Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра уголовного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему: «Уголовная ответственность за совершение кибертерроризма»

Выполнила: Габдрахманова Рамиля Ильшатовна,
40.05.02 – «Правоохранительная деятельность»,
год набора – 2017 г., 071 группа

Руководитель: кандидат юридических наук,
доцент, доцент кафедры
уголовного права , майор полиции
Амирова Диляра Кафилевна

Рецензент: начальник отделения по раскрытию
преступлений, совершенных с использованием
информационно-телекоммуникационных
технологий
ОУР Управления МВД России по г. Казани,
капитан полиции.
Алиев Валех Мубаризович

Дата защиты: «___» _____ 20___ г. Оценка _____

Казань 2022

СОДЕРЖАНИЕ

ВЕДЕНИЕ

Актуальность темы работы. Процесс информатизации общества, внедрение высоких технологий практически в каждую сферу общественной жизни стало благоприятным условием для возникновения новых способов совершения преступных деяний, когда достижения современной (информационной) науки и техники используются в целях достижения преступного результата. На данный момент можно наблюдать постепенное изменение характера преступности, что выражается в увеличении количества преступников, специализирующихся на преступлениях, совершаемых с использованием высоких технологий. Это, в первую очередь, преступления имущественного характера, в частности, дистанционное мошенничество, преступления, связанные с незаконным оборотом запрещенных предметов (оружие, боеприпасы) и веществ (наркотические средства и психотропные вещества), и т.д. Иными словами, преступность уходит в глобальную информационную среду, в так называемое «киберпространство».

В настоящее время современное информационное пространство подвергается различным угрозам. Состояние его защищенности следует рассматривать как неотъемлемый элемент системы обеспечения национальной безопасности. Поэтому одним из актуальных вопросов современной науки является киберпреступность. Многие ученые – специалисты в различных областях знаний, в частности в юриспруденции, занимаются исследованием сущности данного явления, выявлением причин и условий, способствующих его возникновению, разработкой мер, направленных на противодействие киберпреступности.

Киберпреступность представляет собой совокупность преступлений, совершаемых в информационном пространстве с использованием современных компьютерных технологий. Следует отметить, что киберпреступность является относительно новым явлением, поэтому и деятельность по противодействию киберпреступности на данный момент не характеризуется высокой степенью

эффективности. Так, согласно мнению руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий Следственного комитета (СК) России Константина Комарда, «сегодня каждое седьмое преступление в России совершается с помощью информационных технологий или в киберпространстве». Комарда пояснил, что «в борьбе с киберугрозами не достаточно использовать традиционные методы расследования. Преступники тщательно заметают следы и применяют методы цифровой конспирации, что осложняет доказательство их вины».

Наиболее опасной разновидностью киберпреступности является кибертерроризм, уголовно-правовые особенности которого подлежат исследованию в рамках данной работы. Кибертерроризм, согласно общедоступной интернет-энциклопедии «Википедия», представляет собой «использование Интернета для совершения насильственных действий, которые приводят или угрожают гибелью людей или значительным телесным повреждением, с целью достижения политических или идеологических выгод путем угроз или запугивания».[1]

Изучение кибертерроризма, как и киберпреступности в целом, является актуальным направлением и в уголовно-правовой науке, цель которой заключается в совершенствовании уголовного законодательства в сфере борьбы с киберпреступлениями (кибертерроризмом). Данная цель может быть достигнута путем определения уголовно-правовой природы кибертерроризма, закрепления в действующем Уголовном законе[2] норм, предусматривающих ответственность за совершение исследуемого вида киберпреступлений.

Разработанность темы выпускной квалификационной работы. Проблемы исследования уголовно ответственности за совершение кибертерроризма К.И., Васильева, Е.Н. Молодчей, Е.А. Капитоновой, А.А. Паненкова, Е.В. Старостиной, М.И. Шамова и др. Однако большинство исследований

[1] Кибертерроризм [Электронный ресурс]: Википедия. Свободная энциклопедия. – Режим доступа: https://en.wikipedia.org/wiki/Cyberterrorism (дата обращения: 03.04.2022).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.03.2022) // СПС «Консультант плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (Дата обраэения 01.04.2022).

посвящено анализу информационного общества, пределов информационной свободы, правовых, социально-экономических и научно-технических аспектов обеспечения национальной безопасности и антитеррористической деятельности. Комплексных исследований, посвященных уголовной ответственности за совершение кибертерроризма, нет. Можно выделить несколько диссертационных и иных исследований, изучающих проблемы уголовно-правовых мер борьбы с кибертерроризмом, например диссертационное исследование Д А. Зыкова[1], Т.П Кесареевой[2], В.С. Карпова[3], С.Г. Спириной[4], Т.Л. Тропиной[5], А.Л. Осипенко[6], С.И. Ушакова[7] и др .

Указанные исследования, безусловно, внесли вклад в изучение компьютерной преступности в рамках Уголовного кодекса РФ, однако проблема именно кибертерроризма (т.е. преступности не только компьютерной, но и любой, связанной с использованием компьютеров) комплексно и в общемировом масштабе в них не поднималась.

Таким образом, изучение проблемы уголовно-правовой ответственности за совершение кибертерроризма является актуальным, своевременным и необходимым для теории и практики уголовного права.

---

[1] Зыков, Д. А. Виктимологические аспекты предупреждения компьютерного мошенничества : специальность 12.00.08 "Уголовное право и криминология; уголовно-исполнительное право" : диссертация на соискание ученой степени кандидата юридических наук / Зыков Даниил Алексеевич. – Владимир, 2002. – 211 с.

[2] Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : автореферат дис. ... кандидата юридических наук : 12.00.08 / Науч.-исслед. ин-т проблем укрепления законности и правопорядка при Генер. прокуратуре РФ. - Москва, 2002. - 25 с.

[3] Карпов В.С. Уголовная ответственность за преступления в сфере компь-ютерной информации: автореферат дис. ... кандидата юридических наук : 12.00.08 / Краснояр. гос. ун-т. - Красноярск, 2002. - 27 с.

[4] Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации. Автореф. дис. канд. юрид. наук. Волгоград, 2001. - 24 с.

[5] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы // Автореферат на соискание ученой степени к.ю.н., Владивосток — 2005. - 26 с.

[6] Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт / А.Л. Осипенко. — М.: Норма, 2004. – 432 с.

[7] Ушаков С.И. Преступления в сфере обращения компьютерной информации : Теория, законодательство, практика : автореферат дис. ... кандидата юридических наук : 12.00.08 / Кисловод. ин-т экономики и права. - Ростов-на-Дону, 2000. - 30 с.

Цель дипломной работы заключается в комплексном исследовании особенностей кибертерроризма как уголовно-правового явления, а также вопросов уголовной ответственности и наказания за его совершение.

Задачи работы:

1. Сформулировать понятие, выявить сущность кибертерроризма, определить его формы.

2. Выявить признаки кибертерроризма, отличающие его от традиционного террористического акта;

2. Установить причины возникновения и условия функционирования кибертерроризма;

3.Определить особенности юридической конструкции составов преступлений, предусматривающих ответственность за совершение кибертерроризма;

4. Провести анализ санкций статей, предусматривающих ответственность за кибертерроризм, определить виды наказаний, предусмотренные за их совершение;

5. Проанализировать практику назначения наказания за совершение кибертерроризма в практике судов Российской Федерации;

6. Выявить пути совершенствования законодательной системы в противодействии кибертерроризму в России;

7. Сформулировать выводы и предложения по теме выпускной квалификационной работы.

Объектом исследования являются общественные отношения, возникающие в связи с привлечением к уголовной ответственности за совершение кибертерроризма и применением мер противодействия данным видам преступлений.

В качестве предмета исследования выступают нормы права, закрепленные в действующем Уголовном законе, предусматривающие ответственность за совершение кибертеррористических деяний, в иных нормативных правовых актах, теоретические исследования отечественных и

зарубежных ученых в области противодействия кибертерроризму, материалы судебной практики.

Теоретическая основа исследования. При написании работы использованы труды отечественных и зарубежных ученых, исследовавших проблемы ответственности за терроризм и его различные проявления, в том числе освещавших вопросы кибертерроризма. Среди них такие, как: как Т.Л. Торопина, В.П. Журавель, Е.Н. Малик, А.В. Огородник, В.Ф. Джафарли, П.А. Ивлиева и др.

Методологическая основа исследования представлена общенаучными методами познания, с помощью которых проведено исследование: диалектический метод, методы системного и сравнительного анализа. Использовались также такие частные научные методы, как формально-юридический, сравнительно-правовой, историко-правовой, которые позволили рассмотреть явления в их взаимосвязи и взаимообусловленности.

Эмпирической основой исследования являлись различные статистические банки и сборники соответствующих подразделений правоохранительных органов, официально опубликованные материалы судебно-следственной практики, а также собственные наблюдения и практический опыт, полученный во время прохождения производственной (в том числе преддипломной) практики.

Научная и практическая значимость исследования заключается в том, что результаты исследования могут быть использованы в образовательном процессе, при изучении проблем уголовной ответственности за кибертерроризм и его профилактики, в работе следственных и судебных органов.

Новизна исследования заключается в том, что впервые предпринята попытка комплексного исследования вопросов уголовной ответственности за кибертерроризм, а также сформулированных автором предложений по совершенствованию уголовного законодательства, предусматривающего ответственность за кибертерроризм и практики его применения, а также вопросов профилактики этого преступления. В частности автор предлагает

новую законодательную редакцию ст. 205 УК РФ, а также введение новой статьи в текст УК РФ - 207, предусматривающей ответственность за кибертерроризм.

Апробация результатов исследования. Результаты дипломной работы получили апробацию в научных статьях, выступлениях автора на всероссийских, межвузовских научно-практических конференциях, круглых столах, конкурсах, научном кружке «Российское уголовное право: традиции и перспективы» кафедры уголовного права КЮИ МВД России, проводимых КЮИ МВД России и другими образовательными организациями.

Научные статьи.

1. Габдрахманова Р.И. Особенности кибертерроризма – новой разновидности террористического акта, совершаемого бесконтактным способом / Амирова Д.К., Габдрахманова Р.И. // Сборник научных трудов Всероссийской научно-практической конференции. – Казань: КЮИ МВД России, 26-27 марта 2019. С. 57-59.

2. Габдрахманова Р.И. Кибертерроризм как современная угроза безопасности граждан / Амирова Д.К., Габдрахманова Р.И. // Ученые записки КЮИ МВД России, Том 6 № 2 (12). Казань. 2021. С. 126-130.

Участие в конференциях, круглых столах.

1. Всероссийская научно-практическая конференция аспирантов и студентов ВУЗов России, адъюнктов, курсантов и слушателей образовательных организаций МВД России «Теория и практика противодействия преступности уголовно-правовыми средствами» (как второй этап конкурса в виде защиты научных работ, вышедших в финал), 20.05.2021 г., в режиме онлайн.

2. Межвузовская научно-практическая конференция «Уголовное и уголовно-исполнительное законодательство: вчера, сегодня, завтра», 29.03.2022 г., в режиме онлайн.

3. Всероссийский круглый стол «Дистанционные хищения и кибербезопасность», 26.03.2022 г.

4. Межкафедральный круглый стол с курсантами и слушателями на тему: «Уголовное право и современные информационные технологии», 04.06.2021 г.

Структура работы состоит из: оглавления, введения, основной части, которая состоит из 3-х глав, поделенных на параграфы, заключения, списка литературы.

ГЛАВА 1. КИБЕРТЕРРОРИЗМ КАК НОВАЯ ГЛОБАЛЬНАЯ УГРОЗА В РОССИИ И ЗАРУБЕЖОМ

§1.1. Понятие, сущность и формы кибертерроризма

В настоящее время ни в действующем уголовном законодательстве, ни в иных нормативных правовых актах определение понятия «кибертерроризм» не содержится. По нашему мнению, правильная теоретическая интерпретация кибертерроризма обеспечит эффективную реализацию мер уголовной ответственности, а также позволит выработать адекватные меры противодействия ему и эффективно использовать уже имеющиеся средства.

В науке уголовного права существуют следующие подходы к формулировке понятия и изучению сущности кибертерроризма.

Так, по мнению Е.Э. Турутиной, «кибертерроризм – это явление, выражающееся в действиях, произведенных с помощью средств сети Интернет, направленных против интересов страны, деструкции общества, подрыва и дискредитации органов власти по идеологическим или иным убеждениям».[1]

[1] Турутина Е. Э. Угроза кибертерроризма: пути противодействия / Е. Э. Турутина // Вестник Российского университета кооперации. – 2021. – № 4(46). С. 171..

Тропина Т.Л. дает следующее определение понятию «кибертерроризм: «это преднамеренная, мотивированная атака на информацию, которая находится, хранится и обрабатывается компьютером, компьютерную систему и сети, которая создает опасность для самой жизни или здоровья людей, или влечет за собой наступление других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта».[1]

Журавель В.П. рассматривает кибертерроризм как «экстремистские атаки на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, которые совершаются определенными лицами или группами»[2]

Малик Е.Н. рассматривает кибертерроризм как «комплекс противозаконных действий в информационном пространстве, представляющих собой атаки на компьютерные и телекоммуникационные технологии, направленные на создание угрозы международной и государственной безопасности с целью влияния на решение политических, экономических и иных задач»[3]

По мнению Е.М. Геворгян, «исходя из системного толкования, кибертерроризм можно определить как разновидность идеологии насилия и практики воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий в киберпространстве».[4]

Наиболее правильным, на наш взгляд, следует признать теоретический подход к определению сущности кибертерроризма, которого придерживаются Р.И. Дремлюга, А.И. Коробеев, А.В. Федоров: «под кибертерроризмом

---

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы // Автореферат на соискание ученой степени к.ю.н., Владивосток — 2005. С. 10-11.
[2] Журавель В. П. Зарубежное военное обозрение. - 2018. №5. С. 12.
[3] Малик Е. Н. Кибертерроризм как мировая угроза: вызовы и меры борьбы // Вестник Прикамского социального института. 2020. № 1 (85). С. 170.
[4] Геворгян Е. М. Кибертерроризм как угроза информационной безопасности Российской Федерации / Е. М. Геворгян // Скиф. Вопросы студенческой науки. – 2021. – № 6(58). С. 121.

(терроризмом в Интернете) понимается, во-первых, совершение терактов посредством информационных сетей, когда Интернет выступает как способ и средство совершения преступления, и, во-вторых, деятельность, способствующая терроризму, например вербовка в террористические организации, сбор средств для террористов или организация взаимодействия между членами террористических групп».[1]

Изучением сущности кибертерроризма занимались и иностранные ученые.

Так, определение М. Поллитта складывается из двух компонентов: киберпространства и терроризма. Под киберпространством подразумевается «место, где функционируют компьютерные программы и перемещаются данные»[2]. В отсутствие общепринятого понятия терроризма М. Поллитт взял за основу определение, выработанное Государственным департаментом США: «Терроризм – это преднамеренное, политически мотивированное насилие в отношении некомбатантов со стороны субнациональных группировок или подпольно действующих агентов».

В 2000 г. профессор Джорджтаунского университета Д. Дэннинг расширила понятие и определила кибертерроризм как «противозаконные атаки или угрозы атак на компьютеры, сети и хранимую в них информацию для устрашения или принуждения правительства или граждан к какому-либо действию в политических или общественных целях».[3] Позднее профессор уточнила, что актами кибертерроризма могут считаться только те атаки, которые результируют в насилие против людей или собственности, либо наносят урон, достаточный для порождения страха. В качестве примеров –

---

[1] Дремлюга Роман Игоревич, Коробеев Александр Иванович, & Федоров Александр Вячеславович (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. Всероссийский криминологический журнал, 11 (3). С. 609-610.

[2] Pollitt M. Cyberterrorism: Fact or Fancy? // Computer Fraud and Security [Электронный ресурс]. 1998. No. 2. P. 8–10. URL: https://doi.org/10.1016/S1361-3723(00)87009-8 (дата обращения 04.05.2022).

[3] Denning D.E. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives [Электронный ресурс]. 2000. May 23. P. 1. URL: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf (дата обращения: 01.04.2022).

атаки, которые приводят к гибели людей, взрывам, авиакрушениям, заражению воды и др.

Петер Грабоски определяет кибертерроризм как «незаконные атаки на компьютеры, сети и хранящуюся в них информацию, когда они совершаются с целью запугивания или принуждения правительства или его народа к достижению политических или социальных целей».[1]

Таким образом, большинство ученых, и отечественные, и зарубежные, определяя сущность кибертерроризма, указывают на то, что данный вид киберпреступлений: (дата обращения 04.05.2022).

1) совершается в информационном пространстве;

2) в качестве средства достижения преступного результата выступает, прежде всего, информация;

3) преследует такие цели, как создание опасности для жизни или здоровья людей, деструкция общества, провокация военного конфликта, нарушение общественной безопасности и т.д.

На основе вышеназванных определений можно выделить признаки, отличающие кибертерроризм от традиционного терроризма.

Главное отличие кибертерроризма от терроризма заключается в том, что местом совершения данной разновидности киберпреступлений является виртуальное, информационное пространство - киберпространство.

Понятие киберпространства тесно связано с понятием «информационнаябезопасность». Ученые по-разному подходят к определению этого понятия. Так, Р.М Юсупов пишет, что информационная безопасность может быть определена как состояние, в котором субъекту не может быть нанесен существенный ущерб путем воздействия на его информационную сферу[2].

---

[1] Grabosky P. (2017) Cyberterrorism, Cybercrime and the State. Available at: http://ilearn.mq.edu.au/pluginfile.php/4663825/mod_resource/content/1/Slides.pdf (дата обращения 02.04.2022).

[2] Юсупов, Р. М. Информационное обеспечение национальной безопасности // Национальная безопасность. 2010. № 7/8. С. 65-66.

Расторгуев С. П. указывает, что информационная безопасность, являясь составляющей национальной безопасности, имеет два направления: безопасность информации (защита информации) и безопасность от информации (защита от «опасной» информации). При этом оба этих направления реализуются как в технической, так и в гуманитарной сферах[1]. «Очевидно, - отмечает К.И. Васильев, - что определенный дуализм мнений по поводу понятия кибертерроризма существует в отношении его отдельных признаков»[2]. Различаются техническая и гуманитарная сферы, на которую воздействуют кибертеррористы.

Следует отметить, что в виртуальном пространстве выполняется как объективная сторона кибертерроризма в виде атак на информацию, так и приготовление к террористическим актам, например, распространение соответствующей идеологии, вербовка, планирование и организация терактов, финансирование терроризма и т.д. Тогда как традиционный терроризм осуществляется в материальном мире и подразумевает оказание физического воздействия, объектом которого является население (лишение жизни, причинение вреда здоровью и др.) либо материального воздействия (взрывы, поджоги т.д.).

Если при кибертерроризме имеет место посягательство на информационную безопасность государства, то при терроризме объектом террористических действий могут выступать здания, сооружения (метрополитен, образовательное учреждение и т.д.).

Помимо этого, преступный результат при совершении кибертерроризма достигается путем использования информационного оружия, тогда как орудием преступления при терроризме выступают взрывчатые вещества, огнестрельное оружие и т.д., то есть объекты материального мира. Результатом применения

---

[1] Расторгуев С. П. Основы информационной безопасности / Учеб. пособие для студ. высших учебных заведений. — М.: Издательский центр «Академия», 2009. С. 48.

[2] Васильев К.И К вопросу о понятии «кибертерроризм» в российской науке // Молодой учёный. № 17 (97) . С. 337.

информационного оружия может стать блокирование, подмена либо искажение информации.

По мнению А.В. Огородника, «из-за высокого уровня развития техники террорист посредством подключенного к Интернету компьютера может нанести больший вред, чем различные взрывные устройства. Новые гаджеты рассматриваются преступниками, как средство для достижения целей, которые противоречат общепринятым морально-этическим нормам».[1]

Следует отметить, что возможности информационного оружия значительно шире, чем у взрывчатых веществ, огнестрельного оружия, используемых в террористических актах. Так, информационное оружие позволяет:

– получить несанкционированный доступ к личной, коммерческой, банковской информации, к государственным и военным секретам;

– нанести ущерб физическим элементам информационного пространства (например, создание помех, нарушение работы сетей электропитания, использование специальных программ, которые разрушают аппаратные средства);

– уничтожить информацию, программное обеспечение, технические ресурсы путем внедрения вирусов, программных закладок, преодолеть систему защиты;

– осуществить техническое внедрение в каналы трансляции средств массовой информации с целью распространения слухов, дезинформации, объявления требований террористической организации;

– уничтожить или подавить работы линий связи, перегрузить узлы коммуникации, изменить адресации запросов в сети Интернет;

– провести информационно-психологические операции, воздействующих на сознание населения и др.

---

[1] Огородник А. В. История возникновения кибертерроризма: от киберпреступности до кибертерроризма / А. В. Огородник // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: Материалы VI Международной научной конференции, Донецк, 26–28 октября 2021 года / Под общей редакцией С.В. Беспаловой. – Донецк: Донецкий национальный университет, 2021. С. 147.

Согласно мнению ряда отечественных исследователей, для определения понятия «кибертерроризм» необходимо выполнение условий диспозиции ч. 1 ст. 205 УК РФ. Поэтому, исходя из целей терроризма, сформулированных в диспозиции ч. 1 ст. 205 УК РФ, можно согласиться с мнением В. А. Голубева, который отмечает, что кибертерроризм также имеет цель запугивания населения и органов власти, с целью достижения преступных намерений[1]. Это, в частности, проявляется в угрозе насилия, поддержания состояния постоянного страха с целью достижения определенных политических или иных целей, принуждения к определенным действиям, привлечения внимания к личности кибертеррориста или террористической организации, которую он представляет.

В науке существует позиция, согласно которой кибертерроризм рассматривается как синоним компьютерных преступлений. Данный подход акцентирует внимание на технической составляющей кибертерроризма - его воздействии на телекоммуникационные, компьютерные системы и средства связи, обращается внимание на то, что кибертерроризм направлен на использование сетевых инструментов для вывода из строя критически важных компонентов национальной инфраструктуры[2]. Соответственно, под термином «кибертеракт» или «кибератака» понимаются действия по дезорганизации информационных систем, устрашающие население и создающие опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях[3]. Действительно, часто для достижения своих целей кибертеррористы используют специальное

[1] Голубев В. А. Кибертерроризм — понятие, терминология, противодействие // Сайт Саратовского Центра по исследованию проблем организованной преступности и коррупции [Электронный ресурс]. — URL: http://sartraccc. ru/i.php?oper=read_file&filename=Pub/golubev (17–03–05).htm (дата обращения 20.04.2022).

[2]Пахарева Е. Н. Кибертерроризм как технология воздействия на молодежную среду: причины и пути минимизации // Ученые записки. 2009. № 4. С. 78.

[3] Батуева Е. В. Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая // Вестник МГИМО Университета. 2014. № 3. С. 130.

программное обеспечение, предназначенное для несанкционированного доступа, проникают в компьютерные системы и организуют удаленные атаки на информационные ресурсы интересующего их объекта (жертвы). Это могут быть компьютерные программные закладки и вирусы, в том числе сетевые, осуществляющие съем, модификацию или уничтожение информации, так называемые «логические бомбы», троянские программы и иные виды информационного оружия[1].

Таким образом, кибертерроризм от традиционного терроризма отличается, прежде всего, признаками объективной стороны:

1. Характер действий, направленных на достижение преступного результата. При кибертерроризме – это атаки на информацию, в традиционном терроризме – взрыв, поджог, иные действия, устрашающие население.

2. Место совершения преступного деяния. Кибертерроризм совершается в информационной среде, тогда как местом совершения террористических актов выступает материальный мир.

3. Орудие, средства, используемые для достижения преступного результата. Кибертерроризм совершается путем использования информационного оружия. Преступные цели в традиционном терроризме достигаются, как правило, с помощью взрывчатых веществ, огнестрельного оружия и других механических устройств.

В науке выделяют следующие формы киберторризма:

1) нанесение ущерба отдельным физическим элементам информационного пространства, например, разрушение сетей электропитания, создание помех, использование специальных программ, стимулирующих разрушение аппаратных средств;

2) кража или уничтожение информации, программ и технических ресурсов путем преодоления систем защиты, внедрения вирусов, программных закладок и т. п.;

---

[1] Васильева А. Н. Понятие и проблемы противодействия кибертерроризму // Успехи современного естествознания. 2011. № 8. С. 232–233.

3) воздействие на программное обеспечение и информацию;

4) раскрытие и угроза публикации закрытой информации;

5) захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

6) уничтожение или активное подавление линий связи, неправильная адресация, перегрузка узлов коммуникации;

7) проведение информационно-психологических операций и т. п. Эти приемы постоянно совершенствуются в зависимости от средств защиты, применяемых разработчиками компьютерных сетей[1].

§1.2. Причины возникновения и условия функционирования кибертерроризма в XXI веке

В настоящее время существует комплекс причин и условий, способствующих возникновению и развитию кибертерроризма.

Традиционно, при исследовании причин и условий возникновения того или иного вида преступлений, большинство авторов разделяют факторы на политические, социальные и экономические (общие причины и условия).[2]

Политические причины подразделяются на внешние и внутренние. К внешним причинам относятся глобализация, углубление разрыва между уровнями благосостояния различных стран, военная агрессия в отношении другого государства и его оккупация, усиление глобального цифрового противоборства и разрыв в уровне информационного развития стран, столкновение политических интересов различных государств.

---

[1] Иванов С. М., Томило О. Г. Международно-правовое регулирование борьбы с кибертерроризмом // Право и безопасность. 2013. № 3–4 (45). С. 83.

[2] Журавленко Н. И. Основные направления борьбы с угрозами кибертерроризма / Н. И. Журавленко, О. В. Тутова // Противодействие экстремизму и терроризму в крымском федеральном округе: проблемы теории и практики. – Крым: Краснодарский университет МВД России (Крымский филиал), 2015. С. 310.

Внутренними причинами являются политическая нестабильность и обострение политических конфликтов внутри государства, отсутствие механизмов взаимодействия государственной власти и гражданского общества, навязывание правящей элитой не свойственных для данного общества социально-политических реформ и иных нововведений, недовольство граждан страны деятельностью правительств иностранных государств; поощрение кибертерроризма руководством сраны, общественными организациями и в СМИ.

Среди социальных причин возникновения кибертерроризма можно выделить возросшую социальную дифференциацию в обществе, раскол его на группы с различным экономическим положением, заметное снижение качества жизненного уровня людей, слишком медленный процесс формирования среднего слоя общества. Экономические причины возникновения кибертерроризма включают в себя продолжающийся экономический и энергетический кризис, рост цен, инфляции и безработицы.

Помимо общих, можно выделить ряд частных причин, способствующих развитию кибертерроризма.

Так, кибертерроризм, как и многие другие преступные деяния, совершаемые в информационном пространстве, характеризуется анонимностью, когда отсутствует связь реальной личности с пользователем в Интернете. Как справедливо отмечает В.Ф. Джафарли, «анонимность делает киберпространство «параллельным» нашей обычной жизни и позволяет создавать новый образ собственной личности или сразу несколько образов, отличающихся от реального и не отягощенных психологической обязанностью следовать реальному образу, как это было бы в случае идентификации пользователя».[1]

Анонимность также не позволяет правоохранительным органам в полном объеме выявлять и раскрывать преступления, в том числе и террористической

[1] Джафарли В. Ф. Личность преступника в механизме преступлений, совершаемых в сфере информационных технологий / В. Ф. Джафарли. – Москва : Общество с ограниченной ответственностью "Издательство «КноРус», 2017. С. 54.

направленности, устанавливать всех участников преступных сообществ, террористических организаций, так как в таких условиях реальная связь между участниками отсутствует. Согласно мнению П.А. Ивлиева, «получая данные о пользователях, спецслужбы, борющиеся с реальной преступностью, узнают лишь о компьютере или сервере, с которого совершалось преступления или с которого преступник связывался с сообщниками. Но далеко не всегда принадлежность № человеку говорит о том, что этим IP пользуется только владелец. Мы не можем с точностью утверждать, что за каждым конкретным IP скрывается один человек. Тем более, что в цифровом пространстве существуют специальные методы анонимизации через использование поддельного или подставного IP. Для этого используются прокси-сервера, специальные браузеры (к примеру, TOR), расширения для обычных браузеров»[1]

Следующий фактор функционирования кибертерроризма связан с возможностью дистанционного осуществления кибертеррористических действий. Как известно, традиционный терроризм, представляющий собой совершение взрывов, поджогов и иных устрашающих население действий, требует от непосредственных исполнителей соответствующего уровня физической и моральной подготовки. Одним из факторов, вследствие которого лица не доводят преступление до конца, то есть имеет место добровольный отказ от преступления, является опасение расшифровки, задержания правоохранительными органами и последующего привлечения к уголовной ответственности. При кибертерроризме влияние данного фактора на преступника минимальное. Поэтому личность киберпреступника (кибертеррориста) значительно отличается от личности лица, совершающего преступления, которые не имеют прямого отношения к киберпреступности.

Особенности личности киберпреступника в своих исследованиях описывает А.А. Шапошников. Согласно мнению А.А. Шапошникова, «характеризуя личность преступника в сфере компьютерной информации,

[1] П. А. Ивлиев (2019). Анонимность в интернете: проблемы и особенности. Международный журнал гуманитарных и естественных наук, (4-2). С. 7.

следует отметить, что это далеко не всегда «высоколобый» интеллектуал. Он не стремится к «поглощению» больших объемов литературы, не отличается широтой взглядов. Не стремится он также и к благотворительности в форме бесплатного создания каких-либо программ, помимо вредоносных. Основным движущим мотивом чаще всего выступает тщеславие, которое проявляется достаточно противоречиво. С одной стороны, хакер не называет своего имени, так как боится ответственности за совершенное преступление. С другой — самим фактом его совершения он стремится лишний раз самоутвердиться, показать, что он превосходит других людей, выше их на голову, а то и на две. Наряду с этим мотивом совершения преступления может быть также и корысть»[1]

Причина распространения кибертерроризма состоит также в широком охвате практически неограниченной публики. Возможности современных информационно-телекоммуникационных систем позволяют кибертеррористам распространять свою идеологию в весьма короткие сроки для миллионов пользователей до момента идентификации такой информации со стороны правоохранительных органов и ее блокировке. Как справедливо отмечает С.С. Чепец, «главная цель террористов – привлечь как можно больше людей, транслировать свои идеи в общество насколько это возможно. А цифровые технологии и Интернет – идеальное поле для этого. Распространенными способами цифрового терроризма является хищение данных из баз, взлом и искусственная перегрузка сервисов, внедрение вирусов, захват каналов с целью транслирования своей информации. Примером может послужить прошлогодняя ситуация, суть которой состояла в массовой рассылке с зарубежного сервиса писем властям нескольких российских регионов с угрозами минирования государственных учреждений».[2]

---

[1] Шапошников Александр Александрович (2018). Криминологическая характеристика личности киберпреступника. Вестник юридического факультета Южного федерального университета, 5 (3-4). С. 59.

[2] Чепец, С. С. Кибертерроризм как одна из угроз современному миру / С. С. Чепец // Оригинальные исследования. – 2020. – Т. 10. – № 12. С. 20.

Успешное функционирование кибертерроризма, как и террористической деятельности в целом, невозможно без соответствующей финансовой поддержки. Финансирование кибертерроризма осуществляется со стороны лиц, имеющих политический, корыстный или иной интерес в достижении целей данных преступлений. И, если до революции в области информационных технологий, отслеживание таких финансовых операций не составляло особого труда для правоохранительных органов, в последнее время это является весьма трудоемким процессом. Анонимность таких операций привлекает крупные организации с обширными материальными ресурсами, криминальные группы и частные лица, и даже целые государства.

Финансирование и материальная поддержка международного терроризма из различных источников осуществляются с определенными целями. По мнению А.В. Серебренникова, «интерес транснациональных корпораций в финансировании кибертерроризма состоит в том, что таким способом они могут устранять конкурентов или производить изменения в инвестиционном климате государств, в юрисдикции которых они осуществляют свою деятельность».[1] Интерес отдельных государств в финансировании кибертерроризма сводится к решению определенных политических задач на глобальном и региональном уровнях. Кибертерроризм является инструментом для маскировки и легализации преступной деятельности для субъектов теневой экономики. Мотивы финансирования кибертерроризма со стороны частных лиц могут быть различными, однако они выполняют идеологическую функцию, путем поддержки и одобрения кибератак.

Исследования, проведенные в рамках данной главы, позволяют сделать следующие выводы о сущности кибертерроризма, отличительных признаках данного преступного деяния, а также о причинах и условиях, способствующих его возникновению и функционированию.

Кибертерроризм – это:

[1] Серебренникова А.В. (2021). Кибертерроризм: причины и условия. Colloquium-journal, (17 (104)). С. 49.

1) совершение терактов посредством информационных сетей, когда Интернет выступает как способ и средство совершения преступления;

2) деятельность, способствующая терроризму, например вербовка в террористические организации, сбор средств для террористов или организация взаимодействия между членами террористических групп.

От традиционного терроризма кибертерроризм отличается, в первую очередь, признаками объективной стороны:

1. Характер действий, направленных на достижение преступного результата. При кибертерроризме – это атаки на информацию, в традиционном терроризме – взрыв, поджог, иные действия, устрашающие население.

2. Место совершения преступного деяния. Кибертерроризм совершается в информационной среде, тогда как местом совершения террористических актов выступает материальный мир.

3. Орудие, средства, используемые для достижения преступного результата. Кибертерроризм совершается путем использования информационного оружия. Преступные цели в традиционном терроризме достигаются, как правило, с помощью взрывчатых веществ, огнестрельного оружия и других механических устройств.

На возникновение и развитие кибертеррористической деятельности оказывают влияние общие (политические, экономические и т.д.) и частные факторы – наличие неограниченных возможностей финансирования, анонимность, удаленность, многообразие преступных целей, широкий охват практически неограниченной публики.

ГЛАВА 2. УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ СОСТАВОВ СТАТЕЙ УК РФ, ПРЕДУСМАТРИВАЮЩИХ ОТВЕТСТВЕННОСТЬ ЗА СОВЕРШЕНИЕ КИБЕРТЕРРОРИЗМА РФ

§2.1. Юридический анализ объективных признаков составов кибертерроризма по УК РФ

Состав любого преступного деяния, в том числе и террористического акта, складывается из объективных (объект и объективная сторона) и субъективных признаков (субъект и субъективная сторона).

При квалификации преступлений устанавливается его объект – общественные отношения, взятые под охрану уголовным законодательством. В науке уголовного права общепринятым является классификация объектов преступных деяний «по горизонтали» и «по вертикали».

Классификация объектов «по вертикали» предусматривает выделение общего, родового, видового и непосредственного объектов преступных посягательств.

Общий объект преступления - это вся совокупность (система) общественных отношений, охраняемых государством посредством норм уголовного права.[1]

Значение общего объекта при квалификации того или иного деяния заключается в том, что он позволяет установить, нарушены ли общественные отношения вообще и в какой степени они нарушены, можно ли при наличии признаков состава преступления признать деяние преступным.

Необходимо отметить, что кибертерроризм является широким понятием, включает в себя признаки традиционного терроризма, предусмотренного ст. 205 Уголовного закона, а также некоторые признаки компьютерных преступлений, так как при его совершении осуществляется воздействие на компьютерную систему. Поэтому, в рамках данного исследования анализу подлежат объективные и субъективные признаки преступления, предусмотренного ст.205 УК РФ, и признаки преступлений в сфере компьютерной информации (ст. 272–274.1 УК РФ).

Статья 205 УК РФ закреплена в Разделе IX действующего Уголовного закона – «Преступления против общественной безопасности и общественного порядка». Родовой объект преступления, как правило, соответствует разделу

[1] Джинджолия Р.С., Боровиков В.Б. Российское уголовное право: в 2 ч. Общая часть: учеб.-наглядное пособие (схемы). - М.: Прометей, 2018. С.158.

УК РФ, в котором закреплено исследуемое преступное деяние, следовательно, в качестве родового объекта террористического акта выступают общественные отношения в сфере охраны общественного порядка и обеспечения общественной безопасности.

Видовой объект, в свою очередь, определяется главой Уголовного закона, в которой закреплена исследуемая норма. Видовым объектом преступления, предусмотренного ст.205 УК РФ, являются общественные отношения в области охраны общественного порядка (Глава 24. Преступления против общественной безопасности).

Непосредственным объектом, согласно мнению И.А. Харабара, признается тот конкретный вид общественных отношений, которому непосредственно причиняется вред от преступного деяния, или, еще говорят, то, на что направлено преступное посягательство.[1]

Следует согласиться с мнением А.С. Рогожевского о том, что «террористический акт является многообъектным преступным деянием ввиду того, что в результате его совершения наносится реальный вред жизни и здоровью неопределенного круга лиц, имущественного ущерба и т.д. В связи с этим наиболее верным решением является определение непосредственного объекта террористического акта в виде общественной безопасности».[2]

В своих исследованиях М.Г. Беляева указывает, что «непосредственным объектом ст. 205 УК РФ являются общественные отношения, связанные с поддержанием общественной безопасности в сфере повседневной жизнедеятельности, т.е. общественные отношения, обеспечивающие состояние защищенности жизненно важных интересов неопределенного круга лиц, организаций и иных материальных объектов от внутренних и внешних угроз».[3]

Квалификация объектов преступных посягательств по горизонтали предполагает определение основного, дополнительного и факультативного

---

[1] Харабара И.В. (2020). Объект преступления и его виды. Образование и право, (6). С. 321.

[2] Рогожевский А.С. (2021). Краткий анализ состава преступления, предусмотренного ст. 205 Уголовного кодекса Российской Федерации. Вестник магистратуры, (5-3 (116)). С. 36.

[3] Беляева М.Г. (2017). Анализ объекта преступления на примере состава преступления, предусмотренного ст. 205 УК РФ «террористический акт». Современные инновации, (7 (21)). С. 33.

объектов. Если основным непосредственным объектом является общественная безопасность, то в качестве дополнительного объекта террористического акта могут быть признаны жизнь и здоровье, собственность либо нормальное функционирование предприятий, учреждений, органов власти.

Объективная сторона террористического акта, согласно ч.1 ст.205 УК РФ, выражается в совершении взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий. Для определения сущности элементов объективной стороны исследуемого вида преступления следует обратиться к Постановлению Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».[1]

Так, согласно Постановлению Пленума Верховного Суда Российской Федерации № 1, устрашающими население могут быть признаны такие действия, которые по своему характеру способны вызвать страх у людей за свою жизнь и здоровье, безопасность близких, сохранность имущества и т.п.

Опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий должна быть реальной, что определяется в каждом конкретном случае с учетом места, времени, орудий, средств, способа совершения преступления и других обстоятельств дела (данных о количестве людей, находившихся в районе места взрыва, о мощности и поражающей способности использованного взрывного устройства и т.п.).

Законодатель, закрепив в диспозиции статьи 205 УК РФ понятие «иные действия», оставил перечень способов исследуемого вида преступления открытым. Под «иные действия» подпадают любые действия, если они сопоставимы с основными способами совершения террористических актов

[1] О некоторых вопросах судебной практики по уголовным делам о пре-ступлениях террористической направленности: постановление Пленума Верховного Суда РФ от 09.02.2012 № 1» [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 05.01.2022).

(взрыв, поджог). В качестве примера в Постановлении Пленума Верховного Суда Российской Федерации № 1 приводятся следующие «иные действия»:

1) устройство аварий на объектах жизнеобеспечения;

2) разрушение транспортных коммуникаций;

3) заражение источников питьевого водоснабжения и продуктов питания;

4) распространение болезнетворных микробов, способных вызвать эпидемию или эпизоотию;

5) радиоактивное, химическое, биологическое (бактериологическое) и иное заражение местности;

6) вооруженное нападение на населенные пункты, обстрелы жилых домов, школ, больниц, административных зданий, мест дислокации (расположения) военнослужащих или сотрудников правоохранительных органов;

7) захват и (или) разрушение зданий, вокзалов, портов, культурных или религиозных сооружений.

Следует отметить, что законодатель признает преступным также и угрозу совершения вышеназванных действий. В качестве способов выражения угрозы Постановление Пленума Верховного суда Российской Федерации № 1 закрепляет: устное высказывание, публикация в печати, распространение с использованием радио, телевидения или иных средств массовой информации, а также информационно-телекоммуникационных сетей.

Состав преступления является формально-усеченным. Так, согласно мнению А.С. Рогожевского, «разбив диспозицию данной статьи на составляющие можно увидеть, что состав в части совершения взрыва, поджога и иных действий можно расценивать как формальный, тогда как угроза совершения указанных действий представляется в виде усеченного состава».[1]

Далее необходимо определить объективные признаки преступлений в сфере компьютерной информации:

---

[1] Рогожевский А.С. (2021). Краткий анализ состава преступления, предусмотренного ст. 205 Уголовного кодекса Российской Федерации. Вестник магистратуры, (5-3 (116)). С. 37.

1. Неправомерный доступ к компьютерной информации (Статья 272).

2. Создание, использование и распространение вредоносных компьютерных программ (Статья 273).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (Статья 274).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (Статья 274.1).

Родовой объект исследуемых преступных деяний совпадает с родовым объектом террористического акта (общественные отношения в области обеспечения общественной безопасности и охраны общественного порядка).

В качестве видового объекта компьютерных преступлений выступают общественные отношения, которые складываются в сфере обеспечения конфиденциальности, целостности и доступности компьютерной информации, сохранности средств, используемых для её обработки.

Непосредственным объектом преступления, предусмотренного ст.272 являются отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями.

Предметом исследуемого преступления является охраняемая законом компьютерная информация.[1]

Сущность компьютерной информации как предмета преступных посягательств раскрывается в примечании к ст. 272 УК РФ: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Объективная сторона данного преступления складывается из:

[1] Харламова А.А. (2020). Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации. Вестник Уральского юридического института МВД России, (2). С. 165.

1) действий, состоящих в неправомерном доступе к охраняемой законом компьютерной информации;

2) общественно-опасных последствий в виде уничтожения, блокирования, модификации либо копирование компьютерной информации;

3) причинно-следственной связи между указанными действиями и последствиями.

Непосредственным объектом ст. 273 УК РФ являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации. Предмет данного преступления совпадает с предметом неправомерного доступа к компьютерной информации.

Статья 273 предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, которые образуют объективную сторону исследуемого преступления.

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Данный состав преступления является материальным, так как обязательным условием для привлечения лица к уголовной ответственности является наступление таких альтернативных общественно-опасных последствий, как уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Непосредственный объект ст. 274 УК РФ совпадает с непосредственным объектом ст. 273 УК РФ. Предметом исследуемого вида преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

Статьей 274.1 УК РФ УК РФ предусмотрена ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Критическая информационная инфраструктура, согласно Закону «О безопасности критической информационной инфраструктуры Российской Федерации» – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.[1]

Объекты критической информационной инфраструктуры, согласно вышеназванному законодательному акту, – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Неправомерное воздействие оказывается путем создания, распространения и (или) использование компьютерных программ либо иной компьютерной информации.

Создание компьютерных программ, как элемент объективной стороны преступных деяний, предусмотренных ст.273, ст.274.1 представляет собой действия, направленные на разработку, подготовку компьютерной программы, способствующей достижению преступных результатов, закрепленных в диспозициях ст.273, ст.274.1.

Распространение компьютерных программ предполагает предоставление доступа к ним любому постороннему лицу любым из возможных способов.

Использование программы - это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме.

§2.2. Юридический анализ субъективных признаков составов кибертерроризма по УК РФ

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г N 187 ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 14.03.2022).

Далее необходимо проанализировать субъективные признаки исследуемых видов преступлений.

Террористический акт характеризуется умышленной формой вины. Данное преступное деяния совершается с прямым умыслом – лицо осознает общественную опасность своих действий или бездействия, предвидит реальную возможность или неизбежность наступления общественно опасных последствий (интеллектуальный момент) своих действий или бездействия и желает их наступления.

Одним из важнейших элементов состава террористического акта, влияющего на квалификацию данного вида преступления, является его специфическая цель:

1) дестабилизация деятельности органов власти или международных организаций либо воздействие на принятие ими решений – в случае совершения взрыва, поджога, иных действий;

2) воздействие на принятие решений органами власти или международными организациями – при угрозе совершения вышеназванных действий. Некоторые авторы не согласны с данной формулировкой диспозиции статьи 205 УК РФ и считают, что решение законодателя при определении цели угрозы ограничиться лишь закреплением цели воздействия на принятие органами власти решений, и исключение цели дестабилизации деятельности соответствующих органов власти, является необоснованным.

Так, по мнению А.Н. Игнатова, «в современных реалиях вред, причиняемый человеку, обществу и государству, в частности и дестабилизация деятельности органов власти или международных организаций, связанные с вынужденным реагированием на угрозу совершения террористического акта, возрастает пропорционально инновационно-техническим развитием человечества и глобальным развитием информационного общества, а также возрастанием угрозы международного терроризма и ее субъективного восприятия как населением в целом, так и каждым отдельным человеком в частности. Каждое общество, столкнувшееся с террористической угрозой, в

нынешних условиях реальной опасности локального (местного) и тем более международного терроризма, воспринимает любое сообщение об акте терроризма как вредоносное (как по восприятию, так и фактически) и требующее безотлагательного реагирования, поскольку оно служит для него информационным сигналом о потенциальной опасности террористического насилия. Любое сообщение об акте терроризма нарушает нормальные условия и ритм жизни общества и государства, устрашает население, дезорганизовывает деятельность органов власти, в частности правоохранительных органов, государственных учреждений и организаций, нарушает нормальное функционирование объектов социальной инфраструктуры».[1]

Воздействие направлено на побуждение соответствующих органов власти к совершению определенных действий либо воздержанию от их совершения. Так, в 1995 году был совершен террористический акт в Будённовске. Террористами были выдвинуты требования российским властям: остановить военные действия в Чечне и вступить в переговоры с режимом Джохара Дудаева.[2]

Так, П. решил совершить террористический акт путем поджога образовательного учреждения. Наличие террористических целей было подтверждено следующими доказательствами.

Согласно показаниям свидетеля М., осужденный П. в ходе общения рассказал ей о том, что он хочет вступить в террористическую организацию, чтобы бороться с органами власти, желает уничтожить русское население, особенно детей.

Аналогичные показания дал свидетель Н. Виновный сообщил ему, что он намерен совершить террористический акт – массовое убийство детей путем поджога одного из образовательных учреждений в целях мести русскому населению за поддержку власти, ведущей войну против мусульман.

---

[1] Игнатов А.Н. Проблемы законодательной регламентации уголовной ответственности за преступления террористического характера // Вестник Московского университета МВД России. 2017. № 6. С. 100.

[2] Террористический акт в Будённовске - Энциклопедия России [Электронный ресурс]. – URL: https://encyclopaedia russia.ru/article/terroristicheskij-akt-v-budyonnovske/ (дата обращения 01.04.2022).

В отношении осужденного П. были проведены также оперативно-розыскные мероприятия, том числе прослушивания телефонных переговоров, результаты которых подтвердили преследование П. террористических целей.

Показания, данные свидетелями в ходе предварительного следствия, были подтверждены протоколами осмотра предмета - оптического диска, на котором содержатся записи телефонных разговоров между П. и М., П. и Н. содержание которых подтверждает показания последней относительно высказанного осужденным намерения совершить террористический акт путем поджога образовательного учреждения. [1]

Следует отметить, что диспозиция статьи 205 Уголовного закона обладает некоторыми недостатками в виде перегруженности оценочными понятиями. Например, к числу таких понятий относится понятие «устрашение». Взрыв, поджог, иные способы совершения террористического акта должны вызвать страх у населения. Однако в законодательстве критерии страха не закреплены, что может создать проблемы при квалификации исследуемого преступного деяния. Нельзя быть уверенным в том, что поджог, совершенный в террористических целях вызвал страх у проживающих на той или иной территории людей. Отсутствие доказательств, подтверждающих устрашающий характер террористических действий, приводит к переквалификации деяния, предусмотренного ст.205 УК РФ на менее тяжкий состав преступления. Согласно мнению Н.Б. Хлыстовой, «устрашение населения как цель или как последствие преступления является характерным для многих составов преступных деяний, особенно сопряженных с посягательством на жизнь, здоровье, половую свободу и неприкосновенность личности, и выделять этот признак именно для террористического акта вряд ли является правильным, поскольку на практике при квалификации создает больше спорных вопросов,

[1] Апелляционное определение Верховного Суда Российской Федерации от 14 ноября 2019 г. [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/uDVmWyNoFMZ4/ (дата обращения 04.03.2022).

которые, как известно, толкуются в пользу лица, совершившего преступление и создает возможность избежать справедливого наказания».[1]

Оценочным также является понятие «население». Действующие нормативные правовые акты не содержат определения вышеназванного понятия, не устанавливают его количественную характеристику. Поэтому нет однозначного ответа на вопрос: какое минимальное количество людей должно испытать чувство страха для квалификации взрыва, поджога, иных действий по ст.205 УК РФ.

Возможно, вышеназванные оценочные понятия на практике не оказывают существенного влияния на квалификацию преступных деяний по ст.205 УК РФ. Однако их наличие, сложность определения указывают на необходимость совершенствования действующего Уголовного закона. Закон не должен содержать оценочные понятия, однако если они имеются, то должны быть конкретизированы в данном законодательном акте либо в иных принимаемых в соответствии с ним нормативных правовых актах.

В качестве субъекта преступлений в сфере компьютерной информации выступает вменяемое физическое лицо, достигшее шестнадцатилетнего возраста. Иными словами, субъект – общий, за исключением некоторых квалифицированных состав компьютерных преступлений.

Субъективные признаки преступлений в сфере компьютерной информации не вызывают трудности в квалификации. Так, субъективная сторона состава преступлений, предусмотренных ст. 273, ст.274.1 УК РФ, характеризуется виной в виде прямого умысла. При этом виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к указанным в законе общественно опасным последствиям. Мотив и цель не влияют на квалификацию преступления.

---

[1] Хлыстова Н. Б. Террористический акт как угроза общественной безопасности / Н. Б. Хлыстова // Наука. Мысль: электронный периодический журнал. – 2017. – Т. 7. – № 3-1. С. 108.

Субъективная сторона ст. 272 УК РФ, в отличие от субъективной стороны составов предыдущих видов компьютерных преступлений, характеризуется виной в форме умысла (прямого или косвенного) или неосторожности.

Нарушение правил эксплуатации и доступа, предусмотренное ч. 1 ст. 274 УК РФ, может совершаться как умышленно (при этом умысел должен быть направлен на нарушение правил эксплуатации и доступа), так и по неосторожности (например, программист, работающий в больнице, поставил полученную им по сетям программу без предварительной проверки ее на наличие в ней компьютерного вируса, в результате чего произошел отказ в работе систем жизнеобеспечения реанимационного отделения больницы).

§2.3. Квалифицированные признаки кибертерроризма

Среди квалифицированных признаков террористического акта есть признаки, которые традиционно не вызывают трудности в квалификации. К таким признакам относятся:

- террористический акт, совершенный группой лиц по предварительному сговору или организованной группой (п. «а» ч.2 ст. 205);

- террористический акт, повлекший по неосторожности смерть человека (п. «б» ч.2 ст. 205);

- деяния, предусмотренные частями первой или второй статьи 205, сопряженные с посягательством на объекты использования атомной энергии либо с использованием ядерных материалов, радиоактивных веществ или источников радиоактивного излучения либо ядовитых, отравляющих, токсичных, опасных химических или биологических веществ (п. «а» ч.3 ст. 205), либо повлекшие умышленное причинение смерти человеку (п. «б» ч.3 ст. 205).

Некоторые квалифицированные признаки, в свою очередь, требуют разъяснений. Например, к таким признакам относится совершение

террористического акта, повлекшего причинение значительного имущественного ущерба либо наступление иных тяжких последствий.

Согласно Постановлению Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности», решая вопрос о том, является ли ущерб значительным, следует исходить из:

1) стоимости уничтоженного имущества или затрат на восстановление поврежденного имущества;

2) значимости этого имущества для потерпевшего, например в зависимости от рода его деятельности или материального положения

3) либо финансово-экономического состояния юридического лица, являвшегося собственником или иным владельцем уничтоженного либо поврежденного имущества.

Помимо значительного имущественного ущерба, п. «в» ст. 205 УК РФ в качестве квалифицированного признака предусматривает наступление иных тяжких последствий. В Постановлении Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» к иным тяжким последствиям отнесены:

- причинение тяжкого вреда здоровью хотя бы одному человеку;

- причинение средней тяжести вреда здоровью двум и более лицам;

- дезорганизация деятельности органов государственной власти и местного самоуправления;

- длительное нарушение работы предприятия (предприятий) и (или) учреждения (учреждений) независимо от их ведомственной принадлежности, формы собственности, организационно-правовой формы;

- существенное ухудшение экологической обстановки (например, деградация земель, загрязнение поверхностных и внутренних вод, атмосферы, морской среды и иные негативные изменения окружающей среды, препятствующие ее сохранению и правомерному использованию, устранение

последствий которых требует длительного времени и больших материальных затрат).

Таким образом, анализ квалифицированных признаков преступления, предусмотренного ст.205 УК РФ, позволяет сделать вывод о том, что законодатель не предусмотрел использование информационных технологий в качестве квалифицированного признака террористического акта.

В целях криминализации кибертеррористического акта предлагается дополнить статью 205 Уголовного закона следующим квалифицированным признаком.

«Статья 205 УК РФ. Террористический акт.

2. Те же деяния:

г) совершенные путем несанкционированного доступа в компьютерные системы или информационно-коммуникационные сети, осуществляющие автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения с целью нарушения их функционирования и создания аварийной ситуации и угрозы техногенной катастрофы.

наказываются лишением свободы на срок от десяти до пятнадцати лет».

Проблемы в правоприменительной деятельности могут возникнуть при определении некоторых квалифицированных признаков преступлений в сфере компьютерной информации.

Так, ч.4 ст.272 Уголовного закона предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло тяжкие последствия или создало угрозу их наступления. Наступление тяжких последствий или угроза их наступления также является элементом объективной стороны других компьютерных преступлений, предусмотренных ч. 3 273 УК РФ, ч.2 ст. 274 УК РФ, ч.5 ст.274.1 УК РФ.

Однако ни в Уголовном законе, ни в актах Верховного суда Российской Федерации не указано, какие последствия относятся к тяжким. Кроме того, на данный момент не разработан соответствующий Пленум Верховного суда, где

разъясняются вопросы квалификации преступлений в сфере компьютерной информации.

В ст. 272 указан размер крупного ущерба (превышает один миллион рублей), выступающего в качестве квалифицированного признака компьютерных преступлений.

К остальным квалифицированным признакам преступлений в сфере компьютерной информации, которые в отличие от вышеназванного признака не вызывают трудности в квалификации, относятся совершение компьютерных преступлений: группой лиц по предварительному сговору или организованной группой; из корыстной заинтересованности; с использованием служебного положения;

Исследования, проведенные в рамках данной главы, позволяют сделать следующие выводы.

Статья 205 действующего Уголовного закона предусматривает ответственность за совершение террористического акта. Исследуемое преступное деяние посягает на общественные отношения, связанные с поддержанием общественной безопасности в сфере повседневной жизнедеятельности, т.е. отношения, обеспечивающие состояние защищенности жизненно важных интересов неопределенного круга лиц, организаций и иных материальных объектов от внутренних и внешних угроз.

Объективная сторона террористического акта представляет собой совершение взрыва, поджога и иных действий, которые выступают в качестве способов совершения исследуемого вида преступления. Для квалификации указанных действий по ст.205 УК РФ необходимо, чтобы они были направлены на устрашение населения. Понятия «устрашение», «население», в свою очередь, являются оценочными понятиями.

В законодательстве критерии страха не закреплены, что может создать проблемы при квалификации исследуемого преступного деяния. Нельзя быть уверенным в том, что поджог, совершенный в террористических целях вызвал страх у проживающих на той или иной территории людей. Отсутствие

доказательств, подтверждающих устрашающий характер террористических действий, приводит к переквалификации деяния, предусмотренного ст.205 УК РФ на менее тяжкий состав преступления.

Действующие нормативные правовые акты не содержат определения понятия «население», не устанавливают его количественную характеристику. Поэтому нет однозначного ответа на вопрос: какое минимальное количество людей должно испытать чувство страха для квалификации взрыва, поджога, иных действий по ст.205 УК РФ.

Одним из важнейших элементов состава террористического акта, влияющего на квалификацию данного вида преступления, является его специфическая цель:

1) дестабилизация деятельности органов власти или международных организаций либо воздействие на принятие ими решений – в случае совершения взрыва, поджога, иных действий;

2) воздействие на принятие решений органами власти или международными организациями – при угрозе совершения вышеназванных действий. Некоторые авторы не согласны с данной формулировкой диспозиции статьи 205 УК РФ и считают, что решение законодателя при определении цели угрозы ограничиться лишь закреплением цели воздействия на принятие органами власти решений, и исключение цели дестабилизации деятельности соответствующих органов власти, является необоснованным.

Помимо статьи 205 УК РФ, были проанализированы объективные и субъективные признаки составов преступлений в сфере компьютерной информации, которых также можно отнести к категории кибертеррористических.

В качестве предмета указанных видов преступлений выступает компьютерная информация, определение которой дается в примечании к ст.272 Уголовного закона.

Преступления в сфере компьютерной информации чаще всего совершаются путем создания, распространения или использования

компьютерных программ, которые образуют их объективную сторону. Среди преступлений в сфере компьютерной информации встречаются как материальные составы (например, ч.1 ст. 272), требующие наступления общественно-опасных последствий, так и преступления с формальным составом, когда для признания деяния преступным достаточно совершения запрещенного Уголовным законом действия либо бездействия (ч.1 ст. 273).

Что касается субъективных признаков, то в качестве субъекта данных преступных деяний выступает вменяемое лицо, достигшее шестнадцатилетнего возраста. Субъективная сторона компьютерных преступлений характеризуется наличием как умышленных, так и неосторожных преступлений, тогда как террористический акт совершается умышленно.

ГЛАВА 3. ПУТИ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬНОЙ СИСТЕМЫ В ПРОТИВОДЕЙСТВИИ КИБЕРТЕРРОРИЗМУ В РОССИИ

§3.1. Назначение наказания за совершение кибертерроризма в практике судов Российской Федерации

Санкция ст. 205 действующего Уголовного закона предусматривает следующие виды и размеры наказаний за совершение данного преступного деяния:

1. Часть 1 статьи 205 – лишение свободы на срок от 10 до 15 лет. Указанный срок лишения свободы за совершение террористического акта был установлен в 2016 году путем принятия соответствующего федерального закона (№ 375-ФЗ)[1].

До принятия данного законодательного решения санкция ч.1 ст.205 УК РФ предусматривала наказание в виде лишения свободы от 8 до 15 лет (Закон от 09.12.2010 № 352-ФЗ)[2].

С момента закрепления террористического акта как уголовно-наказуемого деяния и до 2004 года санкция части 1 исследуемой статьи Уголовного закона устанавливала наказание в виде лишения свободы на срок от 5 до 10 лет. С 2004 года и до принятия Федерального закона от 09.12.2010 № 352-ФЗ ч.1 ст.205 предусматривала наказание в виде лишения свободы на срок от 8 до 12 лет.

Таким образом, отечественная уголовно-правовая политика направлена на ужесточение наказания за совершение террористического акта, что

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 06.07.2016 № 375-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 04.03.2022).

[2] О внесении изменений в Уголовный кодекс Российской Федерации: федеральный закон от 09.12.2010 № 352-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 03.02.2022).

выражается в увеличении нижнего и верхнего пределов уголовного наказания в виде лишения свободы.

2. Часть 2 статьи 205 – лишение свободы на срок от 12 до 20 лет с ограничением свободы на срок от 1 года до 2 лет. Федеральный закон от 06.07.2016 № 375-ФЗ увеличил нижний предел наказания за совершения террористического акта от 10 до 12 лет.

3. Часть 3 статьи 205 – лишение свободы на срок от пятнадцати до двадцати лет с ограничением свободы на срок от одного года до двух лет или пожизненным лишением свободы.

Следует отметить, что террористический акт (ст.205) в настоящее время является менее распространенным, чем преступные деяния, предусмотренные ст.ст.205.1 – 205.6 УК РФ. Согласно статистическим данным, предоставленным Судебным департаментом при Верховном Суде РФ, в 2021 году количество осужденных по ст.205 УК РФ составило 34. Тогда как по ст. 205.1 было осуждено 121 лицо, по ст.205.2 – 199 лиц. Количество осужденных по ст.205.3 УК РФ в 2021 году составило 5, по ст.205.4 – 30, по ст. 205.5 – 53. По ст. 205.6 были осуждены 104 лица.[1]

Количество осужденных за совершение террористического акта, предусмотренного ч.1-3 ст.205 УК РФ, а также срок назначенного наказания в виде лишения свободы, могут быть представлены в виде таблицы. (Таблица 1. Срок лишения свободы за совершение преступлений, предусмотренных ч.1-3 ст.205 УК РФ).

Таким образом, за совершение преступлений, предусмотренных ч.1-3 ст.205 УК РФ, чаще всего назначается наказание в виде лишения свободы сроком от 5 до 8 лет (см. приложение 1). Это связано с тем, что указанные преступные деяния не представляют собой оконченный состав преступления, то есть, имеет место приготовление либо покушение на террористический акт.

[1] Отчет о сроках лишения свободы за совершение преступления, предусмотренного ч.1-3 ст.205 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru (дата обращения 06.02.2022).

Согласно ст.66 УК РФ, срок или размер наказания за приготовление к преступлению не может превышать половины максимального срока или размера наиболее строгого вида наказания, за покушение – трех четвертей.

Таблица 1.

Срок лишения свободы за совершение преступлений, предусмотренных ч.1-3 ст.205 УК РФ

			Срок лишения свободы					
		Общее число осужденных	свыше 3 до 5 лет	свыше 5 до 8 лет	свыше 8 до 10 лет	свыше 10 до 15 лет	свыше 15 до 20 лет	Наказание ниже низшего предела
2017	205 ч. 1	4	1	1	0	2	0	0
	205 ч. 2	21	0	0	15	4	1	0
	205 ч. 3	3	0	0	0	2	1	0
2018	205 ч. 1	5	3	1	0	0	0	0
	205 ч. 2	17	0	11	4	2	0	0
	205 ч. 3	2	0	0	1	1	0	0
2019	205 ч. 1	9	1	5	1	1	0	0
	205 ч. 2	12	1	9	2	0	0	3
	205 ч. 3	2	0	0	1	1	0	0
2020	205 ч. 1	3	0	2	1	0	0	0
	205 ч. 2	10	1	5	0	3	1	0
	205 ч. 3	0	0	0	0	0	0	0
2021	205 ч. 1	5	2	2	0	1	0	1
	205 ч. 2	17	2	12	1	2	0	3
	205 ч. 3	11	0	0	0	8	3	0

Следует отметить, что исследуемый вид преступлений был распространен в 90-х, 2000-х гг. Так, в феврале 2006 года подсудимым Х. были совершены

следующие деяния, содержащие признаки преступления, предусмотренного ст. 205 УК РФ:

1. Террористический акт у зала игровых автоматов «Честная игра» (пп. «а», «в» ч.2 ст.205 УК РФ).

2. Террористический акт у зала игровых автоматов «Игросервис» (пп. «а», «в» ч.2 ст.205 УК РФ).

3. Террористический акт по подрыву ретранслятора «Мобиком-Кавказ» (пп. «а», «в» ч.2 ст.205 УК РФ).

4. Террористический акт на бирже труда (по пп. «а», «в» ч.2 ст.205 УК РФ).

За каждое из вышеназванных преступных деяний судом было назначено наказание в виде лишения свободы на срок 12 лет. Помимо указанных преступлений, Х. совершил также приготовление к террористическому акту на площади Штыба г. Владикавказа (ч.1 ст.30, пп. «а», «в» ч.2 ст.205 УК РФ), за которое был осужден к 8 годам лишения свободы. По совокупности преступлений, путём частичного сложения наказаний окончательно Х. назначено 22 года 10 месяцев лишения свободы.[1]

Как было отмечено ранее, деяние, предусмотренное статьей 205 УК РФ, в настоящее время относительно редко доводится до конца, то есть становится оконченным. Чаще всего имеет место покушение либо приготовление к террористическому акту.

О.С.И., Д.О.С, И.О.А были осуждены за приготовление к совершению террористического акта организованной группой. Указанные лица были сторонниками экстремистской организации «Артподготовка».[2] По заданию одного из руководителей экстремистской организации вышеуказанные лица изготовили 13 бутылок с воспламеняющейся жидкостью, так называемые

[1] Постановление Президиума Верховного Суда Российской Федерации от 2 марта 2022 г. о возобновлении производства по уголовному делу № 165-П21 ввиду новых обстоятельств [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/qJgnnYO1gpHc/ (дата обращения 04.03.2022).

[2] Московское дело 3 сторонников «Артподготовки» [Электронный ресурс] Правозащитный центр «Мемориал» URL: https://memohrc.org/ru/special-projects/moskovskoe-delo-3-storonnikov-artpodgotovki (дата обращения 04.03.2022).

«коктейли Молотова». Данные предметы следовало поместить в транспортное средство, которое необходимо было припарковать напротив здания Государственной Думы Российской Федерации. С помощью этих зажигательных средств планировалось осуществить 5 ноября 2017 г. поджог административных зданий, автомобилей в центре г. Москвы, что вызвало бы хаос и массовые беспорядки. Для достижения вышеназванной цели, помимо изготовления бутылок с воспламеняющейся жидкостью, осужденные совершили следующие действия, которые судом были квалифицированы как приготовление к террористическому акту:

1) приобретение канистры объемом 20 литров;

2) заправка бензином канистры объемом 20 литров.

В ходе проведенных следственных действий и оперативно-розыскных мероприятий по месту временного проживания были обнаружены и изъяты: две бутылки из полимерного материала с этикеткой «Растворитель 646», 13 стеклянных бутылок с желтой жидкостью, горлышки которых были заткнуты марлей в виде фитиля, металлической канистры с жидкостью.[1]

Приговором Ростовского областного суда Е. и Ф. были осуждены за покушение на террористический акт, совершенный организованной группой. В качестве места совершения данного преступного деяния было выбрано здание УФМС. Взрывное устройство было изготовлено С. Средства, необходимые для изготовления взрывного устройства были переданы ему осужденным Ф. С поставил в картонную коробку с пенопластом пластиковую бутылку с взрывчаткой, проверил соединение проводов в детонаторе. Готовое к использованию взрывное устройство осужденные Ф. и Е. заложили в кучу мусора, который был расположен вблизи здания УФМС.

Г. стал свидетелем данного преступления. После того, как осужденные заложили взрывное устройство, он направился в сторону кучи мусора, осмотрел содержимое коробки, внутри под пенопластом обнаружил взрывное

[1] Апелляционное определение Верховного Суда Российской Федерации от 15 июля 2019 г. по делу № 2-7/2019 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/7dR38XH8ELox/ (дата обращения 04.03.2022).

устройство. Далее Г. сообщил об этом в правоохранительные органы. Территория была оцеплена, осужденные Ф. и Е не смогли довести террористический акт до конца по независящим от них обстоятельствам.[1]

Анализ материалов судебно-следственной практики позволяет сделать вывод о том, что деяние, предусмотренное ст. 205 УК РФ в значительных случаях совершается в совокупности с иными преступными деяниями, в основном, связанными с незаконным оборотом оружия, боеприпасов, взрывчатых веществ. Суд, как правило, назначает наказание в виде лишения свободы путем сложения всех наказаний, предусмотренных за каждое совершенное виновным преступное деяние.

Так, приговором Московского городского суда С. был осужден к лишению свободы за совершение следующих преступных деяний:[2]

1) террористический акт сроком на 10 лет;

2) бандитизм сроком на 7 лет 6 месяцев;

3) незаконная перевозка и ношение взрывного устройства сроком на 4 года;

4) незаконная перевозка взрывного устройства, совершенная организованной группой сроком на 4 года;

5) покушение на террористический акт сроком на 7 лет 6 месяцев;

6) незаконные перевозка и ношение взрывного устройства, совершенные организованной группой сроком на 4 года;

7) покушение на террористический акт, совершенное организованной группой сроком на 7 лет 6 месяцев;

8) незаконные перевозка и ношение огнестрельного оружия, боеприпасов и взрывного устройства, совершенные организованной группой сроком на 4 года;

---

[1] Определение Верховного Суда Российской Федерации от 8 апреля 2013 г. по делу № 2-3/13 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/XAlHXF2ab66Q/ (дата обращения 04.03.2022).

[2] Определение Верховного Суда Российской Федерации от 23 января 2013 г. по делу № 2-124/12 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/uSlv7669MUUV/ (дата обращения 04.03.2022).

9) посягательство на жизнь военнослужащего в целях воспрепятствования законной деятельности указанного лица по охране общественного порядка и обеспечению общественной безопасности сроком на 12 лет;

10) посягательство на жизнь военнослужащего сроком на 12 лет;

11) убийство, то есть умышленное причинение смерти двум и более лицам, совершенное организованной группой и сопряженное с бандитизмом сроком на 12 лет;

12) незаконная перевозка огнестрельного оружия и боеприпасов, совершенная организованной группой сроком на 4 года;

13) террористический акт, совершенный организованной группой сроком на 10 лет;

14) незаконные хранение, перевозку и ношение боеприпасов и взрывного устройства, совершенные организованной группой сроком на 4 года;

15) незаконные перевозку и ношение боеприпасов и взрывного устройства, совершенные организованной группой сроком на 4 года;

16) покушение на террористический акт сроком на 7 лет 6 месяцев

17) незаконная перевозка взрывных устройств, совершенная организованной группой сроком на 4 года.

На основании ч. 3 ст.69 УК РФ по совокупности преступлений путем частичного сложения назначено С. к отбытию лишение свободы сроком на 15 лет с отбыванием наказания в исправительной колонии строгого режима, с ограничением свободы на 2 год с возложением обязанностей являться в специализированный государственный орган два раза в месяц для регистрации, не менять без согласия указанного органа места жительства и не выезжать за пределы территории соответствующего муниципального образования.

Санкции ст.272-274.1 УК РФ предусматривают следующие виды и размеры наказаний за совершение преступлений в сфере компьютерной информации.

За совершение преступления, связанного с неправомерным доступом к охраняемой законом компьютерной информации, если это деяние повлекло

уничтожение, блокирование, модификацию либо копирование компьютерной информации (ч.1 ст.272), действующий Уголовный закон устанавливает такие виды наказаний, как:

штраф (до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев);

исправительные работы (до одного года);

ограничение свободы (до двух лет);

принудительные работы (до двух лет);

лишение свободы (до двух лет).

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ч.1 ст.273), наказываются:

ограничением свободы (до четырех лет);

принудительными работами (до четырех лет);

лишением свободы (до четырех лет) со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Альтернативные санкции содержит статья 274 Уголовного закона, которая предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Часть 1 вышеназванной статьи содержит следующие виды наказаний:

штраф (до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев);

исправительные работы (от шести месяцев до одного года);

ограничение свободы на срок до двух лет;

принудительные работы (до двух лет);

лишение свободы (до двух лет).

Более строгие виды и размеры наказания содержит ст. 274.1 действующего Уголовного закона. Санкция данной нормы содержит следующие виды и размеры наказания за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации:

принудительные работы (до пяти лет) с ограничением свободы (до двух лет) или без такового;

лишение свободы (от двух до пяти лет) со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Анализ материалов, представленных Судебном департаментом при Верховном Суде Российской Федерации[1], позволяет сделать вывод о том, что судами за совершение компьютерных преступлений назначаются следующие виды наказаний (Таблица 2. Практика назначения наказания за преступления в сфере компьютерной информации).

Практика назначения наказания за преступления в сфере компьютерной информации

Таблица 2.

	2017	2018	2019	2020	2021
Всего осуждено	203	129	165	137	225
Лишение свободы на определенный срок	14	4	5	4	6
Условное осуждение к лишению свободы	84	53	59	61	101
Ограничение свободы (основное наказание)	61	46	53	38	67
Штраф (основное наказание)	18	20	34	25	43

[1] Отчет о видах наказания за совершение преступлений в сфере компьютерной информации:ст.272-274.1 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru (дата обращения 06.02.2022).

Анализ статистических данных, представленных в таблице, позволяет сделать вывод о том, что чаще всего судебные органы, рассмотрев уголовные дела о преступлениях в сфере компьютерной информации, назначают наказания, не связанные с изоляцией виновного от общества. Распространенным является назначение виновным условного осуждения, также в качестве основного наказания назначаются штраф, ограничение свободы (Рисунок 2. Практика назначения наказания за совершение преступлений в сфере компьютерной информации).

§3.2. Совершенствование законодательства и практики применения следственными и судебными органами норм Уголовного кодекса Российской Федерации об ответственности за кибертерроризм

Как было отмечено в предыдущих главах, понятие «кибертерроризм» в действующем уголовном законодательстве не закреплено, несмотря на всеобщее его признание в качестве реальной угрозы национальной безопасности Российской Федерации и безопасности мира в целом. В настоящее время, согласно Уголовному кодексу РФ, информационные технологии используются в целях осуществления публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма. По мнению законодателя, действия, совершаемые путем использования высоких технологий, не могут дестабилизировать деятельность органов власти или международных организаций либо воздействовать на принятие ими решений, устрашать население, создавать опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий.

Необходимо отметить, что уголовное законодательство некоторых зарубежных стран было усовершенствовано в целях противодействия исследуемому преступному деянию. Так, Раздел 66F Закона Индии об информационных технологиях предусматривает уголовную ответственность за

«кибертерроризм», угрожающий единству, целостности, безопасности или суверенитету Индии или вселяющий страх в людей. Данное преступное деяние может быть совершено путем получения доступа к компьютерному ресурсу без разрешения или превышение разрешенного доступа, путем использования компьютерных вирусов, внедряемых в информационные ресурсы. Лицо, совершившее кибертеррористический акт либо вступившее в сговор с целью его совершения, подлежит наказанию в виде тюремного заключения, которое может быть продлено до пожизненного заключения.[1]

Законодательство Великобритании, как и отечественное уголовное законодательство, не содержит понятия «кибертерроризм», однако устанавливает нормы, предусматривающие ответственность за совершение террористического акта посредством противоправного вмешательства в электронные системы или нарушение их работы.[2]

Аналогичный подход существует в уголовном законодательстве Австралии. Применение австралийского закона о терроризме в случаях кибератак ограничивается только атаками, представляющими собой серьезное вмешательство, нарушение или уничтожение электронных систем. Закон также включает «исключение для политических протестов». Он устанавливает, что любая форма протеста, инакомыслия или иного не будет считаться терроризмом, если она не направлена на причинение смерти, серьезного физического вреда или угрозы жизни и т. д.[3]

Уголовно-правовое противодействие кибертерроризму осуществляется в США, путем криминализации деяний, составляющих кибертерроризм. Законодательство США относит к преступлениям террористического характера преступные деяния, направленные на взлом правительственных компьютеров;

---

[1] IT Act 2000 – Penalties, Offences With Case Studies - Checkmate [Электронный ресурс] // Leading Cyber Security Services Provider in US, Middle East, India & South Asia URL: https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/ (дата обращения: 04.03.2022).

[2] The Terrorism Act 2006 [Электронный ресурс]. Режим доступа: https://www.gov.uk/ government/publications/the-terrorism-act-2006 (дата обращения 10.03.2022).

[3] Наркулов А. К. (2022). Нормативно-правовая база зарубежных стран и международных организаций в области противодействия кибертерроризму. Academic research in educational sciences, 3 (3). С. 220.

взлом компьютеров, приводящий к воздействию на правительственную, кредитную, финансовую или компьютерную информацию; повреждение правительственного, банковского компьютера или компьютера, используемого или затрагивающего внутреннюю или внешнюю торговлю; совершение мошенничества через несанкционированный доступ к правительственному компьютеру, банковскому компьютеру или компьютеру, используемому во внутренней или внешней торговле; угроза повреждения правительственного, банковского компьютера или компьютера, который используется во внутренней или внешней торговле; незаконный оборот паролей для правительственного компьютера, а также влияние такого оборота на внутреннюю или внешнюю торговлю; использование компьютера для шпионажа.[1]

Уголовное законодательство Китая также не выделяет кибертерроризм в качестве отдельного вида преступления. Однако анализ положений Уголовного кодекса КНР позволяет сделать вывод о наличии следующих составов преступлений кибертеррористической направленности:

1) незаконный доступ к компьютерной информации государственной важности либо связанной с обороноспособностью, а также к данным о прорывных технологиях и научных открытиях;

2) удаление, искажение, внесение компьютерной информации, вызвавшей нарушение работы и существенные последствия, а также за намеренное создание и распространение компьютерных вирусов.[2]

Ответственность за совершение кибертеррористических актов предусмотрена законодательством менее развитых стран, например, Пакистана. Так, Пакистанский закон «О предотвращении электронных преступлений» 2007 года относит к кибертерроризму совершение при помощи вычислительной техники преступления, имеющего негативные последствия для национальной

[1] Charles D. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws [Электронный ресурс]. The Federation of American Scientists. Режим доступа: https://fas.org/sgp/crs/ misc/RS20830.pdf (дата обращения 26.02.2022).

[2] Уголовный кодекс КНР: принят 14 марта 1997 г. URL: http://www.lehmanlaw.com/resource-centre/laws-and-regulations/general/amendment-3-to-the-cnminal-law-of-the-peoples-republic-of-china-2001.html (дата обращения 04.03.2022).

безопасности. Если акт компьютерного терроризма повлечет за собой смерть человека, то лица, совершившие его, приговариваются к смерти или пожизненному лишению свободы, как граждане Пакистана, так и иностранцы. Этим законом в Пакистане также был отменён мораторий на смертную казнь.[1]

Статья 421-1 Уголовного кодекса Франции, предусматривая понятие акта терроризма, лишь дополняет, что оно будет распространяться и на преступные деяния в области информатики в случае выявления их целевой направленности. При этом сделана ссылка на книгу III Уголовного кодекса, устанавливающую уголовную ответственность за преступления в сфере компьютерной информации. После появления специальных электронных журналов и сайтов, пропагандирующих террористические действия, в УК Франции появилась ст. 421-2-5-2, которой введена уголовная ответственность за распространение в сети Интернет сообщений, изображений, иных информационных действий, включающих показ преднамеренных нападений на жизнь с демонстрацией приверженности к террористической идеологии.

Уголовное законодательство Италии имеет свою специфику. Так, помимо специальных составов за акты терроризма в УК Италии есть общая норма (ст. 280), позволяющая отнести к террористическому практически любое преступление, предусмотренное кодексом, если оно было совершено с данной целью. Внимание к кибертерроризму в Италии можно проследить на судьбе ст. 270-quinquies ее Уголовного кодекса, устанавливающей ответственность за обучение террористической деятельности. В 2005 г. эта статья была введена в УК Италии (благодаря Закону Джузеппе Писану, по фамилии инициатора — министра внутренних дел страны), но в 2015 г. получила важное дополнение — наказание увеличивается при обучении с использованием IT-технологий.[2]

---

[1] В Пакистане введена смертная казнь за кибертерроризм. // Новостной аналитический портал Securitylab.ru. Режим доступа: https://www.securitylab.ru/news/362634.php/ (дата обращения 08.03.2022).

[2] Кулешова Галина Петровна, Капитонова Елена Анатольевна, & Романовский Георгий Борисович (2020). Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения. Всероссийский криминологический журнал, 14 (1). С. 160.

Отечественная уголовно-правовая наука следующие способы совершенствования действующего уголовного законодательства в области противодействия кибертерроризму.

Первый способ – внесение изменений в статью 205 Уголовного закона, предусматривающую ответственность за совершение террористического акта. Некоторые ученые-специалисты в области уголовного права, в частности Е.А. Капитонова, считают необходимым введение уголовной ответственности за совершение террористического акта с использованием информационных сетей, включая Интернет, в качестве квалифицированного состава в ст. 205 УК РФ.[1]

Такой же позиции придерживается И. Г. Чекунов, законодательное предложение которого сформулировано следующим образом: «ввести в ст. 205 УК РФ квалифицированный состав — ч.2 – с повышенной уголовной ответственностью за «террористический акт с несанкционированным доступом в компьютерные системы или информационно-коммуникационные сети, осуществляющие автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения с целью нарушения их функционирования и создания аварийной ситуации и угрозы техногенной катастрофы».[2]

В своих исследованиях А.А. Тетюшев также указывает на необходимость криминализации кибертерроризма, однако, в отличие от предыдущих авторов, без внесения каких-либо изменений в статью 205 УК РФ. По мнению А.А. Тетюшева, «необходимым является создание в Особенной части УК РФ нового самостоятельного состава преступления с введением понятия кибертерроризма, так как содержание его элементов будет существенным образом отличаться от предусмотренных в ст. 205 УК РФ:

1. В содержание объекта посягательства для данного состава преступления включаются не только общественная безопасность и

[1]Капитонова, Е. А. Особенности кибертерроризма как новой разновидности террористического акта / Е. А. Капитонова // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2015. – № 2 (34). С. 35-36.

[2] Чекунов И. Г. Киберпреступность: понятие и классификация. // Российский следователь. – 2012. – № 2. С. 40.

общественный порядок, но уже наиболее значимые интересы Российской Федерации: национальная безопасность, законный порядок функционирования органов власти и управления РФ в отношениях с международными организациями и другими государствами, сохранность оборонной, экономической и финансовой систем государства и т.д.

2. Местом совершения данного преступления может быть не только территория РФ, но и другого государства.

3. В числе субъектов совершения актов кибертерроризма могут быть не только отдельные граждане, но и представители иностранных организаций и силовых структур отдельных государств, развязывающих кибервойны»[1]

Аналогичный способ криминализации кибертерроризма предлагает А.С. Питинова: «законодательно закрепить следующее понятие «кибертерроризма» — совершение противоправных действий, направленных на компьютерную информацию, компьютерные системы или сети и создающих угрозу безопасности личности, общества и государства с целью получения преимущества при решении политических, экономических, социальных задач. Полагаем, что следует добавить в Главу «Преступления против общественной безопасности» Уголовного кодекса РФ новый состав преступления, устанавливающий уголовную ответственность за кибертерроризм».[2]

Некоторые авторы, помимо криминализации кибертерроризма путем введения в действующий Уголовный закон нового состава преступления, предлагают закрепить цель исследуемого вида преступления, которая отличается от цели традиционного террористического акта. Так, по мнению Д.В. Пучкова «к основным целям терроризма в кибер-пространстве следует отнести попытки воспрепятствования или разрушение процесса функционирования компьютерных систем или сетей информационной инфраструктуры государства или органов управления. Подобные преступные

[1] Тетюшев, А. А. Противодействие кибертерроризму средствами уголовного закона / А. А. Тетюшев // NovaUm.Ru. – 2018. – № 16. С. 380.

[2] Питинова, А. С. Актуальные вопросы противодействия кибертерроризму / А. С. Питинова. — Текст : непосредственный // Право: история, теория, практика : материалы VI Междунар. науч. конф. (г. Санкт-Петербург, июнь 2018 г.). — Санкт-Петербург : Свое издательство, 2018. С. 32.

действия в отношении критически важных объектов информационной инфраструктуры представляют собой значительную угрозу, которая может иметь самые серьезные последствия для всего общества. Потенциальными целями могут быть государственные структуры, телекоммуникационные сети, навигационные системы для судоходства и воздушного движения, системы управления водными ресурсами, энергетические и финансовые системы, имеющие жизненно важное значение для социума».[1]

Второй способ – усовершенствование статей, закрепленных в Главе 28 действующего Уголовного закона, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации:

1. Неправомерный доступ к компьютерной информации (Статья 272).

2. Создание, использование и распространение вредоносных компьютерных программ (Статья 273).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (Статья 274).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (Статья 274.1).

Следует признать, что диспозиции вышеназванных статей являются максимально приближенными по смыслу и методам к кибертерроризму. Указанные преступные деяния могут быть совершены, в том числе и в террористических целях.

Так, по мнению Е.А. Капитоновой, «статьи 272-274 Уголовного кодекса, посвященные вопросам ответственности за преступления в сфере компьютерной информации, в настоящее время не содержат каких-либо упоминаний о террористической деятельности. Так, несмотря на то, что кибертерроризм может проявляться в виде кибератак посредством использования вредоносных программ, ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»

[1] Пучков Д. В. (2021). Кибертерроризм как новая угроза. Виктимология, 8 (4). С. 390.

этого положения не учитывает. Для устранения данного пробела в праве представляется необходимым либо добавить в ст. 205 УК РФ квалифицированный состав (о чем говорилось ранее), либо внести в ч. 3 ст. 273 УК РФ в качестве особо квалифицирующего признака ответственность за создание и использование вредоносных компьютерных программ в террористических целях».[1]

Таким образом, наука уголовного права предлагает несколько способов усовершенствования уголовного законодательства в целях противодействия кибертерроризму. Несмотря на то, что понятие «кибертерроризм» существует в науке относительно давно и признается одной из главных угроз национальной безопасности РФ, законодательными органами власти не были предприняты попытки криминализации данного деяния.

Эффективное противодействие кибертерроризму возможно при совершенствовании не только норм уголовного законодательства, но и иных нормативных правовых актов, в которых затрагиваются вопросы, связанные с противодействием исследуемому преступному явлению.

Внесение изменений в действующий Уголовный кодекс не является единственным способом усовершенствования отечественного законодательства в сфере противодействия кибертерроризму. Для признания кибертерроризма как преступного уголовно-наказуемого деяния, использования понятий «кибертерроризм», «кибертеррористический акт» не только в науке, но и в правоприменительной деятельности, следует дать ст.205 УК РФ более широкое толкование. Действия кибертеррористической направленности могут быть рассмотрены как «иные действия». В предыдущих главах было указано, что «иные действия» толкуются как разные по характеру действия, способные повлечь за собой такие же последствия, как и при взрыве или поджоге: использование радиоактивных, ядовитых и сильнодействующих веществ, производство массовых отравлений, распространение эпидемий и эпизоотии,

[1]Капитонова Е.А. (2015). Особенности кибертерроризма как новой разновидности террористического акта. Известия высших учебных заведений. Поволжский регион. Общественные науки, (2 (34)). С. 34-35.

устройство аварий и катастроф, вывод из строя жизнеобеспечивающих объектов, нарушение технологических либо производственных процессов, блокирование транспортных коммуникаций.

В Постановлении 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» необходимо внести изменения. В пункте 3 вышеназванного акта в качестве иных действий, сопоставимых по последствиям с взрывом или поджогом, закрепить «совершение атак на компьютерные и телекоммуникационные технологии в целях, предусмотренных ст.205 УК РФ (кибертеррористический акт)».

В этом же акте необходимо определить круг преступных деяний (в качестве примера), которые образуют состав кибертеррористического акта:

1. неправомерное завладение или уничтожение линий связи и телекоммуникаций, информационных ресурсов, программно-технических оборудований, имеющих стратегическую важность, путем преодоления систем защиты, внедрения вредоносных программ или вирусов, программных закладок и т.п.;

2. нанесение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания или электростанций, наведение помех, переадресация потока данных, искусственная перегрузка узлов коммутации, использование химических средств для разрушения элементной базы и др.);

3. воздействие на программное обеспечение или информацию в информационных системах и системах управления с целью их искажения или модификации;

4. раскрытие и угроза распространения или распространение конфиденциальной информации об информационной инфраструктуре государства, стратегически важных и информационных систем обороны, кодах шифрования, принципах работы систем шифрования;

5. захват технических каналов связи или сетей телекоммуникаций с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций и антиконституционных структур; 6. проведение информационно-психологических операций, воздействие на операторов и разработчиков информационных и телекоммуникационных сетей и систем путем насилия или угрозы насилия, шантажа, подкупа, использования нейролингвистического программирования, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и т.д.[1]

Принятие вышеназванных законодательных решений, направленных на юридическое закрепление кибертерроризма как преступления, как разновидности террористической деятельности требует совершенствования иных нормативных правовых актов, регулирующих отношения в сфере противодействия терроризму.

Основным нормативным правовым актом в области противодействия террористической деятельности в Российской Федерации является Федеральный закон от 6 марта 2006 г № 35 ФЗ «О противодействии терроризму».[2] Закон определяет основные принципы противодействия терроризму, организационные основы указанной деятельности (устанавливает перечень субъектов противодействия терроризму и их полномочия), регулирует вопросы, связанные с подготовкой и проведением контртеррористической операции.

В статье 3 данного нормативного правового акта закреплены основные понятия, такие как терроризм, террористическая деятельность, террористический акт и т.д., также определен перечень действий, относящихся к террористической деятельности. Как и во многих других нормативно-правовых актах, понятие «кибертерроризм» и иные связанные с ним понятия в

[1] Расулев А. Противодействие кибертерроризму: международно-правовые и уголовно-правовые аспекты / А. Расулев // Вестник юридических наук. – 2018. – № 4. С. 94.
[2] О противодействии терроризму: федеральный закон от 6 марта 2006 г N 35 ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 15.02.2022).

Законе «О противодействии терроризму» не закреплены. Следовательно, в случае криминализации кибертерроризма, исследуемая норма должна быть дополнена такими понятиями, как «кибертерроризм», «кибертеррористическая деятельность», «кибертеррористическая атака», помимо этого, должен быть определен круг действий кибертеррористического характера. Например, неправомерное завладение или уничтожение линий связи и телекоммуникаций воздействие на программное обеспечение или информацию, раскрытие и угроза распространения или распространение конфиденциальной информации об информационной инфраструктуре государства, стратегически важных и информационных систем обороны, разрушение сетей электропитания или электростанций и т.д.

Единственным правовым актом, в котором содержится понятие «кибертерроризм», является Концепция противодействия терроризму в Российской Федерации (утв. Президентом РФ 5 октября 2009 г.).[1] Концепция определяет основные принципы государственной политики в области противодействия терроризму в Российской Федерации, цель, задачи и направления дальнейшего развития общегосударственной системы противодействия терроризму в Российской Федерации.

В Разделе I Концепции определены внутренние и внешние факторы, которые способствуют распространению терроризма в России. Так, к числу внутренних факторов, способствующих возникновению и распространению терроризма в Российской Федерации, Концепция относит распространение идей терроризма и экстремизма через информационно-телекоммуникационную сеть Интернет и средства массовой информации. Концепция не содержит положений о том, что высокие технологии применяются непосредственно в целях совершения террористических актов. Что еще раз доказывает тот факт, что, по мнению законодателя, действия, совершаемые путем использования высоких технологий, не могут дестабилизировать деятельность органов власти

[1] «Концепция противодействия терроризму в Российской Федерации» (утв. Президентом РФ 05.10.2009) [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 04.01.2022).

или международных организаций либо воздействовать на принятие ими решений, устрашать население, создавать опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий.

В Разделе III Концепции регламентированы вопросы, связанные правовым, информационно-аналитическим, научным, материально-техническим, финансовым и кадровым обеспечением деятельности по противодействию террористической деятельности. В пункте 45 определены основные направления кадрового обеспечения противодействия терроризму, к числу которых относится подготовка специалистов в специфических областях противодействия терроризму (противодействие идеологии терроризма, ядерному, химическому, биологическому терроризму, кибертерроризму и другим его видам). В отличие от кибертерроризма, такие разновидности террористической деятельности, определенные в Концепции, как ядерный, химический и биологический терроризм закреплены на законодательном уровне. Так, ч.3 ст. 205 УК РФ устанавливает ответственность за совершение террористического акта, сопряженного с посягательством на объекты использования атомной энергии либо с использованием ядерных материалов, радиоактивных веществ или источников радиоактивного излучения либо ядовитых, отравляющих, токсичных, опасных химических или биологических веществ.

Исследования, проведенные в рамках данной главы, позволяют сделать следующие выводы.

Действующим уголовным законодательством за совершение террористического акта предусмотрено наказание в виде лишения свободы. Следует отметить, что отечественная уголовно-правовая политика направлена на ужесточение наказания за совершение террористического акта, что выражается в постепенном увеличении нижнего и верхнего пределов уголовного наказания в виде лишения свободы. Анализ материалов судебно-следственной практики позволяет сделать вывод о том, что срок наказания в

виде лишения свободы чаще всего не доходит до верхнего предела, однако и минимальный срок наказания в большинстве случаев судами не назначается.

Деяние, предусмотренное ст. 205 УК РФ в значительных случаях совершается в совокупности с иными преступными деяниями, в основном, связанными с незаконным оборотом оружия, боеприпасов, взрывчатых веществ. Суд, как правило, назначает наказание в виде лишения свободы путем сложения всех наказаний, предусмотренных за каждое совершенное виновным преступное деяние.

Преступления в сфере компьютерной информации являются менее тяжкими, чем террористический акт. Анализ статистических данных позволяет сделать вывод о том, что чаще всего судебные органы, рассмотрев уголовные дела о преступлениях в сфере компьютерной информации, назначают наказания, не связанные с изоляцией виновного от общества. Распространенным является назначение виновным условного осуждения, также в качестве основного наказания назначаются штраф, ограничение свободы. Остальные виды наказания – лишение свободы на определенный срок, исправительные работы, принудительные работы, обязательные работы назначаются реже.

Так как действующее уголовное законодательство не содержит нормы, устанавливающие ответственность за совершение кибертеррористических актов, то в целях противодействия исследуемому явлению большинство ученых в своих исследованиях предлагают криминализировать кибертеррористическую деятельность.

Первая группа ученых (И. Г. Чекунов, Е.А. Капитонова) считает необходимым усовершенствование статьи 205 УК РФ путем введения уголовной ответственности за совершение террористического акта с использованием информационных сетей, включая Интернет, в качестве квалифицированного состава в ст. 205 УК РФ.

По мнению второй группы ученых (А.А. Тетюшев), целесообразно создать Особенной части УК РФ новый самостоятельный состав преступления

с введением понятия кибертерроризма. Так как признаки состава кибертерроризма отличаются от традиционного террористического акта. Кибертеррористический акт, по мнению представителей данного подхода, имеет специфическую цель – попытка воспрепятствования или разрушение процесса функционирования компьютерных систем или сетей информационной инфраструктуры государства или органов управления. Кроме того, при кибертерроризме, как было отмечено ранее, используется информационное оружие, тогда как традиционный террористический акт предполагает использование взрывных устройств, взрывчатых веществ, огнестрельного оружия и боеприпасов, иными словами существует отличие в способах совершения данных преступных деяний.

Некоторые ученые предлагают усовершенствовать статьи, закрепленные в Главе 28 действующего Уголовного закона, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации. Например, внести в ч. 3 ст. 273 УК РФ в качестве особо квалифицирующего признака ответственность за создание и использование вредоносных компьютерных программ в террористических целях.

ЗАКЛЮЧЕНИЕ

На основании вышеизложенного можно сделать следующие выводы.

Понятие «кибертерроризм» в отечественном законодательстве не закреплено. Одни ученые-специалисты в области уголовного права определяют исследуемое деяние как атаку на компьютерные и телекоммуникационные технологии, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, действия, произведенные с помощью средств сети Интернет в террористических целях. Другие считают, что кибертерроризм складывается из следующих действий:

1) совершение терактов посредством информационных сетей, когда Интернет выступает как способ и средство совершения преступления;

2) деятельность, способствующая терроризму, например вербовка в террористические организации, сбор средств для террористов или организация взаимодействия между членами террористических групп.

От традиционного терроризма кибертерроризм отличается, в первую очередь, признаками объективной стороны:

1. Характер действий, направленных на достижение преступного результата. При кибертерроризме – это атаки на информацию, в традиционном терроризме – взрыв, поджог, иные действия, устрашающие население.

2. Место совершения преступного деяния. Кибертерроризм совершается в информационной среде, тогда как местом совершения террористических актов выступает материальный мир.

3. Орудие, средства, используемые для достижения преступного результата. Кибертерроризм совершается путем использования информационного оружия. Преступные цели в традиционном терроризме достигаются, как правило, с помощью взрывчатых веществ, огнестрельного оружия и других механических устройств.

На возникновение и развитие кибертеррористической деятельности оказывают влияние общие (политические, экономические и т.д.) и частные факторы – наличие неограниченных возможностей финансирования, анонимность, удаленность, многообразие преступных целей, широкий охват практически неограниченной публики.

Статья 205 действующего Уголовного закона предусматривает ответственность за совершение террористического акта. Исследуемое преступное деяние посягает на общественные отношения, связанные с поддержанием общественной безопасности в сфере повседневной жизнедеятельности, т.е. отношения, обеспечивающие состояние защищенности жизненно важных интересов неопределенного круга лиц, организаций и иных материальных объектов от внутренних и внешних угроз.

Объективная сторона террористического акта представляет собой совершение взрыва, поджога и иных действий, которые выступают в качестве способов совершения исследуемого вида преступления. Для квалификации указанных действий по ст.205 УК РФ необходимо, чтобы они были направлены на устрашение населения. Понятия «устрашение», «население», в свою очередь, являются оценочными понятиями.

В законодательстве критерии страха не закреплены, что может создать проблемы при квалификации исследуемого преступного деяния. Нельзя быть уверенным в том, что поджог, совершенный в террористических целях вызвал страх у проживающих на той или иной территории людей. Отсутствие

доказательств, подтверждающих устрашающий характер террористических действий, приводит к переквалификации деяния, предусмотренного ст.205 УК РФ на менее тяжкий состав преступления.

Действующие нормативные правовые акты не содержат определения понятия «население», не устанавливают его количественную характеристику. Поэтому нет однозначного ответа на вопрос: какое минимальное количество людей должно испытать чувство страха для квалификации взрыва, поджога, иных действий по ст.205 УК РФ.

Возможно, вышеназванные оценочные понятия на практике не оказывают существенного влияния на квалификацию преступных деяний по ст.205 УК РФ. Однако их наличие, сложность определения указывают на необходимость совершенствования действующего Уголовного закона. Закон не должен содержать оценочные понятия, однако если они имеются, то должны быть конкретизированы в данном законодательном акте либо в иных принимаемых в соответствии с ним нормативных правовых актах.

Одним из важнейших элементов состава террористического акта, влияющего на квалификацию данного вида преступления, является его специфическая цель:

1) дестабилизация деятельности органов власти или международных организаций либо воздействие на принятие ими решений – в случае совершения взрыва, поджога, иных действий;

2) воздействие на принятие решений органами власти или международными организациями – при угрозе совершения вышеназванных действий. Некоторые авторы не согласны с данной формулировкой диспозиции статьи 205 УК РФ и считают, что решение законодателя при определении цели угрозы ограничиться лишь закреплением цели воздействия на принятие органами власти решений, и исключение цели дестабилизации деятельности соответствующих органов власти, является необоснованным.

Помимо анализа состава преступления, предусмотренного ст.205 Уголовного кодекса РФ, также была проанализирована практика назначения

наказания за совершение исследуемого вида преступления. За совершение террористического акта предусмотрено наказание в виде лишения свободы. Следует отметить, что отечественная уголовно-правовая политика направлена на ужесточение наказания за совершение террористического акта, что выражается в постепенном увеличении нижнего и верхнего пределов уголовного наказания в виде лишения свободы. Срок наказания в виде лишения свободы чаще всего не доходит до верхнего предела, однако и минимальный срок наказания в большинстве случаев судами не назначается.

Деяние, предусмотренное ст. 205 УК РФ в значительных случаях совершается в совокупности с иными преступными деяниями, в основном, связанными с незаконным оборотом оружия, боеприпасов, взрывчатых веществ. Суд, как правило, назначает наказание в виде лишения свободы путем сложения всех наказаний, предусмотренных за каждое совершенное виновным преступное деяние.

Помимо террористического акта, была изучена практика назначения наказания за преступления в сфере компьютерной информации. Следует отметить, что виды и размеры наказания за компьютерные преступления являются менее строгими, чем за террористический акт. Чаще всего судебные органы, рассмотрев уголовные дела о преступлениях в сфере компьютерной информации, назначают наказания, не связанные с изоляцией виновного от общества. Распространенным является назначение виновным условного осуждения, также в качестве основного наказания назначаются штраф, ограничение свободы. Остальные виды наказания назначаются реже.

Как известно, понятие «кибертероризм» в настоящее время используется только в науке, например, в уголовном праве, в криминологии и т.д. Так как кибертерроризм является серьезной угрозой национальной безопасности, то первостепенной задачей государства, его законодательных органов является юридическое закрепление исследуемого деяния в качестве преступного, уголовно-наказуемого, то есть криминализация кибертерроризма.

Криминализировать кибертерроризм можно следующими способами.

Первый способ – внести изменения в ч.2 ст. 205 УК РФ:

2. Те же деяния:

г) совершенные путем несанкционированного доступа в компьютерные системы или информационно-коммуникационные сети, осуществляющие автоматизированное управление опасными технологическими производствами и предприятиями жизнеобеспечения с целью нарушения их функционирования и создания аварийной ситуации и угрозы техногенной катастрофы.

Второй способ – введение новой самостоятельной статьи в Особенную часть УК РФ.

Статья 205.7. Кибертеррористический акт.

Кибертеррористический акт, то есть преднамеренная, мотивированная атака на информацию, которая находится, хранится и обрабатывается компьютером, компьютерную систему и сети, которая создает опасность для самой жизни или здоровья людей, или влечет за собой наступление других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта.

Некоторые ученые предлагают усовершенствовать статьи, закрепленные в Главе 28 действующего Уголовного закона, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации. Например, внести в ч. 3 ст. 273 УК РФ в качестве особо квалифицирующего признака ответственность за создание и использование вредоносных компьютерных программ в террористических целях.

Внесение изменений в действующий Уголовный кодекс не является единственным способом усовершенствования отечественного законодательства в сфере противодействия кибертерроризму. Для признания кибертерроризма как преступного уголовно-наказуемого деяния, использования понятий «кибертерроризм», «кибертеррористический акт» не только в науке, но и в правоприменительной деятельности, следует дать ст.205 УК РФ более широкое

толкование. Действия кибертеррористической направленности могут быть рассмотрены как «иные действия».

В Постановлении 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» необходимо внести изменения. В пункте 3 вышеназванного акта в качестве иных действий, сопоставимых по последствиям с взрывом или поджогом, закрепить «совершение атак на компьютерные и телекоммуникационные технологии в целях, предусмотренных ст.205 УК РФ (кибертеррористический акт)».

СПИСОК ИСТОЧНИКОВ И ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, иные нормативные правовые акты и иные официальные документы Российской Федерации

1. Декларация о мерах по ликвидации международного терроризма (Принята 09.12.1994 Резолюцией 49/60 на 84-ом пленарном заседании Генеральной Ассамблеи ООН) // Действующее международное право. Т. 3. М., 1997. С. 90 -94
2. Европейская конвенция о пресечении терроризма (ETS N 90) (Заключена в г. Страсбурге 27.01.1977) (с изм. от 15.05.2003) // СЗ РФ. 2003. № 3. Ст. 202.
3. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Заключена в г. Будапеште 23.11.2001) // СПС «КонсультантПлюс» (дата обращения: 27.02.2022).
4. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: [заключено в г.

Екатеринбурге 16.06.2009 г.] // Бюл. междунар. договоров. 2012. № 1. С. 13-21.

5. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // СПС «КонсультантПлюс» (дата обращения: 27.03.2022).
6. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ (ред. от 25.03.2022) - [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 27.01.2022).
7. О противодействии терроризму: федеральный закон от 6 марта 2006 г N 35 ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения: 15.02.2022).
8. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 06.07.2016 № 375-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 04.03.2022).
9. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г N 187 ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 14.03.2022).
10. О внесении изменений в Уголовный кодекс Российской Федерации: федеральный закон от 09.12.2010 № 352-ФЗ [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 03.02.2022).
11. «Концепция противодействия терроризму в Российской Федерации» (утв. Указом Президента РФ 05.10.2009) [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 04.01.2022).
12. Уголовный кодекс КНР: принят 14 марта 1997 г. [Электронный ресурс] URL: http://www.lehmanlaw.com/resource-centre/laws-and regula-

tions/general/amend ment-3-to-the-cnminal-law-of-the-peoples-republic-of-china-2001.html (дата обращения 04.03.2022).

II. Монографии, учебники, учебные пособия:

13. Боровиков В. Б. Уголовное право. Особенная часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов ; под редакцией В. Б. Боровикова. — 6-е изд., перераб. и доп. — Москва: Юрайт, 2022. — 473 с.
14. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: автореферат дис. ... кандидата юридических наук : 12.00.08 / Краснояр. гос. ун-т. - Красноярск, 2002. - 27 с.
15. Квалификация преступлений: учебное пособие для вузов / О. С. Капинус [и др.]; под редакцией О. С. Капинус. — 2-е изд. — Москва: Издательство Юрайт, 2022. — 204 с.
16. Козаченко И. Я. Уголовное право. Общая часть: учебник для вузов / И. Я. Козаченко, Г. П. Новоселов. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 430 с.
17. Расторгуев С. П. Основы информационной безопасности / Учеб. пособие для студ. высших учебных заведений. — М.: Издательский центр «Академия», 2009. – 186 с.
18. Сверчков В. В. Уголовное право. Особенная часть: учебное пособие для вузов / В. В. Сверчков. — 10-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 280 с.
19. Уголовное право в 2 т. Том 2. Особенная часть : учебник для вузов / А. В. Наумов [и др.]; ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 5-е изд., перераб. и доп. — Москва: Юрайт, 2022. — 499 с.
20. Уголовное право. Особенная часть в 2 т. Том 2: учебник для вузов / И. А. Подройкина [и др.]; ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. — 5-е изд., перераб. и доп. — Москва: Юрайт, 2022. — 536 с.

21. Уголовное право. Особенная часть: преступления против общественной безопасности и общественного порядка: учебник для вузов / В. М. Алиев [и др.]; под общей редакцией В. И. Гладких, А. К. Есаяна. — Москва: Юрайт, 2022. — 352 с.
22. Фоменко Е. В. Правовые основы противодействия терроризму. Уголовно-правовой и криминологический аспекты: учебное пособие для вузов / Е. В. Фоменко, Ю. Н. Маторина. — 2-е изд. — Москва: Юрайт, 2022. — 186 с.

III. Статьи, научные публикации:

23. Батуева Е. В. Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая // Вестник МГИМО Университета. 2014. № 3. – С. 128–136.
24. Беляева М. Г. Анализ объекта преступления на примере состава преступления, предусмотренного ст. 205 УК РФ «террористический акт» // Современные инновации, (7 (21)), 2-17. 2020. – С. 33-34.
25. Васильева А. Н. Понятие и проблемы противодействия кибертерроризму // Успехи современного естествознания. 2011. № 8. – С. 232–233.
26. Васильев К. И. К вопросу о понятии «кибертерроризм» в российской науке // Молодой учёный. № 17 (97) . – С. 337.
27. Геворгян Е. М. Кибертерроризм как угроза информационной безопасности Российской Федерации / Е. М. Геворгян // Скиф. Вопросы студенческой науки. – 2021. – № 6(58). – С. 118-122.
28. Голубев В. А. Кибертерроризм — понятие, терминология, противодействие // Сайт Саратовского Центра по исследованию проблем организованной преступности и коррупции [Электронный ресурс]. — URL: http://sartraccc. ru/i.php?oper=read_file&filename=Pub/golubev (17–03–05).htm (дата обращения 20.04.2022).

29. Джафарли В. Ф. Личность преступника в механизме преступлений, совершаемых в сфере информационных технологий / В. Ф. Джафарли. – Москва: КноРус, 2017. – 108 с.
30. Джинджолия Р.С., Боровиков В.Б. Российское уголовное право: в 2 ч. Общая часть: учеб.-наглядное пособие (схемы). - М.: Прометей, 2018. - 158 с.
31. Дремлюга Р.И, Коробеев А.И, Федоров А.В. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. Всероссийский криминологический журнал, 11 (3), 2017. С. 607-614.
32. Журавель В. П. Зарубежное военное обозрение. - 2018. №5. С. 12-15
33. Журавленко Н. И. Основные направления борьбы с угрозами кибертерроризма / Н. И. Журавленко, О. В. Тутова // Противодействие экстремизму и терроризму в крымском федеральном округе: проблемы теории и практики. – Крым: Изд-во Краснодарского университета МВД России (Крымский филиал), 2015. – С. 303-311.
34. Зыков Д. А. Виктимологические аспекты предупреждения компьютерного мошенничества : специальность 12.00.08 "Уголовное право и криминология; уголовно-исполнительное право" : диссертация на соискание ученой степени кандидата юридических наук / Зыков Даниил Алексеевич. – Владимир, 2002. – 211 с.
35. Ивлиев П.А. Анонимность в интернете: проблемы и особенности // Международный журнал гуманитарных и естественных наук, (4-2), 2019. – С. 6-8.
36. Игнатов А.Н. Проблемы законодательной регламентации уголовной ответственности за преступления террористического характера // Вестник Московского университета МВД России. 2017. № 6. – С. 98-101.
37. Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта / Е. А. Капитонова // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2015. – № 2 (34). – С. 29–41.

38. Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет : автореферат дис. ... кандидата юридических наук : 12.00.08 / Науч.-исслед. ин-т проблем укрепления законности и правопорядка при Генер. прокуратуре РФ. - Москва, 2002. - 25 с.
39. Кулешова Г.П., Капитонова Е.А., Романовский Г.Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал, 14 (1). – С. 156-165.
40. Малик Е. Н. Кибертерроризм как мировая угроза: вызовы и меры борьбы // Вестник Прикамского социального института. 2020. № 1 (85). – С. 169–173.
41. Наркулов А. К. (2022). Нормативно-правовая база зарубежных стран и международных организаций в области противодействия кибертерроризму. Academic research in educational sciences, 3 (3) 2022. – С. 217-224.
42. Огородник А. В. История возникновения кибертерроризма: от киберпреступности до кибертерроризма / А. В. Огородник // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: Материалы VI Международной научной конференции, Донецк, 26–28 октября 2021 года / Под общей редакцией С.В. Беспаловой. – Донецк: Донецкий национальный университет, 2021. – С. 146-149.
43. Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт / А.Л. Осипенко. — М.: Норма, 2004. – 432 с.
44. Питинова А. С. Актуальные вопросы противодействия кибертерроризму / А. С. Питинова. — Текст: непосредственный // Право: история, теория, практика: материалы VI Междунар. науч. конф. (г. Санкт-Петербург, июнь 2018 г.). — Санкт-Петербург: Свое издательство, 2018. — С. 31-34.

45. Пучков Д. В. Кибертерроризм как новая угроза. Виктимология, 8 (4), 2021. – С. 382-391.
46. Расулев А. Противодействие кибертерроризму: международно-правовые и уголовно-правовые аспекты / А. Расулев // Вестник юридических наук. – 2018. – № 4. – С. 93-95.
47. Рогожевский А.С. Краткий анализ состава преступления, предусмотренного ст. 205 Уголовного кодекса Российской Федерации // Вестник магистратуры, (5-3 (116)), 2021. – С. 36-38.
48. Серебренникова А.В. Кибертерроризм: причины и условия. Colloquium-journal, (17 (104)), 2021. – С. 47-49.
49. Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации. Автореф. дис. канд. юрид. наук. Волгоград, 2001. - 24 с.
50. Тетюшев А. А. Противодействие кибертерроризму средствами уголовного закона / А. А. Тетюшев // NovaUm.Ru. – 2018. – № 16. – С. 387-390.
51. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы // Автореферат на соискание ученой степени к.ю.н., Владивосток — 2005. - 26 с.
52. Турутина Е. Э. Угроза кибертерроризма: пути противодействия / Е. Э. Турутина // Вестник Российского университета кооперации. – 2021. – № 4(46). – С. 170-174. – EDN YNUUES.
53. Харабара И.В. Объект преступления и его виды // Образование и право, (6), 2020.– С. 318-323.
54. Ушаков С.И. Преступления в сфере обращения компьютерной информации: Теория, законодательство, практика : автореферат дис. ... кандидата юридических наук : 12.00.08 / Кисловод. ин-т экономики и права. - Ростов-на-Дону, 2000. - 30 с.
55. Харламова А.А. (2020). Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы

квалификации. Вестник Уральского юридического института МВД России, (2). – С. 162-167.

56. Хлыстова Н. Б. Террористический акт как угроза общественной безопасности / Н. Б. Хлыстова // Наука. Мысль: электронный периодический журнал. – 2017. – Т. 7. – № 3-1. – С. 107-109.
57. Чекунов И. Г. Киберпреступность: понятие и классификация. // Российский следователь. – 2012. – № 2. – С. 37–44.
58. Чепец С. С. Кибертерроризм как одна из угроз современному миру / С. С. Чепец // Оригинальные исследования. – 2020. – Т. 10. – № 12. – С. 17-21.
59. Шапошников А.А. Криминологическая характеристика личности киберпреступника // Вестник юридического факультета Южного федерального университета, 5 (3-4), 2018. С. 58-63.
60. Charles D. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws [Электронный ресурс]. The Federation of American Scientists. Режим доступа: https://fas.org/sgp/crs/ misc/RS20830.pdf (дата обращения 26.02.2022).
61. Denning D.E. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives [Электронный ресурс]. 2000. May 23. P. 1. URL: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf (дата обращения: 01.04.2022).
62. Grabosky P. Cyberterrorism, Cybercrime and the State. Available at: http://ilearn.mq.edu.au/pluginfile.php/4663825/mod_resource/content/1/Slides.pdf (дата обращения 02.04.2022).
63. Pollitt M. Cyberterrorism: Fact or Fancy? // Computer Fraud and Security [Электронный ресурс]. 1998. No. 2. P. 8–10. URL: https://doi.org/10.1016/S1361-3723(00)87009-8 (дата обращения 04.05.2022).

IV. Материалы судебной практики

64. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: постановление Пленума Верховного Суда РФ от 09.02.2012 № 1» [Электронный ресурс] // Доступ из СПС «КонсультантПлюс» (дата обращения 05.01.2022).
65. Постановление Президиума Верховного Суда Российской Федерации от 2 марта 2022 г. о возобновлении производства по уголовному делу № 165-П21 ввиду новых обстоятельств [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/qJgnnYO1gpHc/ (дата обращения 04.03.2022).
66. Определение Верховного Суда Российской Федерации от 8 апреля 2013 г. по делу № 2-3/13 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/XAlHXF2ab66Q/ (дата обращения 04.03.2022).
67. Определение Верховного Суда Российской Федерации от 23 января 2013 г. по делу № 2-124/12 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/uSlv7669MUUV/ (дата обращения 04.03.2022).
68. Апелляционное определение Верховного Суда Российской Федерации от 15 июля 2019 г. по делу № 2-7/2019 [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/7dR38XH8ELox/ (дата обращения 04.03.2022).
69. Апелляционное определение Верховного Суда Российской Федерации от 14 ноября 2019 г. [Электронный ресурс]. – URL: https://sudact.ru/vsrf/doc/uDVmWyNoFMZ4/ (дата обращения 04.03.2022).
70. Уголовное судопроизводство. Данные о назначенном наказании по статьям УК [Электронный ресурс] // Судебная статистика РФ URL: http://stat.апи-пресс.рф/stats/ug/t/14/s/17(дата обращения 04.03.2022).

IV. Иные источники

71. IT Act 2000 – Penalties, Offences With Case Studies - Checkmate [Электронный ресурс] // Leading Cyber Security Services Provider in US, Middle East, India & South Asia URL:

https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/ (дата обращения 04.03.2022).

72. The Terrorism Act 2006 [Электронный ресурс]. Режим доступа: https://www.gov.uk/ government/publications/the-terrorism-act-2006 (дата обращения 10.03.2022).
73. В Пакистане введена смертная казнь за кибертерроризм. // Новостной аналитический портал Securitylab.ru. Режим доступа: https://www.securitylab.ru/news/362634.php/ (дата обращения 08.03.2022).
74. Кибертерроризм [Электронный ресурс]: Википедия. Свободная энциклопедия. – Режим доступа: https://en.wikipedia.org/wiki/Cyberterrorism (дата обращения: 03.04.2022).
75. Московское дело 3 сторонников «Артподготовки» [Электронный ресурс] // Правозащитный центр «Мемориал» URL: https://memohrc.org/ru/special-projects/moskovskoe-delo-3-storonnikov-artpodgotovki (дата обращения 04.03.2022).
76. Террористический акт в Будённовске - Энциклопедия России [Электронный ресурс]. – URL: https://encyclopaedia russia.ru/article/terroristicheskij-akt-v-budyonnovske/ (дата обращения 04.03.2022).
77. Отчет о видах наказания за совершение преступлений в сфере компьютерной информации:ст.272-274.1 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru (дата обращения 06.02.2022).
78. Отчет о сроках лишения свободы за совершение преступления, предусмотренного ч.1-3 ст.205 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru (дата обращения 06.02.2022).

ПРИЛОЖЕНИЕ 1.

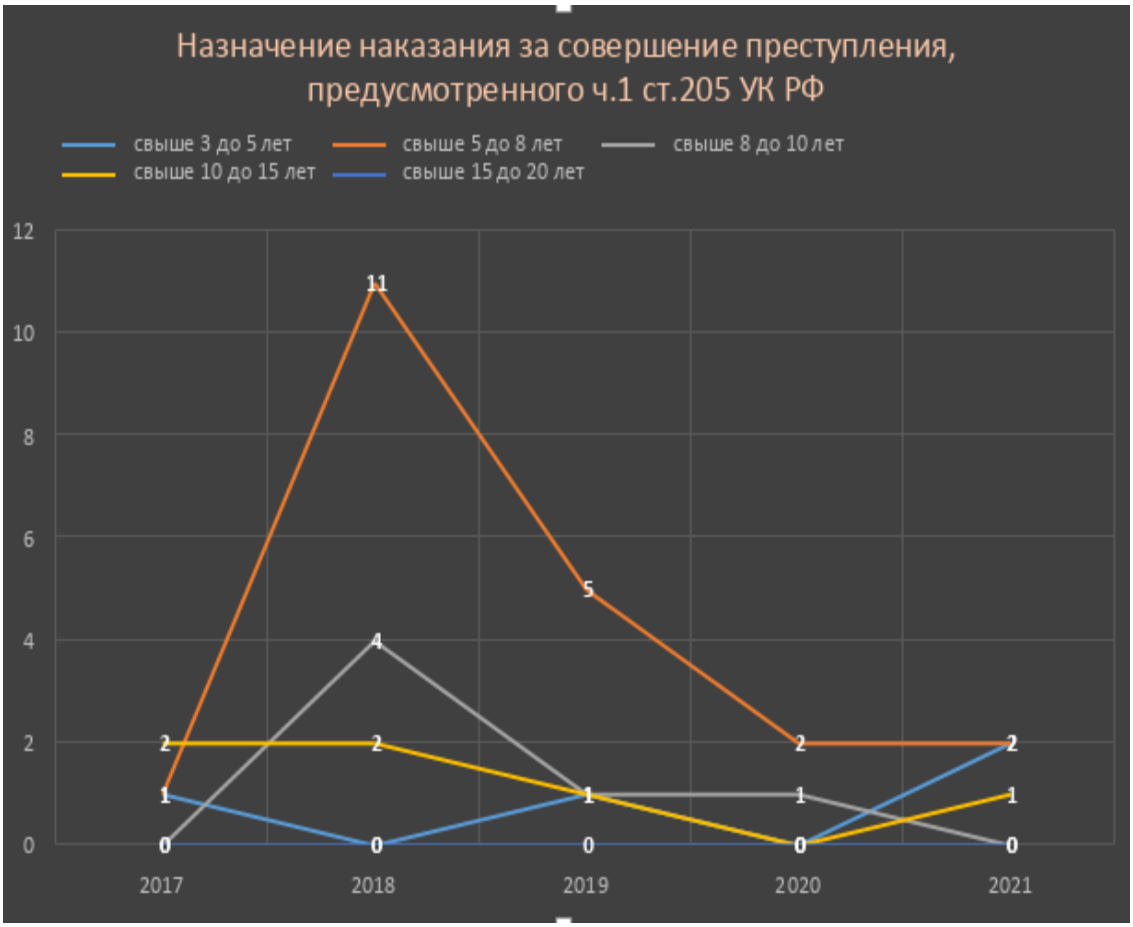

Рисунок 1. Сроки лишения свободы, назначаемые за совершение террористического акта [1]

[1] Отчет о сроках лишения свободы за совершение преступления, предусмотренного ч.1-3 ст.205 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru


Назначение наказания за совершение преступления, предусмотренного ч.2 ст.205 УК РФ
свыше 3 до 5 лет
свыше 5 до 8 лет
свыше 8 до 10 лет
свыше 10 до 15 лет
свыше 15 до 20 лет
16
14
12
10
8
6
4
2
0
2017
2018
2019
2020
2021


Назначение наказания за совершение преступления, предусмотренного ч.3 ст.205 УК РФ
свыше 3 до 5 лет
свыше 5 до 8 лет
свыше 8 до 10 лет
свыше 10 до 15 лет
свыше 15 до 20 лет
9
8
7
6
5
4
3
2
1
0
2017
2018
2019
2020
2021

ПРИЛОЖЕНИЕ 2

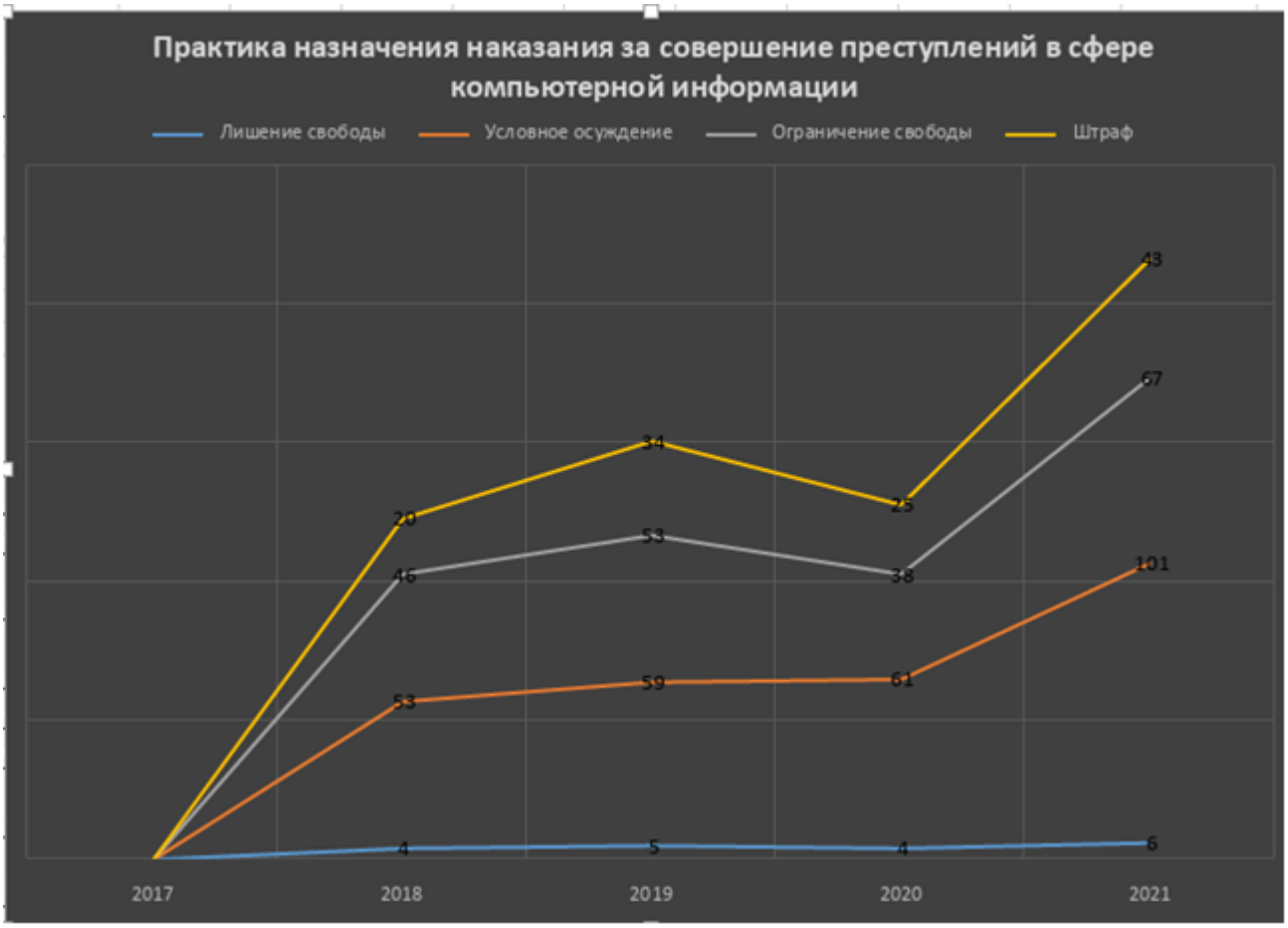

Рисунок 2. Практика назначения наказания за совершение преступлений в сфере компьютерной информации.[1]

[1] Отчет о видах наказания за совершение преступлений в сфере компьютерной информации:ст.272-274.1 УК РФ. Сводные статистические сведения о состоянии судимости [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном суде Российской Федерации URL: http://www.cdep.ru (дата обращения 06.02.2022)

Министерство внутренних дел Российской Федерации
Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра уголовного права

УТВЕРЖДАЮ

Начальник кафедры уголовного права
полковник полиции

_____Куликов Р.С.
(подпись, фамилия, инициалы)
«_30_» _04_____ 2021 г.

ПЛАН-ГРАФИК
выполнения выпускной квалификационной работы

Тема: Уголовная ответственность за совершение кибертерроризма

Курсант (слушатель): Габдрахманова Рамиля Ильшатовна Учебная группа № 071
(фамилия, имя, отчество)

Специальность Правоохранительная деятельность
Форма обучения Очная Год набора 2017

№ п/п	Характер работы (главы, параграфы и их содержание)	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1	Составление и обсуждение плана ВКР	100 %	15.09.2021	Выполнено
2	Сбор, анализ и обобщение учебной и специальной литературы. Изучение диссертационных исследований, в том числе авторефератов диссертаций, статистических данных МВД РФ, МВД РФ по РТ, по теме.	100 %	01.10.2021	Выполнено
3	Введение	100 %	25.10.2021	Выполнено
4	Глава 1. Кибертерроризм как новая глобальная угроза в России и за рубежом: §1.1. Понятие, сущность и формы кибертерроризма	100 %	06.11.2021	Выполнено
5	Глава 1. Кибертерроризм как новая глобальная угроза в России и за рубежом: §1.2. Причины возникновения и условия функционирования кибертерроризма в XXI веке	100 %	20.11.2021	Выполнено
6	Глава 2. Уголовно-правовой анализ	100 %	15.12.2021	Выполнено

	составов статей УК РФ, предусматривающих ответственность за совершение кибертерроризма: §2.1. Юридический анализ объективных признаков составов кибертерроризма по УК РФ			
7	Глава 2. Уголовно-правовой анализ составов статей УК РФ, предусматривающих ответственность за совершение кибертерроризма: §2.2. Юридический анализ субъективных признаков составов кибертерроризма по УК РФ	100%	15.01.2022	Выполнено
8	Глава 2. Уголовно-правовой анализ составов статей УК РФ, предусматривающих ответственность за совершение кибертерроризма: §2.3. Квалифицированные признаки кибертерроризма	100%	30.01..2022	Выполнено
9	Глава 3. Пути совершенствования законодательной системы в противодействии кибертерроризму в России: §3.1. Назначение наказания за совершение кибертерроризма в практике судов Российской Федерации	100%	15.02.2022	Выполнено
10	Глава 3. Пути совершенствования законодательной системы в противодействии кибертерроризму в России: §3.2.Совершенствование законодательства и практики применения следственными и судебными органами норм Уголовного кодекса Российской Федерации об ответственности за кибертерроризм	100%	15.03.2022	Выполнено
11	Заключение	100%	15.04.2022	Выполнено
12	Список использованной литературы	100%	20.04.2022	Выполнено
13	Приложения	100%	25.04.2022	Выполнено

Подпись выпускника _____

«__» _____ 20 __г.

СОГЛАСОВАНО

Научный руководитель:
доцент кафедры уголовного права, к.ю.н.,
доцент
«____»_____202__ г. Д.К. Амирова

Отзыв

о работе обучающейся 071 учебной группы очной формы обучения, 2017 года набора, по специальности 40.05.02 – Правоохранительная деятельность

Габдрахмановой Рамили Ильшатовны

в период подготовки выпускной квалификационной работы

на тему «Уголовная ответственность за совершение кибертерроризма»

Тема выбрана из списка тем, предложенных кафедрой. Габдрахманова Р.И. проявила высокую степень заинтересованности в выборе темы выпускной квалификационной работы, поскольку проблемой уголовной ответственности за совершение кибертерроризма, вопросами их квалификации занимается с 3 курса обучения в КЮИ МВД России.

Габдрахманова Р.И. обосновала заинтересованность в выбранной теме ее актуальностью, наличием эмпирического материала по теме исследования, а также личными мотивами. Тема, выбранная автором, докладывалась на круглых столах, конференциях, являлась темой исследования на конкурсных работах. Кроме того, написан ряд статей по теме исследования.

Соответствие содержания работы заданию полное.

Габдрахманова Р.И. продемонстрировала навыки и умения в формулировании цели и постановке конкретных задач, которые соответствуют теме работы и отражают актуальность выбранной темы исследования.

Структура работы логична, построена таким образом, что позволяет раскрыть наиболее актуальные вопросы темы. Так, работа состоит из введения, трех глав, объединяющих семь параграфов, заключения и списка использованной литературы, приложения.

Во введении автор обосновывает актуальность выбранной темы, формулирует цель, задачи, определяет его объект, предмет, теоретическую, нормативную, методологическую основы, показывает апробацию результатов исследования и т.д.

В первой главе «Кибертерроризм как новая глобальная угроза в России и зарубежом» автор изучил вопросы, связанные с определением сущности, причин возникновения и условий функционирования кибертерроризма.

Во второй главе «Уголовно-правовой анализ составов статей УК РФ, предусматривающих ответственность за совершение кибертерроризма» автор проанализировал составы преступлений в сфере компьютерной информации, и состав преступления, предусмотренного ст. 205 УК РФ, а также проанализировал практику назначения наказания за совершение преступления, предусмотренного, ст. 205 УК РФ и преступлений в сфере компьютерной информации.

В третьей главе «Пути совершенствования законодательной системы в противодействии кибертерроризму в России» Габдрахманова Р.И. определила пути совершенствования законодательной системы в противодействии кибертерроризму в России. В частности, рассмотрела вопросы, связанные с совершенствованием практики применения следственными и судебными органами норм Уголовного кодекса Российской Федерации об ответственности за кибертерроризм, а также иных нормативных правовых актов, регламентирующих вопросы противодействия кибертерроризму.

В работе автор использовала такие методы научного познания, как: диалектический метод, общенаучный (анализ, синтез, системный) и частно-научный (исторический, формально-юридический).

Габдрахманова Р.И. выполнила работу в установленные сроки. Самостоятельно составила план выпускной квалификационной работы, осуществила поиск источников, статистических данных по теме исследования. В процессе подготовки исследования автор осуществлял взаимодействие с научным руководителем. В установленные сроки предоставляла текст работы для проверки, в кротчайшие сроки устраняла замечания.

Габдрахманова Р.И. продемонстрировала способность и умения пользования научной литературой, в том числе профессиональной направленности, навыки к поиску, обобщению, анализу материалов практики. Автор проявила эрудицию, показала хорошую теоретическую подготовку по дисциплинам уголовно-правового цикла, а также ранее изученным предметам, имеющим связь с уголовным правом и темой выпускной квалификационной

работы.

Автор показала способность формулировать собственную точку зрения, навыки и умения работы с законодательными актами, а также обобщению и анализу эмпирического материала по тематике ВКР. В работе отразились умение и навыки Габдрахманова Р.И. в оперировании научными, юридическими терминами и категориями и их применение в процессе написания работы, а также в работе с материалами следственной и судебной практики, способность и умения к проведению анализа статистических данных и их применения в исследовании.

Габдрахманова Р.И. продемонстрировала способность к самостоятельному формулированию обоснованных и достоверных выводов и результатов исследования.

Автор продемонстрировала навыки владения компьютерными методами сбора, хранения и обработки информации, применяемой в сфере профессиональной деятельности. Умение и навыки работы с компьютерными программами (Word, PowerPoint, Excel и т.п.), информационно-справочными ресурсами, работы в системе интернет.

Работа написана грамотно, имеет научный стиль изложения. Тема выпускной квалификационной работы имеет смысловую законченность, тема работы автором раскрыта, цель достигнута, задачи решены. В работе отсутствуют противоречия, имеются четкие авторские выводы по главам, которые соответствуют поставленным целям и задачам, обоснованы, аргументированы и целесообразны.

Оформление работы в целом соответствует предъявленным требованиям ФГОС ВПО по специальности 40.05.02 Правоохранительная деятельность, а также Положению об организации подготовки и защите выпускных квалификационных работ в КЮИ МВД России.

Анализ выводов, сформулированных автором, показывает, что они имеют не только теоретическую, но и практическую значимость. Выводы и предложения, содержащиеся в работе, могут быть использованы в учебном

процессе преподавателями и обучающимися при подготовке дидактического материала: фондовых лекций, планов семинарских и практических занятий, разработке экзаменационных вопросов, а также вопросов для сдачи зачетов. Результаты исследования могут быть использованы в научно-исследовательской деятельности ученых, преподавателей, курсантов и слушателей КЮИ МВД РТ, а также обучающихся иных учебных заведений. Материал может быть полезен в следственной и судебной практике, а также законотворческой деятельности. Данный материал может быть полезен в качестве дополнительной информации всем тем, кто интересуется изучением проблем уголовной ответственности за квалифицированное убийство.

Работа выполнена самостоятельно. Так, проверка текста на процент заимствования в системе «Антиплагиат.вуз» показала, что оригинальность текста составляет – 50,16 %, цитирования- 17,51 %, заимствования – 32,33 %, что соответствует предъявляемым требованиям к оригинальности текста работы.

Выпускная квалификационная работа Габдрахманова Рамили Ильшатовны на тему: «Уголовная ответственность за совершение кибертерроризма» может быть допущена к защите и заслуживает высокой положительной отметки, а ее автор присвоения искомой квалификации.

Научный руководитель:
доцент кафедры уголовного права
Казанского юридического института
МВД России
кандидат юридических наук, доцент
майор полиции _____ Д.К. Амирова
«____» _____2022 г.

С отзывом ознакомлена _____ Р.И. Габдрахманова
«____» _____2022 г.

Подпись Амировой Д.К.
УДОСТОВЕРЯЕТСЯ
Начальник Р КЮИ МВД России

РЕЦЕНЗИЯ

на выпускную квалификационную работу

слушателя 071 учебной группы очной формы обучения, 2017 года набора, по специальности 40.05.02«Правовоохранительная деятельность»

Габдрахмановой Рамили Ильшатовны

на тему: «Уголовная ответственность за совершение кибертерроризма»

Рецензируемая выпускная квалификационная работа выполнена на актуальную тему, поскольку в настоящее время кибертерроризм является наиболее опасной разновидностью киберпреступности. Изучение кибертерроризма, как и киберпреступности в целом, является актуальным направлением и в уголовно-правовой науке, цель которой заключается в совершенствовании уголовного законодательства в сфере борьбы с киберпреступлениями (кибертерроризмом). Данная цель может быть достигнута путем определения уголовно-правовой природы кибертерроризма, закрепления в действующем Уголовном законе норм, предусматривающих ответственность за совершение исследуемого вида киберпреступлений.

Цели и задачи работы соответствуют ее названию. План работы составлен логично, что позволило автору последовательно изложить исследуемый материал. Структура работы обусловлена целью исследования и задачами, которые решались для ее достижения. Работа состоит из введения, трех глав, объединяющих шесть параграфов, заключения, списка использованной литературы, приложения. Исследуемая проблематика по частям работы изложена равномерно.

Структура выпускной квалификационной работы соответствует содержанию. Во введении дипломной работы автором обосновывается актуальность исследуемой темы, характеризуется ее теоретическая разработанность, указаны объект и предмет исследования, обозначены цели и задачи, эмпирическая и нормативная база, описаны методология и научная

новизна исследования, а также обосновывается практическая значимость данной работы.

Первая глава посвящена рассмотрению вопросов, связанных с определением сущности, причин возникновения и условий функционирования кибертерроризма.

Вторая глава посвящена противодействию кибертерроризму в России средствами Уголовного закона. В главе дается юридический анализ состава преступления, предусмотренного, ст. 205 УК РФ, анализируется практика назначения наказания за совершение преступления, предусмотренного, ст. 205 УК РФ.

Третья глава посвящена определению путей совершенствования законодательной системы в противодействии кибертерроризму в России. В частности, рассматриваются вопросы, связанные с совершенствованием практики применения следственными и судебными органами норм Уголовного кодекса Российской Федерации об ответственности за кибертерроризм, а также иных нормативных правовых актов, регламентирующих вопросы противодействия кибертерроризму.

В заключении сформулированы выводы и предложения по рассмотренной теме исследования.

В приложении представлен результат анализа практики назначения наказания за совершение преступления, предусмотренного ч.1-3 ст. 205 УК РФ.

Степень научности, глубина теоретического анализа проблемы высокая. Автор выпускной квалификационной работы правильно в работе расставляет акценты, анализирует значительный массив нормативно-правовых актов, учебных пособий, монографий и публикаций, содержащих понятие кибертерроризма, определяющих его сущность, основные черты.

При выполнении дипломной работы автор использовал достаточное количество нормативных правовых актов, учебных пособий, монографий и публикаций, материалов судебно-следственной практики.

В работе присутствуют выводы и заключения, к которым автор пришел самостоятельно, изучая заявленную тему.

Практическая направленность работы заключается в том, что на основе изученного материала в процессе выполнения выпускной квалификационной работы, автор делает самостоятельные выводы и заключения, а также формулирует предложения по совершенствованию действующего уголовного законодательства в сфере ответственности за совершение кибертерроризма и практики его применения.

Полнота использования нормативных актов и других литературных источников. Автор при написании работы использовал достаточное количество литературы и нормативной правой базы.

Степень решения слушателем поставленных задач. Слушатель в достаточной степени решил поставленные перед ним задачи и достиг цели исследования.

Оформление выводов и заключения. Выводы и заключения, сделанные автором, соответствуют логике изложения материала, а также целям и задачам, поставленным при выполнении работы.

В то же время у рецензента имеется ряд замечаний, которые можно рассматривать в качестве пожеланий для будущего исследования. Проводя анализ видов составов киберпреступлений, автор подробно остановился на анализе состава ст. 205 УК РФ, а также компьютерных преступлений. По мнению рецензента интересно было бы узнать мнение автора относительно иных статей, предусматривающих ответственность за террористические преступления (ст.ст. 205.1-207 УК РФ). Данная рекомендация не снижает ценности проведенного исследования и не меняет положительного мнения рецензента о проделанной работе.

Заключение о соответствии работы предъявляемым требованиям и предложения об оценке. Представленная на рецензирование выпускная квалификационная работа соответствует предъявляемым требованиям, может

быть допущена к защите, заслуживает высокой положительной оценки, а ее автор присвоения искомой квалификации.

Рецензент:

Начальник отделения по раскрытию преступлений, совершенных с использованием информационно- телекоммуникационных технологий ОУР Управления МВД России по г.Казани
старший лейтенант полиции В.М. Алиев

«__»_____ 2022 г.

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Казанский юридический институт МВД России

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Габдрахманова Рамиля Ильшатовна
Самоцитирование рассчитано для: Габдрахманова Рамиля Ильшатовна
Название работы: Уголовная ответственность за совершение кибертерроризма
Тип работы: Выпускная квалификационная работа
Подразделение: кафедра уголовного права

РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

ЗАИМСТВОВАНИЯ		33.1%	ЗАИМСТВОВАНИЯ		32.33%
ОРИГИНАЛЬНОСТЬ		49.39%	ОРИГИНАЛЬНОСТЬ		50.16%
ЦИТИРОВАНИЯ		17.51%	ЦИТИРОВАНИЯ		17.51%
САМОЦИТИРОВАНИЯ		0%	САМОЦИТИРОВАНИЯ		0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 26.04.2022

ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 26.04.2022 21:19

Модули поиска: ИПС Адилет; Библиография; Сводная коллекция ЭБС; Интернет Плюс; Сводная коллекция РГБ; Цитирование; Переводные заимствования (RuEn); Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по Интернету (EnRu); Переводные заимствования издательства Wiley (RuEn); eLIBRARY.RU; СПС ГАРАНТ; Модуль поиска "КЮИ МВД РФ"; Медицина; Сводная коллекция вузов МВД; Диссертации НББ; Перефразирования по eLIBRARY.RU; Перефразирования по Интернету; Патенты СССР, РФ, СНГ; Коллекция СМИ; Шаблонные фразы; Кольцо вузов; Издательство Wiley

Работу проверил: Амирова Диляра Кафилевна, к.ю.н., доцент, доцента кафедры уголовного права КЮИ МВД России

ФИО проверяющего

Дата подписи:

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

с проверкой ознакомлена