УДК 004.621

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРТЕРРОРИЗМА

К. т. н. Е. В. Иванченко, д. т. н. В. А. Хорошко

Национальный авиационный университет
Украина, г. Киев
professor_va@ukr.net

В работе рассмотрены вопросы, связанные с современным состоянием информационного терроризма и использованием для его реализации информационных технологий, а также аспекты привлекательности телекоммуникационных сетей для кибертерроризма. Определены тенденции развития кибертерроризма и пути противодействия ему.

Ключевые слова: информационный терроризм, кибертерроризм, телекоммуникационные сети.

Вопросы, связанные с безопасностью информационных систем, постепенно обострялись по мере развития информационных технологий и широкого использования каналов передачи данных и сетей во всех областях народного хозяйства. На сегодня в сфере защиты сформировалась довольно мощная индустрия, которая объединила в себе науку и производство.

Индустрия информационных технологий — одна из наиболее стремительно развивающихся сфер мировой экономики, способная конкурировать по доходности с топливно-энергетическим комплексом и автомобилестроением. Она сделала рынок значительно более масштабным, динамичным и конкурентным, дала стимул к зарождению множества новых сфер бизнеса. В мире постоянно увеличивается количество персональных компьютеров, так же как и пользователей глобальной сети Интернет, чему способствует чрезвычайно быстрое развитие компьютерных технологий и систем телекоммуникаций. Но вместе с тем растет и количество преступлений, которые осуществляются с использованием вычислительной техники, одним из которых и является кибертерроризм.

Кибертерроризм сравнительно молод и состоит из двух понятий: киберпространство и терроризм. Понятие терроризма можно определить как преднамеренные общеопасные действия, которые посягают на общественную безопасность и направлены на создание в социальной сфере обстановки страха, беспокойства, подавленности, с целью прямого или непрямого влияния на принятие какого-либо решения или отказ от него в интересах террористов. Следовательно, кибертерроризм представляет собой преднамеренные действия, которые определяются в форме атак на информацию, вычислительные системы, компьютерные программы или данные, а также другие действия, которые приводят к нарушению информационного пространства и следствием которых есть насилие, создающее опасность гибели людей, причинения значительного имущественного ущерба или наступления других общественно опасных последствий (определение кибертерроризма было сформулировано в НДР № 497–ДБ08 «Нові методи і моделі систем виявлення кібертерористичних атак»). Главными мишенями атак кибертеррориста являются вычислительные системы и циркулируемая в них информация.

Компьютеры, компьютерные сети Интернет стали основной частью бизнеса, социальной активности, а, следовательно, и кибертерроризма. Таким образом, работа посвящена определению тенденций развития кибертерроризма в государстве с целью разработки соответствующих мер противодействия ему.

Можно выделить следующие аспекты привлекательности телекоммуникационных сетей для кибертерроризма:

— большинство серверов коммуникационных сетей позволяют пользователям работать относительно конфиденциально и анонимно;

— существует возможность использования специальных роботов (bots) для снижения времени и затрат на террористическую деятельность;

— киберпреступления сложно отследить и собрать доказательства;

— меньший риск по сравнению с обычными видами преступления и более высокая эффективность;

— возможность совершать киберпреступления через границы стран и континентов;

— не требует физического присутствия.

Неудивительно, что формы терроризма перемещаются в область кибертерроризма и требуют глубокого изучения с целью эффективного противодействия.

Проблемы информационной безопасности многогранны и требуют решения многих вопросов от обеспечения безопасности отельного компьютера до обеспечения безопасности функционирования локальных и глобальных сетей.

Киберпреступность активизируется и в настоящее время рассматривается различными экспертами, как стремительно нарастающая угроза безопасности как отдельным государствам, так и мировому сообществу в целом.

Несмотря на усилия правоохранительных органов и спецслужб, число преступных актов с использованием информационных технологий не уменьшается, а напротив, постоянно увеличивается, и возрастает их общественная опасность.

Меняется и сам облик терроризма, о чем наглядно свидетельствует появление информационного терроризма. Одной из наиболее опасных угроз безопасности является использование кибертеррористами возможностей открытых телекоммуникационных сетей для оказания пропагандирующего действия на мировую общественность.

Информационные технологии предоставляют террористам возможность скрытно, планомерно и эффективно воздействовать на индустриальное и массовое сознание, общественное мнение, процессы принятия решений; распространять информацию для вербовки в свои ряды новых членов, пропаганды своих идей; проводить дезинформацию; вызывать панику, а также непосредственно совершать террористические акты. Эти технологии позволяют террористическим группам, большинство из которых сейчас имеют сетевую структуру организации, эффективно и скрытно осуществлять взаимодействие между ее разрозненными ячейками и отдельными членами, а также проводить сбор информации о будущих целях.

Таким образом, в итоге можно спрогнозировать следующие тенденции развития кибертерроризма:

— наиболее реальными целями кибертерроризма будут персональные мобильные средства телекоммуникации, процесс совершенствования и развития которых в настоящие время чрезвычайно динамичен;

— вредоносные коммуникационные сообщения в настоящий момент являются бичом практически всех телекоммуникационных систем и, согласно прогнозам, объем этих преступлений в общем количестве кибертерроризма не будет уменьшаться, а наоборот, будет увеличиваться;

— количество атак на банковские системы будет в дальнейшем все более возрастать, а соответственно, будут увеличиваться уязвимые места, например на получение банковских и идентификационных параметров пользователей.

Для противодействия вышеперечисленным угрозам кибертерроризма необходимо вводить дополнительные механизмы обеспечения информационной безопасности, т. к. существующих недостаточно для эффективного решения вопросов, а сделать это в информационной сфере можно за счет координации и прогрессивного развития норм международного права. Необходимо также предпринимать меры на международном уровне в направлении снижения угроз от кибертерроризма национальной безопасности.

———————

Y. V. Ivanchenko, V. A. Khoroshko

Tendencies of electronic terrorism development.

The study considers the problems of the current state of information terrorism and application of information technologies for its realization, as well as aspects of appeal that telecommunication networks have for cyberterrorism. The authors define tendencies of cyberterrorism development and ways to counteract it.

Keywords: *information terrorism, cyber terrorism, telecommunication networks.*