Ахмадеева Елена Владимировна,

старший преподаватель кафедры общей психологии;

Додух Тамара Сергеевна,

магистр,

ФГБОУ ВО «Башкирский государственный университет»,

г. Уфа. Республика Башкортостан, Россия

КИБЕРТЕРРОРИЗМ И ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ЛИЧНОСТИ ТЕРРОРИСТА

Аннотация. В статье обозначены основные понятия о компьютерных преступлениях и информационных атаках, возможностях виртуального пространства для преступных действий, а также характеристика личности компьютерного преступника.

Ключевые слова: кибертерроризм, хакер, киберпреступник, виртуальное пространство, интернет.

Жизнь современного человеческого общества все больше перетекает в виртуальное пространство, которое представляет собой «пространство, созданное компьютерной системой, как обозначение всего диапазона информационных ресурсов, доступных через компьютерные сети» [1]. В настоящее время Интернет – это постоянно растущее и видоизменяющееся информационное пространство: сайтов-новостей разных тематик и мнений, сайтов государств и отдельных личностей, госучреждений и частных компаний, социальных сетей, платежных систем и банков, «облачных» онлайн-хранилищ, вмещающих террабайты информации: от мультимедийных файлов до секретной информации. Повсеместное использование интернета в деловых и личных целях ведет к тому, что многие сферы современной жизни прочно основываются в виртуальном пространстве, которое становится местом повышенной опасности для его пользователей [3, с. 242].

Целью данной статьи является определение основных причин, способствующих развитию и росту преступлений в виртуальном пространстве, а также выделение особенностей личности, предрасположенной к киберпреступлениям.

Актуальность данной работы обуславливается тем, что виртуальное пространство занимает неотъемлемую часть жизни современного общества, в связи с чем, любой пользователь сети интернет может стать жертвой различных преступлений.

Виртуальное пространство, являясь продолжением пространства реального, несет те же угрозы, предоставляя обширные возможности для краж, взломов, саботажа и провокации со стороны людей, обладающих умениями и навыками по проникновению в чужое виртуальное пространство посредством хакерства. Существуют разные трактовки термина «хакер», наиболее точное, по нашему мнению, определение приводится на сайте Лаборатории Касперского: «Хакерами называют тех, кто получает или пытается получить незаконный доступ к данным через компьютерные сети (обычно через Интернет)» [6].

Интернет является источником получения практически любых необходимых данных и сведений, в том числе незаконного характера: от способов взлома аккаунтов социальных сетей, предложений потенциальных поставщиков запрещенных веществ и товаров вплоть до руководств по их самостоятельному изготовлению и реализации, взлому онлайн-хранилищ информации и денежных средств. Интернет-пространство позволяет осуществлять перевод необходимых финансовых средств анонимно для покупки разных товаров, сбор «ложных» пожертвований, вступление в разного рода группы по терроризму в социальных сетях или самостоятельную вербовку наёмников и осуществление пропаганды. Наряду с описанными выше возможностями существует самая главная и основная для хакеров – осуществить в краткие сроки и с малыми затратами сбой в нормальном функционировании объектов гражданской важности (военные инфраструктуры, порталы правительства, банки и прочее), что грозит информационной и финансовой безопасности на государственном уровне.

Одной из самых социально опасных угроз «всемирной паутины» можно выделить новый вид терроризма – «кибертерроризм».

Согласно Акопову Г.Л., «кибертерроризм – несанкционированное вмешательство в работу компонентов компьютерных сетей общего пользования, вызывающее дезорганизацию работы элементов инфраструктуры политически значимых институтов общества, причинение морального и материального ущерба, а также иные социально опасные последствия» [2, с. 24-27]. Автор определяет киберпреступника как пользователя компьютера, нарушившего законодательство с использованием сети общего пользования.

Учитывая своеобразность киберпространства, для психологической характеристики личности киберпреступника необходимо изучение следующих направлений:

1) общих особенностей интернет-среды;

2) психологии отдельных категорий преступников.

Развитие и рост информационных технологий позволяет кибертеррористам извлекать прибыль при низком риске, использовать информационные ресурсы для финансовых и организационных вопросов, обеспечивать связи, планировать и организовать акты терроризма, осуществляя всеохватывающий контроль над их проведением. Последние события показывают, что виртуальное информационное пространство становится «пристанищем» национальных террористических организаций, где они имеют возможность изучить весь контингент пользователей, провести пропаганду и сбор, минуя контроль государственных органов. Многочисленные социальные сети, чаты и форумы идеально приспособлены для создания анонимных переписок и передачи зашифрованных посланий, технологии позволяют распознавать карты и фотографии, что способствует легкой организации мест для теракта. Тем самым интернет является недорогим средством осуществления своей деятельности, а также сложным для выявления самих террористов [4].

Выделим несколько особенностей преступлений в виртуальном пространстве в дополнение к вышеприведенным.

1) Среда, образованная электронным устройством и сетями – меняется психологическое содержание взаимосвязей «преступник – электронное

устройство (сеть) – потерпевший», что способствует устранению социального взаимодействия и материальной составляющей.

2) Анонимность – предполагает предоставление ложной информации, скрытность, защиту, ощущение безнаказанности, отсутствие механизмов порицания. Анонимность позволяет создавать разные образы личности, отличающиеся от реальности, что может вызвать у преступников различные расстройства типичных пользователей интернета: интернет-зависимость, тревожные расстройства, диссоциативные расстройства личности.

3) Психологические процессы – совершение киберпреступлений не требует присутствия непосредственно на месте, т.е. преступник может находиться дома в комфортной обстановке, отчего исчезает чувство дискомфорта, страха быть обнаруженным и задержанным. Киберпреступники не имеют возможности в полной мере оценить ущерб, увидеть реакцию жертвы, отчего не чувствуют раскаяние, а, наоборот, при удачно спланированном преступлении, удовлетворении своим результатом закрепляют образ акта преступного поведения.

4) Минимизация власти – чувство равенства в виртуальном пространстве, что возникает из-за опосредованного восприятия составляющих высокого социального статуса и положения.

По мнению Макса Килгера, кибертеррористы имеют несколько мотивов для своей деятельности: жажда славы, легкий способ разбогатеть, политические разногласия, розыгрыш. На первое место он поставил деньги и легкий способ заработка: отмечено, что убытки, связанные с киберпреступлениями, увеличиваются каждый год, а любителей внести сбой в компьютерной системе становится гораздо больше – доступ к интернету и компьютеру имеется у подавляющей части общества.

На наш взгляд наиболее точная типология личности представлена А.Н. Косенковым, Г.А. Черным. Авторы выделили 7 типов личности, имеющих склонность к совершению киберпреступлений:

1) корыстный тип;

2) насильственный тип;

3) сексуальный тип;

4) социально-дезорганизующий тип;

5) идеологически или политически мотивированный тип;

6) статусный тип;

7) исследовательский тип.

1) Корыстный тип – получение финансовых средств или специфических предметов, имеющих ценность в виртуальном пространстве, как с целью продажи, так и для личного пользования и коллекционирования.

2) Насильственный тип – доведение до самоубийства, угрозы, запугивания посредством электронных сетей и устройств.

3) Сексуальный тип – незаконное распространение порнографических материалов, принуждение к действиям сексуального характера.

4) Социально-дезорганизующий тип – нарушение социальных норм и оказанием деструктивного влияния на общество и отношения.

5) Идеологически или политически мотивированный тип – форма протеста, идеологической или политической борьбы (в преддверии выборов).

6) Статусный тип – получение высокого неформального статуса в сообществах киберсоциума.

7) Исследовательский тип – изучение программных и аппаратных составляющих устройств и сетей, поиск уязвимостей, возможности дальнейшего использования или устранения [5, с. 90-93].

Данная типология позволяет на основе личностных особенностей выделить предрасположенность к киберпреступлениям у определённых лиц, а также составить примерный психологический портрет преступника.

Таким образом, данные возможности и особенности киберпространства способствуют формированию такого слоя преступного мира как киберпреступники. Профилактика и борьба с таким видом преступлений невозможна без мультидисциплинарного подхода, который, помимо использования технологических средств, требует активизации психологии,

исследований в рамках нее и подготовки специальных кадров, способных выявлять подобные преступления в виртуальном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. David G. Post «Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace»// Journal of Online Law – No.1, art. 3, 1995. – URL: http://www.temple.edu/lawschool/dpost/Anarchy.pdf

2. Акопов Г.Л. Хактивизм в процессе информационно-политических конфликтов // NB: Национальная безопасность. – 2014. – № 1. – С. 24-32.

3. Ахмадеева Е.В. Виртуальное пространство как угроза психологической безопасности семьи // Вестник Башкирского университета. – 2014. – Т.19. – №1. – С. 242-247.

4. Кибертерроризм и особенности его проявления [Электронный ресурс] // «Kursak.NET». – 2015. – Режим доступа: http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/

5. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал ОГУЭП. – 2012. – № 3(21). – С. 87-94.

6. Целевые атак» [Электронный ресурс] / Лаборатория Касперского. – 2015. –Режим доступа: http://www.kaspersky.ru/hackers