УДК 343 **DOI 10.34670/AR.2019.89.8.016**

Кибертерроризм – актуальная проблема современного общества

Камергоев Беслан Мухамедович

Лейтенант полиции,
преподаватель кафедры деятельности ОВД в особых условиях,
Северо-Кавказский институт повышения квалификации
сотрудников МВД России (филиал),
Краснодарский университет МВД России,
360016, Российская Федерация, Нальчик, ул. Мальбахова, 123;
e-mail: Beslan_Kamergoev@mail.ru

Аннотация

Мы живем в эпоху информационного общества, когда информация становится необходимой для нормального функционирования всего общества. Развитие сети Интернет позволило людям передавать огромные потоки информации на расстояния, что предоставило людям новые реальности – от возможности общаться и видеть друг друга, находясь в разных точках земного шара, до объединения усилия целых исследовательских групп, которые, находясь в разных странах и даже на разных континентах, могут работать слаженно и эффективно. Однако сеть Интернет используется не только во благо. Огромными темпами во всем мире растет такое явление, как киберпреступность. Среди всех киберпреступлений особую опасность представляет деятельность террористических групп в сети Интернет. Появляется все больше сайтов террористической направленности, через которые происходит вербовка новых членов в террористические группы, распространяются видео экстремистского содержания и т. д. Перед террористическими актами, которые совершаются посредством сети Интернет, уязвимы все сферы жизнедеятельности общества и государства, в которых активно применяются информационные технологии.

Для цитирования в научных исследованиях

Камергоев Б.М. Кибертерроризм – актуальная проблема современного общества // Вопросы российского и международного права. 2019. Том 9. № 8А. С. 121-126. DOI 10.34670/AR.2019.89.8.016

Ключевые слова

Интернет, терроризм, кибертерроризм, кибероружие, кибератака.

Введение

Современный этап развития мирового сообщества характеризуется стремительным развитием научно-технического прогресса, в который включается и сфера высоких технологий [Байгускарова, 2015; Бечелов, Абазова, Курманова, 2015]. Сегодня с помощью компьютерной техники происходит управление полетами гражданской и военной авиации, железнодорожными транспортными потоками, технологическими процессами на гидро- и атомных электростанциях, обработкой финансовых документов и электронных платежей, проверкой качества продуктов питания или очистки вод. Вычислительные системы используются для хранения информации, будь то финансовый годовой отчет компании или архивы служб, обеспечивающих национальную безопасность.

Основная часть

В мире, где постоянно растет количество персональных компьютеров и пользователей сети Интернет, неминуемо повышается и количество преступлений, совершаемых с использованием вычислительной техники, т. е. речь уже идет о киберпреступности и одной из ее форм – кибертерроризме [Наговицин, Наговицин, Соловьев, 2012]. Арсенал компьютерных террористов – различные вирусы, логические бомбы, команды, заранее встроенные в программу и срабатывающие в нужный момент. Современные террористы используют Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие [Байгускарова, 2015].

Термин «кибертерроризм» относительно молод и образован сочетанием (слиянием) двух слов: киберпространство и терроризм. И поэтому требует корректного определения.

В большинстве случаев многие средства массовой информации отождествляют термин «кибертерроризм» с понятием «хакер» и «кибертеррорист». Это неправильно. Терроризм – это преступление, но не каждое преступление есть терроризм, и кибертеррориста, как правило, можно назвать хакером, но не всякий хакер совершает теракты в киберпространстве или с помощью компьютера [Голубев, www; Наговицин, Наговицин, Соловьев, 2012].

Обращаясь к ст. 205 УК РФ, приведем определение терроризма: «совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями».

Кибертерроризм, в свою очередь, можно определить как умышленную атаку на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Это деяние, совершаемое в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти. Таким образом, налицо схожие определения [Наговицин, Наговицин, Соловьев, 2012].

Что касается природы кибертерроризма, то он качественно отличается от общепринятого понятия терроризма, сохраняя лишь стержень этого явления и основные признаки – выдвижение

разного рода требований к властным структурам и попытка их достижения путем противоправных насильственных действий. Сегодня кибертеррорист, находясь практически в любой точке земного шара, может нанести больший вред, используя в своем преступном арсенале компьютерную технику, нежели «традиционный» террорист, использующий взрывное устройство (например, бомбу) или отравляющие вещества.

На сегодняшний день на счету кибертеррористов успешные атаки на сайты различных органов власти и управления, британский спутник связи, центр управления полетами НАСА в Гринбелте, штат Мериленд, энергосеть США, систему управления ПВО Ирака, ряд банковских систем и др. Это говорит о том, что в арсенале киберзлоумышленников в настоящее время имеются достаточно эффективные, успешно апробированные на практике методы, способы и средства проникновения к информационным ресурсам и программно-аппаратным средствам самого разного назначения, в том числе объектам и сетям жизнеобеспечения. При наличии такого разнообразия кибероружия вполне можно ожидать кибератаков, направленных против действующей власти, банковской и коммерческой систем, электронного сервиса, управляемых компьютером инфраструктур, например газо- и нефтепроводов, электрических сетей, систем контроля за наземным и воздушным транспортом, телефонных систем, сферы здравоохранения, оборонных систем коммуникации и снабжения [Богорад, www; Наговицин, Наговицин, Соловьев, 2012].

Совершение указанных действий преследует следующие цели:

– принуждение их принять выгодные для террористов решения;
– дестабилизация общественно-политической обстановки за счет устрашения населения либо посягательства на личную безопасность государственного или общественного деятеля;
– осложнение международных отношений как следствие воздействия на используемые ими транспортные средства, линии связи и банки данных [Матвиенко, 2011; Наговицин, Наговицин, Соловьев, 2012; Шогенов, 2017].

Таким образом, на сегодняшний день мы наблюдаем тенденцию к увеличению кибератак и кибертерроризма. И обусловлено это прежде всего отсутствием четкого юридического определения и осмысления данного явления, в то время как в числе участников кибертеррористической деятельности, кроме кибертеррористов-одиночек и кибертеррористических организаций, можно назвать и целые государства, занимающиеся кибертерроризмом. Кибертерроризм постепенно становится одним из стратегических орудий, нацеленных на разрушение и ослабление политической, экономической, военной мощи страны, тем более что кибертерроризм является относительно недорогим средством для осуществления стратегических целей государства, где основными мишенями кибертеррориста будут являться вычислительные системы, управляющие различными процессами, и циркулирующая в них информация (особенно он выгоден странам с низким уровнем жизни, где за неимением другого оружия кибертерроризм остается единственным средством осуществления террора).

В тактике кибертерроризма, как и при простом терроре, необходимо, чтобы киберпреступление имело опасные последствия, стало широко известно населению, получило большой общественный резонанс и создавало атмосферу угрозы повторения подобного акта без указания конкретного объекта атаки. В условиях информационного общества ожидать кибертеракт можно где угодно. Теоретически возможно блокировать работу, например, метрополитена любого из крупных городов или нарушить график движения пригородных электропоездов; так как основная масса населения добирается до места работы на метро или на

электричке, на некоторое время город будет попросту парализован. Вполне возможными представляются проникновение в локальные сети, изменение или уничтожение информации, блокирование работы компьютеров какого-либо государственного учреждения или предприятия. Нарушение работы электроподстанций может повлечь за собой повсеместное отключение электроэнергии и, как следствие, сбои в работе или отключение компьютерных систем связи и управления. Нарушение работоспособности структур финансовой системы страны может привести к резкому социальному напряжению и ухудшению экономической ситуации в отдельном регионе или стране в целом [Дроздов, Егозарьян, 2004].

Уже сегодня, по заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, 48% компаний и 50% банков потерпят крах в течение нескольких суток. Разорение компаний и банков нанесет урон не только владельцам, работникам и вкладчикам, но и экономике страны.

До недавнего времени информационная инфраструктура России не представлялась сколько-нибудь уязвимой в отношении рассматриваемых террористических актов [Камергоев, 2018]. Причинами этого можно считать низкий уровень ее развития и наличие значительной доли неавтоматизированных операций при осуществлении процесса управления. Вместе с тем в последние годы многие государственные и коммерческие структуры приступили к активному техническому переоснащению своих предприятий, организаций. Информационная составляющая таких организаций реализуется практически исключительно на технических и программных средствах иностранного производства, что в определенной степени повышает угрозу успешных атак со стороны кибертеррористов [Байгускарова, 2015; Васенин, www].

Заключение

Последствия от кибертеракта могут быть весьма разнообразными: от снижения уровня жизни и гибели людей до полного экономического разорения государства. В связи с этим необходимо закрепить на государственном уровне обязанность государственных структур по разработке и внедрению технических, правовых и организационных мер, обеспечивающих защиту компьютерных сетей как одного из уязвимых элементов современного российского общества.

Библиография

1. Байгускарова Э.И. Кибертерроризм как угроза информационной безопасности // Материалы внутривузовской конференции «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи». Магнитогорск, 2015. С. 48-55.
2. Бечелов З.Ш., Абазова М.В., Курманова М.К. Противодействия современному терроризму // Материалы Всероссийской научно-практической конференции преподавателей, аспирантов, магистрантов и студентов «Актуальные проблемы и приоритетные инновационные технологии развития АПК региона». Нальчик, 2015. С. 325-327.
3. Богорад Е. Искусство войны II: стратегия // Популярная механика. 2003. № 9. URL: https://www.popmech.ru/weapon/8509-iskusstvo-voyny-ii-strategiya/#part0
4. Васенин В.А. Информационная безопасность и компьютерный терроризм. URL: http://www.crime-research.ru/articles/vasenin
5. Голубев В.А. Кибертерроризм – угроза национальной безопасности. URL: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism
6. Дроздов Ю., Егозарьян В. Мировая террористическая… М.: Бумажная галерея, 2004. 388 с.
7. Камергоев Б.М. Особенности распространения молодежного экстремизма // Социально-политические науки.

2018. № 3. С. 54-56.
8. Матвиенко Ю.А. Предупредить – значит вооружить (кибертерроризм вчера, сегодня и завтра) // Информационные войны. 2011. № 2. С. 60-70.
9. Наговицин А.И., Наговицин К.А., Соловьев С.В. Кибертерроризм как новая форма терроризма // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2012. № 1-2. С. 101-104.
10. О противодействии терроризму: федер. закон Рос. Федерации от 06.03.2006 № 35-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 26.02.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 01.03.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_58840/
11. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24.05.1996: одобр. Советом Федерации Федер. Собр. Рос. Федерации 05.06.1996. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
12. Шогенов Т.М. О некоторых вопросах противодействия экстремизму в сети Интернет // Пробелы в российском законодательстве. 2017. № 3. С. 58-59.

Cyberterrorism as a pressing problem of modern society

Beslan M. Kamergoev

Police Lieutenant,
Lecturer at the Department of the activities of internal affairs bodies under special conditions,
North Caucasus Institute of Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation (branch),
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation,
360016, 123 Malbakhova st., Nalchik, Russian Federation;
e-mail: Beslan_Kamergoev@mail.ru

Abstract

The article aims to view cyberterrorism as a pressing problem of modern society. We live in the age of the information society, when information becomes essential for the normal functioning of the entire society. The author of the article pays attention to the fact that the development of the Internet has allowed people to transmit huge flows of information over distances, which has provided people with new realities – from being able to communicate and see each other from different parts of the world to bringing together the efforts of entire research groups that can work in a coherent and effective manner from different countries and even continents. However, the Internet is not only used for good purposes. The article points out that the phenomenon of cybercrime is growing at an enormous rate around the world. Among all types of cybercrime, the activities of terrorist groups on the Internet are considered to be particularly dangerous. The sites of terrorist groups are increasingly emerging, through which new members are recruited, videos of extremist content are distributed, etc. Terrorist acts committed through the Internet have an impact on all the spheres of society and states, in which information technologies are actively used, including the Russian Federation.

For citation

Kamergoev B.M. (2019) Kiberterrorizm – aktual'naya problema sovremennogo obshchestva [Cyberterrorism as a pressing problem of modern society]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (8A), pp. 121-126. DOI 10.34670/AR.2019.89.8.016

Keywords

Internet, terrorism, cyberterrorism, cyberweapons, cyberattack.

References

1. Baiguskarova E.I. (2015) Kiberterrorizm kak ugroza informatsionnoi bezopasnosti [Cyberterrorism as a threat to information security]. *Materialy vnutrivuzovskoi konferentsii "Informatsionnaya bezopasnost' i voprosy profilaktiki kiberekstremizma sredi molodezhi"* [Proc. Conf. "Information security and the prevention of cyber-extremism among young people"]. Magnitogorsk, pp. 48-55.
2. Bechelov Z.Sh., Abazova M.V., Kurmanova M.K. (2015) Protivodeistviya sovremennomu terrorizmu [Counteraction to modern terrorism]. *Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii prepodavatelei, aspirantov, magistrantov i studentov "Aktual'nye problemy i prioritetnye innovatsionnye tekhnologii razvitiya APK regiona"* [Proc. Conf. "Topical problems and priority innovative technologies of the development of agribusiness in the region"]. Nalchik, pp. 325-327.
3. Bogorad E. (2003) Iskusstvo voiny II: strategiya [The art of war 2: the strategy]. *Populyarnaya mekhanika* [Popular mechanics], 9. Available at: https://www.popmech.ru/weapon/8509-iskusstvo-voyny-ii-strategiya/#part0 [Accessed 15/07/19].
4. Drozdov Yu., Egozar'yan V. (2004) *Mirovaya terroristicheskaya…* [Global terrorist…] Moscow: Bumazhnaya galereya Publ.
5. Golubev V.A. *Kiberterrorizm – ugroza natsional'noi bezopasnosti* [Cyberterrorism as a threat to national security]. Available at: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism [Accessed 15/07/19].
6. Kamergoev B.M. (2018) Osobennosti rasprostraneniya molodezhnogo ekstremizma [The features of the spread of youth extremism]. *Sotsial'no-politicheskie nauki* [Sociopolitical sciences], 3, pp. 54-56.
7. Matvienko Yu.A. (2011) Predupredit' – znachit vooruzhit' (kiberterrorizm vchera, segodnya i zavtra) [To warn is to arm (cyberterrorism yesterday, today and tomorrow)]. *Informatsionnye voiny* [Information wars], 2, pp. 60-70.
8. Nagovitsin A.I., Nagovitsin K.A., Solov'ev S.V. (2012) Kiberterrorizm kak novaya forma terrorizma [Cyberterrorism as a new form of terrorism]. *Voprosy oboronnoi tekhniki. Seriya 16: Tekhnicheskie sredstva protivodeistviya terrorizmu* [Issues of defence engineering. Series 16: Technical means of counter-terrorism], 1-2, pp. 101-104.
9. *O protivodeistvii terrorizmu: feder. zakon Ros. Federatsii ot 06.03.2006 № 35-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 26.02.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 01.03.2006* [On counteraction to terrorism: Federal Law of the Russian Federation No. 35-FZ of March 6, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_58840/ [Accessed 15/07/19].
10. Shogenov T.M. (2017) O nekotorykh voprosakh protivodeistviya ekstremizmu v seti Internet [On some issues of combating extremism on the Internet]. *Probely v rossiiskom zakonodatel'stve* [Gaps in Russian legislation], 3, pp. 58-59.
11. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon Ros. Federatsii ot 13.06.1996 № 63-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 24.05.1996: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 05.06.1996* [Criminal Code of the Russian Federation: Federal Law of the Russian Federation No. 63-FZ of June 13, 1996]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/ [Accessed 15/07/19].
12. Vasenin V.A. *Informatsionnaya bezopasnost' i komp'yuternyi terrorizm* [Information security and cyberterrorism]. Available at: http://www.crime-research.ru/articles/vasenin [Accessed 15/07/19].