Терроризм **–** это идеология насилия и практика воздействия на принятие органами государственной власти, международными организациями решений, связанных с устрашением населения и (или) иными формами противоправных насильственных действий.

Одной из разновидностей терроризма является *кибертерроризм* («электронный терроризм», «информационный терроризм» и др.).

Кибертерроризм – это действия по дезорганизации информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо иных общественно опасных последствий, совершенные со специальной целью нарушить общественную безопасность, устрашить население путем создания условий для аварий и катастроф техногенного характера либо оказать воздействие на органы власти с целью принятия ими решений, выгодных террористам.

Основной формой кибертерроризма

является политически мотивированная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемая группами или отдельными лицами. Она позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия.

Объектами информационного терроризма, в зависимости от преследуемых целей и задач, могут быть:

- информационные ресурсы;
- системы формирования, распространения и использования информационных ресурсов;
- информационная инфраструктура вооруженных сил, правоохранительных органов и центров управления АЭС, транспортными структурами и высокотехнологичными производствами;
- корпоративные группы людей и институты государства, а также сам человек.

Для достижения поставленных целей в киберпространстве могут быть использованы *различные приемы* совершения теракта:

- хищение или уничтожение информационных, программных и технических ресурсов, имеющих стратегическую значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок;
- нанесение ущерба отдельным физическим элементам, например, разрушение сетей электропитания, временное выведение из строя отдельных сайтов, наведение на них помех, использование специальных программ, стимулирующих разрушение аппаратных средств, а также биологических и химических средств для уничтожения элементной базы;
- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;
- уничтожение либо активное подавление линий связи, ошибочное адресование, искусственная перегрузка узлов коммутации и др.;
- раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодов шифрования, принципов работы систем шифрования;
- захват каналов телекоммуникационного вещания с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
- воздействие на операторов, разработчиков, эксплуатационников информационных и телекоммуникационных систем с целью совершения ими ошибочных действий;
- ложная угроза акта кибертерроризма, влекущая за собой серьезные экономические последствия.

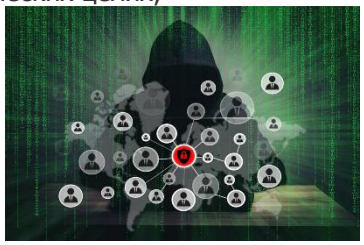
В последнее время террористы все чаще используют Интернет для организации связи и управления в среде своих последователей. Так, экстремистские группировки для призывов к осуществлению террористической деятельности, демонстрирования своей мощи, распространения, пропаганды и оправдания своих идей, дезинформации населения, а также для вербовки в свои ряды граждан, особенно молодежи, постоянно создают и обновляют свои многочисленные веб-сайты. Это позволило ИГИЛ (ИГ) (запрещена в РФ) довести численность своей организации в Сирии и Ираке до 30 тыс. боевиков, прибывших из 100 государств.

Интернет позволяет оказывать

психологическое давление на отдельных лиц, группы людей, компании, банки (финансовые институты) с целью получения требуемых денежных средств, а также принятия выгодных террористам решений.

Основными направлениями противодействия мирового сообщества кибертерроризму являются:

- развитие и укрепление сотрудничества между государствами, правоохранительными органами, специальными службами, международными организациями в сфере обеспечения информационной безопасности от возможных угроз кибертерроризма и транснациональной компьютерной преступности;
- создание национальных подразделений по борьбе с кибертерроризмом, образование международного контактного пункта по оказанию помощи при реагировании на транснациональные компьютерные инциденты;
- установление и расширение обмена информацией об угрозах совершения компьютерных атак, о признаках, фактах, методах и средствах использования ГИС в террористических целях;



- обмен опытом и лучшими практиками мониторинга информационных ресурсов Интернета, поиска и отслеживания содержимого сайтов террористической направленности, проведения криминалистических компьютерных экспертиз в этой сфере;
- принятие мер превентивного характера, направленных на формирование у населения негативного отношения ко всем возможным проявлениям терроризма, к использованию насилия для достижения соответствующих целей;
- привлечение к уголовной ответственности лиц, причастных к кибертерроризму.

Памятка разработана
Учебно-методическим центром
по гражданской обороне и чрезвычайным
ситуациям Нижегородской области
имени Маршала Советского Союза
В.И. Чуйкова
и носит рекомендательный характер

Противодействие кибертерроризму

г. Нижний Новгород

Примеров противоправной деятельности кибертеррористов сегодня уже достаточно.

В 1998 году хакерской атаке подвергся индийский Центр ядерных исследований имени Баба, где террористы угрожали вывести из строя систему управления реактором.

В начале 1999-го хакерам удалось захватить систему управления военным телекоммуникационным спутником серии "Скайнет" и изменить его орбиту. Только через несколько недель британские власти признали факт проникновения в эту систему и незаконного вмешательства в ее работу.

В 1999 году через Интернет в адреса правительств более чем 20 стран (США, Великобритании, Израиля, Австрии и др.) были направлены электронные письма от имени офицеров российской воинской части, имеющей на вооружении стратегические ракеты шахтного базирования. В этих письмах содержалась угроза "самовольно произвести пуски ракет по целям, расположенным в столицах и промышленных центрах западных стран", а также требование выплаты крупной денежной суммы. В результате проведенного ФСБ России расследования анонимы были задержаны. Следствием и судом их действия были квалифицированы как заведомо ложное сообщение об акте терроризма.

В Азии 1 мая 2000 года через Интернет был запущен компьютерный вирус "Ай лав ю", который нарушил работу правительственных учреждений, парламентов и корпораций многих стран. Госструктуры в сотрудничестве с частными компаниями в области компьютерной безопасности не сразу начали работу по борьбе с "жучком любви" с целью создания необходимого антивируса, в результате чего за первые пять дней с момента его появления он нанес материальный ущерб в размере 6,7 млрд долларов.

В конце 2001 года была предпринята акция против Всемирной торговой организации. Антиглобалисты "создали" два дубля вэб-сайта ВТО, которые совпадали по дизайну, но содержали совершенно разную информацию.

В июне 2010 года в компьютерной системе иранского центра по обогащению урана был обнаружен вирус, получивший название "Стакснет", изменивший скорости вращения центрифуг, что привело к их выходу из строя. Именно этот инцидент вынудил многие развитые страны пойти на укрепление защиты своих жизненно важных промышленных объектов, в частности, в энергетике и водоснабжении.

Летом 2017 года вирусы "Петя" и "Бона Край" атаковали сотни компьютеров в информационных системах государственных органов, финансовых организациях и частном секторе. Был нанесен совокупный экономический ущерб в сотни миллионов долларов США.

На территории Западной Европы ежегодно фиксируется до 300 удачных проникновений хакеров в военные, государственные и коммерческие сети.

Известны массовые нападения на информационные сети Китая, Тайваня, Индии, Индонезии, противостояние хакерских групп Армении и Азербайджана.

По заявлению генсека НАТО Й. Столтенберга, число хакерских атак на системы Североатлантического союза увеличилось в 2017 году на 60 проц. - каждый месяц в НАТО отражали до 500 атак.