войны в современных условиях: основные акторы и стратегии / С.В. Володенков, В.В. Митева // Politbook. — 2016. — № 3. — С. 18–35.

4. *Артамонова, Ю.Д.* Постструктурализм М. Фуко и новые методологические проблемы политических исследований / Ю.Д. Артамонова, А.Л. Демчук // Политическая наука. — 2015. — № 2. — С. 174–191.