https://cyberleninka.ru/article/n/vliyanie-usloviy-tsifrovizatsii-na-pravosoznanie-i-povedenie-nesovershennoletnih (дата обращения: 12.04.2025).

4. Криминология: Учебник для вузов/Под общ. ред. д. ю. н., проф. А. И. Долговой. — 3-е изд., перераб. и доп. — М.: Норма, 2005. - 912 с.

5. Серебренникова А. В. Криминологические проблемы цифрового мира (цифровая криминология) // Всероссийский криминологический журнал. - 2020. - №3. - URL: https://cyberleninka.ru/article/n/kriminologicheskie-problemy-tsifrovogo-mira-tsifrovaya-kriminologiya (дата обращения: 12.04.2025).

Телятников Михаил Александрович[1]

Студент 5 курса Института государства и права

Тюменского государственного университета,

stud0000239839@utmn.ru

КИБЕРТЕРРОРИЗМ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. В эпоху стремительных цифровых перемен, оказывающих значительное влияние на существование каждого отдельного человека, общества и государства, особенно актуальными становятся вопросы противодействия террористическим угрозам, исходящим из информационного пространства. Последние годы в российском правовом поле активно обсуждаются вопросы противодействия киберпреступности среди которой особую опасность представляет преступления террористического характера. Российскому законодателю необходимо учитывать реальность существования и всю опасность такого явления как кибертерроризм, а цифровое пространство, оценивать, как потенциальное место, через которое (с помощью которого) реализуются различные террористические

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

деяния, представляющие угрозу для общественной безопасности. В целях преодоления обозначенной проблемы необходимо уделить приоритетное внимание модернизации существующей правовой базы в рамках усиления эффективности уголовно-правовых мер борьбы с кибертерроризмом, путем внесения законодательных изменений.

Ключевые слова: Кибертерроризм, цифровое пространство, информационная безопасность, кибертеррорист, информационное воздействие.

Mikhail Aleksandrovich Telyatnikov
5th year student of the Institute of State and Law
University of Tyumen

CYBERTERRORISM AS A THREAT TO INFORMATION SECURITY OF THE RUSSIAN FEDERATION: CURRENT PROBLEMS AND PROSPECTS OF COUNTERACTION

Abstract. In the era of rapid digital changes that have a significant impact on the existence of every individual, society and state, the issues of countering terrorist threats emanating from the information space are becoming particularly relevant. In recent years, the Russian legal field has been actively discussing issues of countering cybercrime, among which terrorist offences are of particular danger. The Russian legislator should take into account the reality of existence and the danger of such phenomenon as cyberterrorism, and assess the digital space as a potential place through which (with the help of which) various terrorist acts that pose a threat to public safety are realised. In order to overcome this problem, it is necessary to give priority attention to modernising the existing legal framework within the framework of strengthening the effectiveness of criminal law measures to combat cyberterrorism by introducing legislative amendments.

Key words: Cyberterrorism, digital space, information security, cyberterrorist, informational impact.

Современное общество стремительно развивается и совершенствует информационно-коммуникационные технологии (далее – ИКТ), влияние которых трудно не дооценивать для жизни каждого человека и функционирования государственного аппарата. Научно-технический прогресс, охвативший большинство стран мира, с беспрецедентной скоростью трансформирует все привычные нам сферы общественных отношения, включая непосредственное взаимодействия граждан и государства, перенося их в цифровое пространство.

Но за последние десятилетия цифровая среда и новейшие технологии все чаще используются преступниками. В связи с существенным ростом объемов информации, переходом критически важных систем жизнедеятельности государства и общества в цифровое пространство, появляется прямая угроза неправомерного воздействия на эти объекты, а также использования новейших технологий для совершения преступлений, в том числе в террористических целях.

Подобно любому преступному явлению, терроризм характеризуется своей изменчивостью и адаптацией к существующим условиям, использованием новых технологий для реализации террористических целей. Кибертерроризм как форма терроризма обладает рядом специфических особенностей: во-первых, поле деятельности террористов – цифровая среда, которая может быть, как целью атаки, так и инструментом для реализации преступных намерений; во-вторых, кибертеррористические атаки могут воздействовать на множество разнообразных объектов, начиная от государственных информационных систем, заканчивая личными данными граждан и компаний. При этом такие атаки могут быть направлены одновременно сразу на несколько различных объектов[1].

Отсутствие четкого определения «кибертерроризма» в российском законодательстве создает трудности в разработке эффективной правовой основы борьбы с этим явлением. А ввиду того, что «кибертерроризм» обладает уникальными признаками (которые еще находятся в процессе становления) и учитывая,

[1] 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.

что данное явление выступает разновидностью терроризма, правильным представляется подход его определения через одно из направлений террористической деятельности.

Важно помнить, что реализация кибертерроризма возможна за счет посягательства на информационные объекты государства, вербовку и склонения лиц к совершению преступлений террористического характера, а также призывы к осуществлению террористической деятельности и пропаганду (оправдание) идеологии терроризма через информационно-телекоммуникационные сети, включая сеть «Интернет», что в целом соответствует положениям о формах террористической деятельности, закрепленной в ст. 3 ФЗ «О противодействии терроризму».

В Уголовном кодексе РФ кибертерроризм в чистом виде не встречается вообще. Однако, можно обозначить две группы преступлений, которые могут рассматриваться как формы осуществления кибертеррористической деятельности.

К первой группе относятся преступления, включающиеся в себя деяния, направленные на содействие и призывы к осуществлению террористической деятельности (ст. 205.1, ч. 2 ст. 205.2 УК РФ). В настоящее время указанные преступные деяния регламентируются соответствующими статьями УК РФ, однако следует отметить, что в ст. 205.1 УК отсутствует прямое указание на совершение преступления с помощью ИКТ. Во многом это объясняется позицией Верховного Суда РФ, который отмечал, что на квалификацию совершения действий, перечисленных в диспозиции статьи, не влияют, совершены ли они с помощью информационно-телекоммуникационных сетей или нет.

Вместе с тем, совершения действий, направленных на склонение, вербовку, иного вовлечения с применяем ИКТ обладают куда большей общественной опасностью. Это объясняется наличием возможности осуществления преступления дистанционно, т.е. без непосредственного контакта между субъектами, высокой анонимностью пользователей, а также широким воздействие на самые разные слои населения (молодежь, людей пенсионного возраста и др.), что

упрощает совершение преступления и осложняет работу по установлению лиц, совершающих данные деяния.

Активную деятельность по вербовке ведут террористические организации, используя цифровое пространство как площадку для размещения своих материалов, поиска социально уязвимых категорий граждан для их вовлечения в террористическую деятельность. Изучая просторы социальных сетей, сайтов, террористы просматривают множество профилей, аккаунтов, отбирая наиболее уязвимых людей. Нередко сами пользователи, сообщают всю необходимую информацию о себе и террористам остается только вовремя войти в круг общения. Главная цель вербовщика – вызвать у пользователя стойкий интерес к террористической идеологии, убедить в ее правоте и необходимости для разрешения общественно-политических и социальных проблем[1].

Еще в 2021 г. директор ФСБ А.В. Бортников обращал внимание на то, что в цифровой среде активно развивается широкая инфраструктура, целью которой выступает вербовка и привлечение новых сторонников терроризма[2].

В это связи предлагается изложить ст. 205.1 УК РФ путем добавления в ч. 2 квалифицирующего признака, изложив ее в следующей редакции: «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». Данное законодательное дополнение позволит отравить всю степень общественной опасности применение ИТК для склонения, вербовки и вовлечения лиц для совершения террористических преступлений.

Как справедливо указывал Н.А. Бондаренко, ко второй группе следует причислить преступные деяния, направленные на посягательство критически важных информационных ресурсов государства[3]. Речь идет о совершении кибертерактов, прямое указание на которые в УК РФ отсутствует.

---

[1] Шумилова М. А. О вовлечении молодежи в деятельность террористических организаций через сеть «Интернет» / М. А. Шумилова // Евразийская адвокатура. – 2023. – № 1(60). – С. 85-89.

[2] Выступление директора Федеральной службы безопасности Российской Федерации Александра Бортникова на IX Московской конференции по международной безопасности [Электронный ресурс]. URL: https://mil.ru/ mcis/news/more.htm?id=12369152@cmsArticle

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

Несмотря на наличие в УК РФ специальной главы 28, посвященной преступлениям в сфере компьютерной информации, ни одна из статей (ст. ст. 272 – 274.2 УК РФ) не содержит положений, указывающих на признаки кибертерроризма или даже на совершение компьютерных преступлений с террористическими целями. Также отсутствует данный признак и в ст. 205 УК РФ. В условиях реального осуществления с помощью различных вирусов, DDoS-атак, фишинга и т.п. на информационные объекты государства, неурегулированность вопроса совершения кибертеракторов выступает пробелом.

Ряд авторов для решения данной проблемы предлагают дополнить статьи 273 или 274.1 УК РФ специальными квалифицирующими признаками[1]. Однако осуществление данного подхода видится проблематичным, т.к. при его реализации может возникнуть сложность с определением родового объекта уголовно-правовой охраны. Ведь террористические кибератаки напрямую посягают на общественную безопасность, а не на компьютерную информация, выступающей инструментом для реализации террористических намерений, т.е. как факультативный объекта.

Более целесообразным подходом к преодолению указанной проблемы представляется добавление квалифицирующего признака в ст. 205 УК РФ. Это во многом будет соответствовать и сущности кибертератка, который заключается в незаконных действиях, направленных на умышленное влияние на информационную систему, чтобы оказать воздействие на органы государственной власти[2]. Такая конструкция нормы способствовать эффективной защите от террористических киберугроз и возможности привлечению к уголовной ответственности лиц, совершающих посягательства на информационную инфраструктуру государства разными методами.

[1] Капитонова Е.А. Современный терроризм : моногр. / Е. А. Капитонова, Г. Б. Романовский. – М. : Юрлитинформ, 2015. 216 с.
[2] Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. М.: ЮИ МВД РФ, 2003. 66 с.

В современном мире кибертерроризм представляет собой значительную угрозу для информационной безопасности и стабильности Российской Федерации. Предложенный комплекс правовых мер позволит успешно справляться с теми вызовами, которые стоят пред нашим государством в цифровом пространстве.

Список литературы

1. Арипшев А. М. Кибертерроризм: проблемы в понимании и способах противодействия // Журнал прикладных исследований. 2023. № 4. С. 109-112.

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

3. 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. Федеральное государственное казенное образовательное учреждение высшего образования «Университет прокуратуры Российской Федерации», 2021. – С. 118-122.

4. Капитонова Е.А. Современный терроризм : моногр. / Е. А. Капитонова, Г. Б. Романовский. – М. : Юрлитинформ, 2015. 216 с.

5. 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.

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

7. Шумилова М. А. О вовлечении молодежи в деятельность террористических организаций через сеть «Интернет» / М. А. Шумилова // Евразийская адвокатура. – 2023. – № 1(60). – С. 85-89.