УДК 34

Барановский Андрей Валерьевич,
старший преподаватель кафедры физической подготовки,
ФГКОУ ВСИ МВД России,
г. Иркутск
Казазаева Арина Алексеевна,
магистр,
Восточно-Сибирский государственный университет технологий и управления,
г. Улан-Удэ

КИБЕРТЕРРОРИЗМ КАК НОВАЯ ФОРМА ТЕРРОРИСТИЧЕСКОЙ УГРОЗЫ: УГОЛОВНО-ПРАВОВА ОЦЕНКА

Аннотация. *В условиях цифровой трансформации общества кибертерроризм становится одной из наиболее опасных форм преступной деятельности. Глобализация информационных сетей, зависимость критически важных объектов инфраструктуры от цифровых технологий создают новые возможности для реализации террористических замыслов. Цель статьи — проанализировать сущность кибертерроризма как угрозы и рассмотреть его уголовно-правовую оценку в российском законодательстве.*

Ключевые слова. *Кибертерроризм, признаки кибертерроризма, киберпреступления, кибертеррористические угрозы, виды атак.*

Abstract. *In the context of the digital transformation of society, cyberterrorism is becoming one of the most dangerous forms of criminal activity. The globalization of information networks and the dependence of critical infrastructure on digital technologies create new opportunities for terrorist plots.*

The purpose of this article is to analyze the essence of cyberterrorism as a threat and to consider its criminal legal assessment in Russian legislation.

Keywords. *Cyberterrorism, signs of cyberterrorism, cybercrimes, cyberterrorist threats, types of attacks.*

Кибертерроризм — это использование информационных технологий для осуществления террористических актов, направленных на дестабилизацию общества, причинение вреда жизни и здоровью людей либо существенного материального ущерба [5].

Среди ключевого признака кибертерроризма можно выделить следующие: политическая, идеологическая или религиозная мотивация — действия совершаются с целью воздействия на органы власти или международные организации; использование компьютерных технологий — атаки на информационные системы, сети, базы данных; публичность и устрашение — демонстрация возможностей для запугивания общества; целенаправленность на критически важные объекты — энергетика, транспорт, финансы, здравоохранение.

Ключевое отличие кибертеррорима от других видов киберпреступлений, в том числе кибермошенничества, состоит в наличие террористического мотива и нацеленности на создание общественно опасных последствий.

Основные виды атак, в первую очередь это DDoS-атаки на государственные ресурсы, финансовые учреждения и СМИ. Взлом и дефейс веб-сайтов с размещением террористических призывов. Распространение вредоносного ПО для вывода из строя инфраструктуры. Кибератаки на промышленные системы (SCADA), управляющие энергосетями, водоснабжением и т.д. также можно выделить использование соцсетей для координации террористических групп и вербовки других лиц.

Основная проблема области уголовной ответственности за преступления, связанные с кибертерроризмом, связана с тем, что российское

законодательство не содержит отдельной статьи за кибертерроризм, но предусматривает ответственность за смежные составы [4].

Во-первых, это статья 205 Уголовного Кодекса Российской Федерации «Террористический акт» — охватывает кибератаки, если они создают угрозу гибели людей, значительного имущественного ущерба или иных тяжких последствий [1].

Во-вторых, статья 273 Уголовного Кодекса Российской Федерации «Создание, использование и распространение вредоносных программ» — применяется при разработке и применении вирусов для атак на критическую инфраструктуру [1].

В-третьих, статья 274 Уголовного Кодекса Российской Федерации «Нарушение правил эксплуатации ЭВМ» — ответственность за неправомерный доступ к информации, повлёкший уничтожение, блокирование, модификацию или копирование данных [1].

А также, статья 205.2 Уголовного Кодекса Российской Федерации «Публичные призывы к терроризму» — распространяется на онлайн-пропаганду [1].

Так же имеется проблема в области квалификации таких преступлений, в первую очередь, это связано с тем что в законодательстве нет четкого определения понятия «кибертерроризма», что затрудняет отнесение конкретных деяний к этой категории преступлений. Именно поэтому возникаю трудности доказывания — анонимность в сети, трансграничный характер атак; недостаточная детализация норм, то есть отсутствие чётких критериев отнесения кибератаки к террористическому акту; необходимость международного сотрудничества, так как преступники часто действуют за рубежом [7].

Для решения всех вышеперечисленных проблем и повышения эффективности противодействия кибертерроризму необходимо:

1. ввести в Уголовный Кодекс Российской Федерации отдельную статью «Кибертерроризм» с чётким определением состава преступления и санкциями;

2. укрепить международное взаимодействие через создание единой базы данных киберугроз и координацию правоохранительных органов;

3. развивать технические меры защиты — внедрение систем обнаружения вторжений, криптографической защиты;

4. повысить квалификацию следователей в сфере киберпреступлений, путем проведения лекций;

5. усилить превентивную работу — мониторинг соцсетей, просвещение пользователей о киберугрозах.

Кибертерроризм представляет собой серьёзную угрозу национальной безопасности, требующую комплексного подхода. Совершенствование уголовного законодательства, развитие международного сотрудничества и внедрение передовых технологий защиты — ключевые условия для минимизации рисков. Дальнейшие исследования в этой области должны быть направлены на разработку унифицированных правовых механизмов противодействия кибертерроризму на глобальном уровне [4].

Список использованных источников:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от актуальной даты) [Электронный ресурс] // КонсультантПлюс. — URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс] // КонсультантПлюс.

4. Степанова О.А. Актуальные проблемы противодействия кибертерроризму: монография. — М.: Академия Генеральной прокуратуры РФ, 2014. — 99 с.

5. Кобец П.Н. Совершенствование противодействия современным вызовам и угрозам в сфере информационной безопасности Российской Федерации, исходящих от международных террористических организаций // Вестник Восточно-Сибирского института МВД России. — 2022. — № 2 (101). — С. 51–64.

6. Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. — 2021. — № 2 (18). — С. 64–71.

7. Лемайкина С.В. Актуальные вопросы противодействия киберпреступлениям // Криминалистика: вчера, сегодня, завтра. — 2020. — № 4 (16). — С. 54–59.

8. Доклад ООН о глобальных тенденциях в области киберпреступности и кибертерроризма (2023) [Электронный ресурс]. — URL: https://www.un.org/