

Тема: Кибертерроризм угроза национальной безопасности



- Мы живем в эпоху информационного общества, когда информация становится необходимой для нормального функционирования всего общества. Развитие сети «Интернет» позволило людям передавать огромные потоки информации на расстояния, что предоставило людям новые реальности — от возможности общаться и видеть друг друга, находясь в разных точках земного шара, до объединения усилия целых исследовательских групп, которые, находясь в разных странах и даже континентах, могут работать слаженно и эффективно.
- Глобальная сеть Интернет постоянно совершенствуется: в ней появляются новые сервисы и огромное количество информации. Это открывает не только дополнительные возможности для развития мирового сообщества, но и сопровождается появлением ряда новых глобальных угроз.
- Террористические организации и группы, включая «Аль-Каиду», активно используют Интернет для связи и обмена информацией, ведения пропаганды, вербовки новых членов и организации подрывной деятельности. Так, Рамзи Юзеф, организовавший взрыв Всемирного торгового центра в Нью-Йорке 11 сентября 2001 г., получал по Интернету зашифрованные инструктивные послания от Усамы бен Ладена. Таким образом, в конце XX века появилось совершенно новое явление в сфере информационных технологий: компьютерный или кибертерроризм, использующий для достижения своих преступных целей компьютеры,

Кибертеррористы



- Кибертерроризм рассматривают, как преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта
- Перед террористическими актами, которые совершаются посредством сети «Интернет» уязвимы все сферы жизнедеятельности общества и государства, в которых активно применяются информационные технологии. Так, например, в отношении аэропортов, как объектов транспортной инфраструктуры, кибертерроризм может быть использован самыми различными способами. От самого простого варианта – дезинформации и психологической атаки посредством сообщений об угрозе террористического акта, что вносит хаос в работу аэропорта и самолетов, до вмешательства в электронные системы управления полетами воздушных судов, что может повлечь тяжкие последствия, либо угрозу повреждений инфраструктуры аэропортов и самолетов в воздухе.



- В киберпространстве могут быть использованы различные приемы для совершения кибертеракта:
- - получение несанкционированного доступа к государственным и военным секретам, банковской и личной информации;
- - нанесение ущерба отдельным физическим элементам информационного пространства, например, разрушение сетей электропитания, создание помех, использование специальных программ, стимулирующих разрушение аппаратных средств;
- - кража или уничтожение информации, программ и технических ресурсов путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.;
- воздействие на программное обеспечение и информацию; - раскрытие и угроза публикации закрытой информации;
- - захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
- - уничтожение или активное подавление линий связи, неправильная адресация, перегрузка узлов коммуникации;
- - проведение информационно-психологических операций и т.п.

КОНЕЦ

- Готовил: Тыналиев Тагай
- ФАЮ 5-16