Секция «Глобальная безопасность»

Компьютерный терроризм как новейшая угроза глобальной безопасности

Научный руководитель – Комарова Людмила Валерьевна

Андрюшина Дарья Валериевна
Студент (бакалавр)
Донецкий национальный университет, Исторический факультет, Кафедра международных отношений и внешней политики, Донецк, Украина
E-mail: da0907rina@gmail.com

Современное развитие человеческого общества характеризуется высокой степенью развития научно-технического прогресса, под которым понимается область высоких технологий. Но нельзя не отметить тот факт, что с развитием компьютерных технологий стало возникать такое явление, как компьютерный терроризм или кибертерроризм, или киберпреступность. Профессионалы уверяют нас, что такой вид терроризма не является менее опасным, чем терроризм в привычных нам формах, или, например, бактериологический терроризм [1].

Так называемое «вооружение» компьютерных террористов - это вирусы, программы, которые внедрены в компьютер заранее и готовы быть применены в любой момент независимо от того, где находится непосредственный исполнитель. На данный момент человеческое общество не сможет представить свой обычный рабочий день без гаджетов, которые, по мнению многих, не могут представлять ни малейшей угрозы.

Можно встретить множество определений таких понятий, как копьютерный терроризм, кибертерроризм. В основном, многие исследователи сходятся в том мнении, что это противозаконные действия с использованием информационных технологий, особенно с использованием глобальной сети с целью привлечения умышленного вреда и для достижения террористических целей. В настоящее время лишь немногие из систем могут быть надежно защищены от цифрового терроризма [2].

Можно отметить, что, во-первых, кибертерроризм имеет своей формой информационное поражение, т.е. в своем арсенале использует компьютерные сети, во-вторых, нет необходимости находится в момент совершения данного террористичесого акта рядом с местом происшествия, в-третьих, такой вид терроризма наносит колоссальный материальный ущерб, хотя сам по себе может быть не столь затратным.

Социальные сети, которые охватили и заполнили собой почти все информационное пространство, являются отправной точкой для террористов, использующих глобальные сети в своих интересах. Социальные сети предоставляют террористам огромный поток информации и неограниченное количество ресурсов, а именно тот слой общества, который более всего подвержен всяческим новшествам и изменениям. И это молодежь: студенты, школьники и многие другие. Они в большей степени привязаны к технологиям и их легче вовлечь в какую-либо преступную деятельность, которая, на первый взгляд, даже может такой и не показаться. Ведь было уже достаточно много случаев, когда вербовка в самые известные террористические организации имела место быть в обыкновенных социальных сетях, которыми пользуемся и мы с вами [2].

Многие террористические организации уже давно имеют свои сайты или же страницы в сети интернет. Они объявляют о том что берут на себя ответственность за тот или иной теракт именно в глобальной сети. Их поддержка также оформляется с помощью компьютерных технологий, например финансовая или поддержка иного рода.

Существуют информационные атаки высокого уровня. Их можно подразделить на две группы:

· Нарушение работы или полное выведение из строя информационных систем. Такие действия являются наиболее распространенными, в основном, он нацелены на временную остановку работы тех или иных информационных систем с целью внедрения различных вирусных программ, возможно на какие-либо производства, например биологической промышленности или ядерной.

· Хакерские атаки разрушительной силы. Направлены против информационных систем в целом для их разрушения и уничтожения всяческой информации, программ, данных, разработок. В наихудших сценариях такие атаки имеют все возможности нанести ущерб равноценных привычным нам террористическим актам, которые могут быть осуществлены при помощи бомбы [3].

Научно-технические достижение, разработки, инновации, различные программные технологии, разработанные в эпоху глобализации представляют собой лакомый кусок для кибертеррористов. Все то, что на данный момент разрабатывается или уже разработано, должно находиться под строгим информационным запретом и защитой. С помощью новых технологий террористы совершают теракты с все большим размахом, в котором с каждым разом может погибать все большее количество людей. С каждый новый шаг в положительном развитии человечества несет за собой и новый шаг в развитии кибертерроризма, ведь на каждое действие есть свое противодействие.

Источники и литература

1) Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/articles/vasenin

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

3) Голубев В.А. Кибертерроризм – понятие, терминология, противодействие [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/articles/Golubev0804/3