

## **КИБЕРТЕРРОРИЗМ**

**Гаряева А.М., Папуця А.А.**

*Национальный технический университет  
«Харьковский политехнический институт», г. Харьков*

Технический прогресс, развивается настолько стремительно, что некоторые его последствия осознаются обществом слишком поздно, когда для исправления ситуации требуются уже значительные усилия. Такая ситуация складывается в области информационных технологий.

Сегодня можно говорить, что Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара. Внедрение современных информационных технологий, привело, к сожалению, к появлению новых видов преступлений, таких как компьютерная преступность и компьютерный терроризм. Кибертерроризм – это новая форма терроризма, которая для достижения своих террористических целей использует компьютеры и электронные сети, современные информационные технологии. По своему механизму, способам совершения и сокрытия компьютерные преступления имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости.

Относительная новизна возникших проблем, застала врасплох правоохранительные органы, которые оказались не готовыми к адекватному противостоянию и борьбе с этим новым социально-правовым явлением.

Особенно остро вопрос обеспечения информационной безопасности, как одной из важных составляющих национальной безопасности государства, встает в контексте появления транснациональной (трансграничной) компьютерной преступности и кибертерроризма. Актуальность проблем компьютерного терроризма для Украины двойственна: с одной стороны, государство не настолько богато, чтобы переоборудовать современными средствами управления своих химических предприятий, атомных электростанций и других критических и уязвимых структур, что сделало бы их неуязвимыми для нападений интеллектуальных диверсантов. С другой стороны, образующаяся информационная инфраструктура становится стратегическим ресурсом, который требует постоянного внимания. Открытые сети сегодня – это средства информационного противоборства в руках политиков, бизнесменов, религиозных организаций, террористических групп и преступных группировок.

Эффективная борьба с транснациональной компьютерной преступностью и терроризмом – это ключевой элемент обеспечения безопасности, причем не только в плане борьбы с кибертерроризмом, но и реальное противодействие новым формам терроризма и организованной преступности.