УДК 614.8

С.В. Богинская, А.Л. Головин, Л.А. Кудрич

КИБЕРТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

ФГБОУ ВО Тверской государственный медицинский университет Минздрава России

В настоящее время во всем мире возросла угроза новой формы терроризма – кибертерроризма. При этом, определениеэтогопонятияпредставляется весьма важной задачей [5]. Вместе с тем,довольно сложно отделить кибертерроризм от акций информационной войны и и выявить его специфику.Психологический и экономический аспекты этого явлениявзаимосвязаны. Поэтому приоритет того или другого невозможно определить. В связи с этим,указанная проблема является актуальной и требует дополнительного изучения [2].

Основнымвидомкибертерроризма является атака на компьютерную информацию, вычислительные системы и аппаратуру передачи данных [3]. В основном,ее совершают отдельныелюди или группы. Она заключается в проникновении, перехвате управления и подавлении средств сетевого информационного обмена. Эффективность указанныхдействий зависит от особенностей информационной структуры и степени ее защищенности.Последствия кибертерроризма– это нанесение ущерба элементам информационного пространства;разрушение сетей электропитанияи элементной базы; наведение помех;уничтожение программного и технического ресурсов, имеющих общественную значимость. В результате этого преодолеваются системы защиты и внедряются вирусы [4]. При этом, возникает воздействие на программное обеспечение с целью искажения имодификации в информационных системах.Это позволяет продемонстрировать цель террористической акции: уничтожение или активное подавление линий связи, неправильную адресацию, искусственную перегрузку узлов коммутации; проведение информационно-психологических операций.Вместе с тем, эти действия вызывают серьезные экономические последствия. Повсеместное отключение электроэнергии и, как следствие, отключение компьютерных систем – также вполне реальная угроза. Возможно и проникновение в локальные сети, изменение или уничтожение информации, блокирование работы компьютеров какого-либо государственного учреждения. Все это позволяет сегодня говорить, что деятельность террористов переходит из реального в виртуальное пространство.Особенностьюкибертерроризмаявляется отсутствие стремления хакерских групп афишировать свои данные.Они выступают исключительно под псевдонимом.Проведение кибератак обеспечивает высокую степень анонимности и требует большего времени реагирования.Главное в тактике кибертерроризма состоит в том, чтобы это киберпреступление имеетсерьезные последствия:оно делается широко известным населению, получает большой общественный резонанс, создает атмосферу угрозы повторения акта без указания конкретного объекта.

Осуществление атаки через информационные системы вообще может оказаться нераспознанным как акт терроризма, а будет воспринято, например, как случайный сбой системы. Это подчеркивает серьезность этого явления. Нет общего мнения по поводу определения объекта актов терроризма. Отмечено, что им могут стать не только международные организации, народы, но и конкретный политический или государственный деятель. В том числе, гражданские и военные объекты. В государстве наиболее уязвимыми точками считаются энергетика, телекоммуникации, авиационные диспетчерские, финансовые электронные и правительственные информационные системы, автоматизированные системы управления войсками и оружием. Так, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за

собой ядерную катастрофу или прекращение подачи электроэнергии в города и на военные объекты. Искажение информации или блокирование работы информационных систем в финансовой сфере может иметь следствием экономический кризис, а выход из строя электронно-вычислительных систем управления войсками и оружием – непредсказуемые необратимые последствия. То есть цели, на которые направлены атаки кибертеррористов, соответствуют национальной информационной инфраструктуре. Информация, играющая решающую роль в функционировании как государственной власти, так и общественных институтов, становится самым слабым звеном национальной инфраструктуры государства на современном этапе развития, поэтому проблема международного терроризма приобретает в условиях информационного противостояния новое звучание. Терроризм на международной арене выступает и как инструмент вмешательства во внутренние дела государств, дезорганизует международные связи, грубо нарушает права человека, международный правопорядок. Вот почему следует проблему терроризма рассматривать на международном уровне как прямую угрозу международной безопасности, а угрозу кибертерроризма – как вторую составляющую такого рода угроз.

Вопрос обеспечения информационной безопасности как одной из важных составляющих национальной безопасности государства особенно остро возникает в контексте появления транснациональной трансграничной компьютерной преступности и кибертерроризма[1]. Специализированные подразделения официально используют несколько десятков стран, а неофициально более сотни. В тройке стран, где эти направления наиболее развиты США, Китай и Великобритания.Специалисты подчеркивают,что злоумышленники идут в ногу со временем и делают упор на самые последние технологии или наиболее распространенные продукты.Отмечается, что сейчас уже 46% мирового населения имеет доступ к интернету. В этой связи особенно опасной эксперты видят угрозу усиления киберпропаганды. Речь идет, в том числе о генерации автоматического информационного трафика, направленного на пользователей соцсетей и микроблогов, а также о растущем числе ложных новостных материалов в соцсетях.

Таким образом, в условиях наращивания в мире процессов глобализации и формирования «информационного общества», кибертерроризм может выступать в качестве самостоятельного фактора, способного угрожать отдельным государствам и международному сообществу в целом, что обусловливает увеличение значимости противодействия угрозам данного типа для государственной системы национальной безопасности.

Список литературы

1. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия / О. О. Андреев, А. С. Шундеев, С. А. Афонин и др. –None, 2008. –С. 607.

2. Авцинова Г. И. Тенденции информационной войны против России // Научно-аналитический журнал Обозреватель. – Observer. – 2011. – № 7. – С. 41–43.

3. Голубев В. А. Кибертерроризм – понятие, терминология, противодействие. URL: http://www.crime-research.ru/articles/Golubev0804.

4. Тропина Т. Л. Киберпреступность и кибертерроризм. URL: http://www.crime-research.ru/library/Tropina.html.

5. Мазуров В.А. Кибертерроризм: понятие, проблемы, противодействия / Доклады ТУСУРа. – 2010. –№ 1 (21). – С. 41– 44.