Подводя итог, отметим, что посягательства на жизнь человека, совершаемые с помощью «Интернета», становятся все более изощренными. С развитием интернет-пространства злоумышленники придумывают новые способы совершения преступлений. Особенно важной в данной ситуации является адекватная и своевременная реакция законодателя на стабильное увеличение количества киберпреступлений, в том числе совершаемых посредством сети «Интернет».

СПИСОК ЛИТЕРАТУРЫ

1. Бычкова А.М., Раднаева Э.Л. Доведение до самоубийства посредством использования интернет-технологий: социально-психологические, криминологические и уголовно-правовые аспекты // Всероссийский криминологический журнал. — 2018. — № 1. — С. 101-115.
2. Бычков С.Н. Публичность как признак объективной стороны в преступлениях против личности // Вопросы студенческой науки. — 2017. — № 15. URL: https://cyberleninka.ru/article/n/publichnost-kak-priznak-obektivnoy-storony-v-prestupleniyah-protiv-lichnosti (дата обращения: 28.03.2024).
3. Крылова Н.Е. «Группы смерти» и подростковый суицид: уголовно-правовые аспекты // Уголовное право. — 2016. — № 4. — С. 529-535.
4. Суходолов А.П., Бычкова А.М. К вопросу о роли средств массовой информации в противодействии пропаганде суицида в социальных сетях // Евроазиатское сотрудничество: гуманитарные аспекты. — 2017. — № 1. — С. 111-121.
5. Шарапов Р.Д., Дидрих М.П. Вопросы квалификации преступлений против жизни несовершеннолетних, совершенных с использованием сети Интернет // Электронное приложение к Российскому юридическому журналу. — 2017. — № 6. — С. 81-91.

Телятников Михаил Александрович[1]

Студент 4 курса Института государства и права
Тюменского государственного университета
stud0000239839@utmn.ru

ПРОТИВОДЕЙСТВИЕ КИБЕРТЕРРОРИЗМУ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В современном мире, где цифровые технологии проникли во все сферы жизни человека, кибертерроризм стал одной из наиболее серьезных угроз, стоящих пред государством и обществом. Данная форма объединяет в себе

[1] Научный руководитель: Иванова Лилия Викторовна, доцент кафедры уголовно-правовых дисциплин Тюменского государственного университета.

традиционные методы терроризма с учетом использования новейших информационных технологий, что делает его особенно опасным и сложным для своевременного пресечения. Противодействие кибертерроризму становится все более актуальным на всех уровнях. Государства прилагают огромные усилия для разработки эффективных мер безопасности и сотрудничества в сфере противодействия кибертерроризму. Однако основной проблемой являются существующие пробелы законодательного урегулирования этого явления в нормах уголовного закона. Ведь защита информационной инфраструктуры государства и общества требует разработки и внедрения не только современных технических средств, но также и надлежащей уголовно-правовой охраны.

Ключевые слова: киберпространство, кибертерроризм, кибертеракт, информационно-коммуникационные технологии, кибертеррорист.

Mikhail Aleksandrovich Telyatnikov
4th year student of the Institute of State and Law
University of Tyumen

COUNTERING CYBERTERRORISM IN THE AGE OF ARTIFICIAL INTELLIGENCE

Abstract. In today's world, where digital technologies have penetrated all spheres of human life, cyberterrorism has become one of the most serious threats facing the state and society. This form combines traditional methods of terrorism with the use of the latest information technologies, which makes it particularly dangerous and difficult to combat in a timely manner. Countering cyberterrorism is becoming increasingly important at all levels. States are making great efforts to develop effective security and co-operation measures to counter cyberterrorism. However, the main problem is the existing gaps in the legislative regulation of this phenomenon in the norms of criminal law. After all, the protection of the information infrastructure of the state and society requires the development and implementation of not only modern technical means, but also appropriate criminal law protection.

Key words: Cyberspace, cyberterrorism, cyberterrorism, cyberterrorist, information and communications technology, cyberterrorist

Современное общество активно развивается и совершенствуется в плане научно-технического прогресса, который носит глобальный характер. В рамках этого активное развитие также получили информационно-телекоммуникационные технологии (далее ИТК), которые стали незаменимым спутником современного человека. Искусственный интеллект, большие базы данных для хранения информации, нейронная сеть, виртуальная реальность — все это привычные атрибуты общества двадцать первого века. Технологиче-

ские новинки полностью модифицировали организацию общественных отношений, перенеся их большую часть в информационное пространство. Применение ИТК сейчас носит активно развивающийся характер. За счет этого и формируется огромное информационное поле, в рамках которого взаимодействуют различные субъекты.

Особую опасность при использовании данных технологий приобретают преступления террористической направленности. Терроризм — это злокачественная опухоль всего мирового сообщества. Понятие «терроризм» происходит от латинского слова «terror», что означает в переводе «страх», «ужас». Оно отражает ключевую цель террористов — посеять панику и страх в обществе, используя насильственные, крайне радикальные методы[1].

В настоящее время терроризм принимает различные формы и использует новые технологии для достижения своих целей. Особую популярность в последние годы набирает кибертерроризм. Причиной этого является значительное перемещение общественных отношений разного вида и уровня в киберпространство. При этом его общественная опасность, в условиях активной цифровизации, сравнима с таким видом терроризма как бактериологический или ядерный терроризм, а то и превышает их[2].

При этом в нормативных правовых актах Российской Федерации нет легального закрепления понятия «кибертерроризм». История появления понятия «кибертерроризм» начинается с появления компьютерных сетей. М. Поллитт в 1997 году предложил рассматривать данную форму терроризма как умышленную, политически мотивированную атаку на компьютерные системы[3]. Из предложенной дефиниции сложно произвести разграничение между обычным компьютерным взломом и кибертерактом. Н.А. Голубев предлагает

[1] Семеновский Н.Н. Терроризм как угроза национальной безопасности России // Вестник государственного и муниципального управления. 2015. № 4. С. 42-49.

[2] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10. С. 24-25.

[3] Бураева Л.А Кибертерроризм как новая и наиболее опасная форма терроризма // Пробелы в российском законодательстве. 2017. № 3. С. 35-37.

рассматривать кибертерроризм через умышленную атаку на компьютерную систему (сеть), которая может повлечь наступление тяжких последствий в виде угрозы жизни и здоровья граждан[1]. Иной подход представлен Ю.В. Гавриловой и Л.В. Смирновым, которые предлагают выделение сущности кибертерроризма, так как в целом это понятие во многом идентично терроризму. Сущность заключается в действиях противоправного характера, направленных на умышленное воздействие на информационную систему с целью исполнения требований террористов[2].

Одновременно с этим представляется необходимым выделить и индивидуализирующие признаки кибертерроризма. Во-первых, это присущая данной форме высокая анонимность. Террористы действуют через псевдонимы или создают множество фиктивных учетных записей, что затрудняет работу по их идентификации. Во-вторых, в отличие от традиционного терроризма, кибертерроризм может быть направлен на широкий круг объектов: государственные сайты, системно-информационные хранилища (например, базы данных в банках), а также частные сайты граждан и юридических лиц. Такая большая разносторонность объектов посягательства позволяет кибертеррористам постоянно искать новые уязвимости и слабые места для совершения атак[3]. В-третьих, скорость и масштаб распространение идей кибертерроризма. Все эти признаки в совокупности помогают нам выделять исключительные моменты данной категории терроризма.

Особое внимание следует обратить на то, что в последние годы использование ИТК происходит для подготовки экстремистов и террористов. Как правило, данные технологии направлены на будущую реализацию террористического акта, предусмотренного

---

[1] Голубев В.А. Кибертерроризм — угроза национальной безопасности. URL: www.crive-research.ru.

[2] Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. М.: ЮИ МВД РФ, 2003. 66 с.

[3] Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. 2014. № 4. С. 3-13.

статьей 205 УК РФ[1]. Также создаются и вредоносные программы, с помощью которых возможно выведение из работы жизненно важных государственных систем («Stuxnet», «WannaCry» и др.). Они выступают здесь вместо бомб и взрывчатки, образуя такое явление как кибертеракт. При этом термин «кибертеракт» полностью отвечает признакам террористического акта, но отличается от него только местом его совершения — информационное пространство. С появлением искусственного интеллекта создание и усовершенствование вирусных программ, создание интернет-сообществ, бот-программ с генеративным искусственным интеллектом террористической направленности ускорилось, так как теперь эти алгоритмы выполняет компьютер.

Главной проблемой по противодействию кибертерроризму на сегодня является серьезное отставание законодательной базы от информационных технологий и их правового регулирования. Так, в Уголовном кодексе РФ кибертерроризм в чистом виде не встречается вообще. Можно выделить две группы преступлений, относящихся к кибертерроризму. Первая — это преступления, направленные на финансирование, пропаганду терроризма, призывы к осуществлению и содействию терроризму и другие (ст. 205.1, ч. 2 ст. 205.2 и др.). Важно понимать, что реализация этих действий также может происходить в киберпространстве. Данные составы преступлений на сегодняшний момент законодательно урегулированы в соответствующих статьях Уголовного кодекса, хотя при этом некоторые статьи напрямую не содержит такого признака как «совершенное в сети «Интернет». Но исходя из положений судебной практики, ИТК выступает одним из способов реализации совершения преступления. Верховный Суд Российской Федерации подчеркивал, что действия лица будут также подпадать под ст. 205.1 УК РФ и в случае, если склонение или вербовка осуществляется посредством размещения материалов на различных носителях

[1] Серебренникова А.В. Кибертерроризм: причины и условия // Colloquium-journal. 2021. № 17 (104). С. 47-49.

и путем распространения через ИТК[1]. Ко второй группе, как правильно отмечал Н.А. Бондаренко, можно отнести преступления, целью которых является посягательство на жизненно важные информационные ресурсы государства[2]. Под этим мы подразумеваем совершение кибертеракта. Здесь прямого регулирования в УК РФ нет. Существуют самостоятельные статьи 205 и 273 УК РФ, что в полной мере не отвечает современным угрозам, исходящим из информационной сити. При этом определение кибертеракта в рамках статьи 274.1 УК РФ является не верным. Так как не каждая кибератака на информационную систему — это акт кибертерроризма. Она должна отвечать признакам преступления террористической направленности. Ученые в области уголовного права предлагают разные подходы для преодоления действующего пробела. Так, одним из способов решений данной проблемы является добавление квалифицирующего признака в рамках статьи 205 УК РФ. Данный подход представляется правильным, так как выделение кибертеракта в самостоятельную статью Особенной части УК РФ является громоздким и не нужным.

Не менее интересным представляется подход в рамках которого предлагается дополнить статью 273 УК РФ квалифицирующим признаком, предусматривающим ответственность за создание и использование вредоносных программ в террористических целях[3]. Но использование данного способа урегулирования кажется сложным, так как в рамках этого подхода будет возникать проблема с определением родового объекта уголовно-правой охраны. Перемещение кибертеракта как разновидности преступлений террористического характера в главу, посвященную преступлениям в сфере компьютерной информации, является неверным с точки построения действующего уголовного законодательства.

---

[1] Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 (ред. от 03.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

[2] Прудникова К.К., Бондаренко Н.А. Терроризм в эпоху информационных технологий // Уральский журнал правовых исследований. 2022. № 2 (19). С. 74-80.

[3] Капитонова Е.А. Современный терроризм: монография / Е. А. Капитонова, Г. Б. Романовский. М.: Юрлитинформ, 2015. 216 с.

Кибертерроризм стал серьезной угрозой для национальной безопасности и благополучия Российской Федерации. Для эффективного противостояния киберпреступникам необходимо комплексное и многогранное решение, включающее четкое законодательное определение кибертерроризма, которое позволит разграничивать его с иными составами преступлений. Внесение соответствующих изменений в Уголовный кодекс РФ позволит эффективно противодействовать киберагрессии и привлечь к ответственности лиц, угрожающих критически важной государственной информационной инфраструктуре и жизням граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Бураева Л.А Кибертерроризм как новая и наиболее опасная форма терроризма // Пробелы в российском законодательстве. — 2017. — № 3. — С. 35-37.
2. Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. — М.: ЮИ МВД РФ, 2003. — 66 с.
3. Голубев В.А. Кибертерроризм — угроза национальной безопасности [Электронный ресурс]. — Режим доступа: www.crive-research.ru, свободный (дата обращения: 24.03.2024).
4. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. — 1997. — № 10. — С. 24-25.
5. Иванова Л.В. Уголовно-правовое противодействие киберпреступности в странах БРИКС // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: Сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. — М.: Университет прокуратуры Российской Федерации, 2021. — С. 118-122.
6. Капитонова Е.А. Современный терроризм: монография / Е.А. Капитонова, Г.Б. Романовский. — М.: Юрлитинформ, 2015. — 216 с.
7. Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. — 2014. — № 4. — С. 3-13.
8. Прудникова К.К., Бондаренко Н.А. Терроризм в эпоху информационных технологий // Уральский журнал правовых исследований. — 2022. — № 2 (19). — С. 74-80.
9. Семеновский Н.Н. Терроризм как угроза национальной безопасности России // Вестник государственного и муниципального управления. — 2015. — № 4. — С. 42-49.
10. Серебренникова А.В. Кибертерроризм: причины и условия // Colloquium-journal. — 2021. — №. 17 (104). — С. 47-49.