Безопасность в сети интернет. Информационная безопасность в интернете.

Киберпространство и информационный терроризм

Важность и актуальность противоборства в киберпространстве подтверждается тем, что исследования в этой области активно проводятся не только отдельными учеными, но и исследовательскими группами ряда аналитических центров ведущих мировых держав и глобальная информатизация всех сфер жизни общества не повышает, а понижает степень его безопасности.

Нужно полагать, что термин «информационный терроризм» является более общим, чем «кибертерроризм», который охватывает вопросы использования разнообразных методов и средств информационного воздействия на различные стороны человеческого общества (физическую, информационную, когнитивную, социальную).

Под информационным терроризмом следует понимать один из видов террористической деятельности, ориентированный на использование различных форм и методов временного или безвозвратного вывода из строя информационной инфраструктуры государства или ее элементов, а также целенаправленное использование этой инфраструктуры для создания условий, влекущих за собой катастрофические последствия для различных сторон жизнедеятельности общества и государства.

При этом можно выделить следующие основные его виды:

1) информационно-психологический терроризм – контроль над СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций; воздействие на операторов, разработчиков, представителей информационных и телекоммуникационных систем путем насилия или угрозы насилия, подкупа, введения наркотических и психотропных средств, использование методов нейролингвистического программирования, гипноза, средств создании иллюзий, мультимедийных средств для ввода информации в подсознание и т. д.;

2) информационно-технический терроризм – нанесение ущерба отдельным физическим элементам информационной среды государства; создание помех, использование специальных программ, стимулирующих разрушение систем управления, или, наоборот, внешнее террористическое управление техническими объектами (в т. ч. самолетами), биологические и химические средства разрушения элементной базы и т. д.; уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и т. д.

Средства информационного оружия

Под информационным оружием следует понимать - совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения. Основными видами информационного оружия можно считать:

· компьютерные ”вирусы” - специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, ”вирусы” способны самостоятельно размножаться, то есть копировать себя на магнитных носителях.

· программные продукты типа “троянский конь” - программы, внедрение которых позволяет осуществлять скрытый несанкционированный доступ к информационному массиву объекта террористической атаки для добывания интересующих данных;

· нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения;

· преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему. Они, как правило, сознательно вводятся в программное обеспечение программистами-разработчиками с далеко идущими целями;
· малогабаритные устройства, способные генерировать электромагнитный импульс высокой мощности, обеспечивающий вывод из строя радиоэлектронной аппаратуры, а также другие средства подавления информационного обмена в телекоммуникационных сетях, фальсификации информации в каналах управления;
· различного рода ошибки, сознательно вводимые в программное обеспечение объекта.

Один из видов оружия, который также может быть отнесен к информационному, - это средства радиоэлектронной борьбы. Они включают в себя средства радиоэлектронного подавления, радиоэлектронной защиты и радиоэлектронного обеспечения. Радиоэлектронная борьба в больших масштабах началась во время воздушной войны между Германией и Великобританией осенью 1940 года, получившей название “Битва за Англию”.