УДК 343.7

КИБЕРТЕРРОРИЗМ: ПОНЯТИЕ, ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Ю.Е. Паламарчук

магистрант направления подготовки 40.04.01 Юриспруденция,

ЧОУ ВО ЮУ (ИУБиП), e-mail: palamarchuk.elena76@mail.ru

Научный руководитель: Фоменко А.И., к.ю.н., доцент.

Аннотация: Статья посвящена рассмотрению вопросов, затрагивающих легальное определение «кибертерроризма», а также будут рассмотрены некоторые способы совершения преступлений в сфере террористической направленности, а также проблемы противодействия терроризму.
Ключевые слова: кибертерроризм, определение, компьютерные преступления, кибертеракт, террористический акт, Уголовный кодекс Российской Федерации.

CYBERTERRORISM: CONCEPT, PROBLEMS OF COUNTERACTION

Y. E. Palamarchuk

Abstract: The article is devoted to the consideration of issues affecting the legal definition of «cyberterrorism», as well as some ways of committing crimes in the sphere of terrorist orientation, as well as problems of countering terrorism.
Keywords: cyberterrorism, definition, computer crimes, cyberattack, terrorist act, criminal code of the Russian Federation.

На сегодняшний день, современный мир очень трудно представить без информационных технологий, несмотря на то, что еще десятки лет назад человечество и понятия не имело о них. Сегодня же, информационные технологии плотно вошли во все сферы нашей жизни. Следовательно, если появляются новые технологии, то и появляются новые виды преступлений, направленные на посягательство таких общественных отношений, как сфера высоких технологий.

На данный момент Уголовный кодекс Российской Федерации (далее-УК РФ) закрепляет несколько видов преступлений террористической направленности[1]:

1. террористический акт (статья 205);
2. содействие террористической деятельности (статья 205.1);

3. публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (статья 205.2);

4. заведомо ложное сообщение об акте терроризма (статья 207).

Данные виды преступлений террористической направленности являются самыми коварными в истории человечества, т.к. всегда наносят большой вред как обычным людям, так и государству в целом.

В повседневной жизни, мы очень часто стали сталкиваться с таким понятием как компьютерный терроризм, еще чаще его называют «кибертерроризм». Что же понимается под таким понятием?

Кибертерроризм – это совокупность противоправных действий в киберпространстве, с использованием компьютерных и (или) телекоммуникационных технологий (в основном в информационно-телекоммуникационной сети «Интернет») в террористических целях, совершение которых, создает угрозу безопасности личности, общества и государства[2].

Впервые термин «компьютерный терроризм» был представлен старшим научным сотрудником Института безопасности и разведки Барри Коллином в 1980 году. Именно Барри Коллин впервые попытался использовать этот термин в контексте тенденции к переходу терроризма из физического в виртуальный мир, возрастающего пересечения и срастания этих миров.

Так какие же цели преследует в себе «кибертерроризм»? Попробуем определить некоторые из них:

1. взлом компьютерных устройств и (или) систем и получение доступа к различным данным конфиденциальной информации

2. вывод из строя оборудования и различного программного обеспечения либо создание помех для его работы

3. кража данных с помощью взлома компьютерных систем, вирусных атак

4. утечка важной государственной конфиденциальной информации в открытый доступ

5. нарушение работы каналов связи[3, с.66].

Чтобы достичь желаемых целей, кибертеррористы применяют специальное программное обеспечение, используемое для взлома компьютерных систем компаний и организаций, проводят атаки на удаленные сервера компаний и организаций.

Сейчас, по мнению многих ученных, «кибертерроризм» является не менее опасным, нежели ядерный или бактериологический, поскольку большая часть нашей жизни сокрыта в виртуальном пространстве.

В Российской Федерации, на данный момент такой термин как «кибертерроризм» легально не закреплен в единственном источнике уголовного права – УК РФ, следовательно, и его возможные определения рассматриваются весьма слабо.

По мнению к.ю.н., доцента В. А. Покровского под кибертерроризмом понимается преднамеренная и четко спланированная атака, посягающая на информацию, которая обрабатывается компьютером или компьютерной сетью, и которая создает опасность жизни и здоровью людей либо наступлением других тяжких последствий, но при условии, если такие последствия были совершены с целью нарушить общественную безопасности, запугать население либо спровоцировать военный конфликт[6].

Каждое представленное определение, по своей сути и характеристики является правильным, но необходимо разработать такое, которое бы имело закрепленную юридическую трактовку в Федеральном законе.

По своей правовой природе преступления, совершенные в киберпространстве - это виновное противоправное деяние (вмешательство) в работу компьютеров, компьютерных программ либо сетей, а также иные противоправные действия, совершаемые с помощью либо по средствам компьютера, либо компьютерной сети[4].

В свою очередь, под термином «кибертеракт» понимается активные действия по дезорганизации информационных сетей, которые устрашают население и создают серьезную опасность гибели человека либо причиняют другие тяжкие последствия в целях оказания влияния на органы государственной власти, либо международные организации в собственных целях.

Данная область совершения таких преступлений, в силу своей новизны, изучается довольно медленными темпами и возникают множество проблем и вопросов, связанных с противодействием таким видам преступлений.

Для начала хочется сказать конкретно о средствах и способах совершения преступления. Если брать террористический акт в классическом его проявлении, то здесь будет понятно, что в качестве орудия совершения преступления будут использованы взрывчатка или обычное стрелковое оружие, а вот кибертеракт, будет совершен с использованием информационных технологий, что достаточно сложно проследить и предотвратить на данный момент.

Главным способов совершения террористического акта в сфере высоких технологий, т.е. на просторах киберпространства - является атака на компьютерную информацию, профессиональную аппаратуру передачи данных, и иные составляющие информационных систем. Именно такая атака позволит проникнуть в атакуемую информационную систему, перехватывать управление или подавить нужную информационную среду для достижения желаемой преступной цели [5, С.510-515].

Еще одной значимой проблемой в противодействии кибертерроризму является тотальная нехватка квалифицированных специалистов в этой области. Следовательно, обычному работнику правоохранительных органов просто не хватает навыков, для того чтобы оказать должное сопротивление такой кибератаке. Для того, чтобы решить такую проблему, необходимо на базах высших образовательных учреждений организовать специальный профиль, который будет направлен на обучение нужных для

противодействия таким видам преступлений как кибертерроризм [7, С.546-551].

Таким образом, высокотехнологичные террористические акции новой эпохи способны сегодня продуцировать системный кризис всего мирового сообщества и поставить под угрозу существование отдельных регионов мира, что не было характерно для традиционных террористических актов.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от. 27.10.2020 года) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 13.12.2020).
2. Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. – Режим доступа: www. crime-research.ru, свободный (дата обращения: 13.12.2020).
3. Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. – М.: ЮИ МВД РФ, 2020. – 66 с.
4. Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2019: угрозы и нейтрализация [Электронный ресурс]. – Режим доступа: http://www.crimeresearch.ru/articles/vagif, свободный (дата обращения: 13.12.2020).
5. Кунделеев С.В., Коханова В.С. Криминологические аспекты совершенствования системы противодействия преступности в сети Интернет // Интеллектуальные ресурсы – региональному развитию. – 2020. – №2. – С. 510-515.
6. Покровский В.А. Кибертерроризм – угроза национальной безопасности [Электронный ресурс]. – Режим доступа: www.crive-research.ru, свободный (дата обращения: 13.12.2020).
7. Семиёхин В.А. Проблемы использования уголовного права России в условиях развития цифровой экономики // Интеллектуальные ресурсы – региональному развитию. – 2020. – №2. – С. 546-551.