

Таким образом, ввиду того, что информационное общество в стране и мире все еще идет по пути своего развития, кибертерроризм остается недостаточно хорошо изученной, но весьма прогрессивной проблемой, которая требует к себе особого внимания и активных мер противодействия, как на международном, так и на государственном уровне.



Если вы стали жертвой киберпреступников, вы должны сообщить об этом в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого.



Муниципальное автономное учреждение культуры
«Культурный центр: библиотека-музей»

**Центральная городская библиотека
Отдел информационных технологий**



Терроризм в киберпространстве

Буклет

Составитель: библиотекарь
Отдела информационных технологий
Е. С. Алексеенко

Оформление: библиотекарь
Отдела методической и инновационной работы
К. Н. Фролова

**Library_pyti-yah-muzej@mail.ru
www.pytyahlib.ru**

Пыть-Ях
2021

12+

Кибертерроризм – комплекс незаконных действий в киберпространстве, создающих угрозу государственной безопасности, личности и обществу. Может привести к порче материальных объектов, искажению информации или другим проблемам.

В своих акциях преступники активно используют все возможности современных технологий, в том числе современные гаджеты и программные продукты, радиоэлектронные устройства, достижения в других областях (вплоть до микробиологии и генной инженерии).

Официально кибертерроризмом признаются кибертерракты, совершенные одним человеком или независимыми группами, состоящими из нескольких участников. Если в подпадающих под это определение действиях принимают участие представители правительств или иных государственных структур, это считается проявлениями кибервойны.

Кибертерракт — это террористический акт с использованием цифровых технологий, который может рассматриваться как преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, атаки, выраженные в применении насилия по отношению к гражданским целям со стороны преступных групп или отдельных лиц.

CYBER TERRORISM

Цели кибертерроризма

- Взлом компьютерных систем и получение доступа к личной и банковской информации, военным и государственным конфиденциальным данным;
- Вывод из строя оборудования и программного обеспечения, создание помех, нарушение сетей электропитания;
- Кража данных с помощью взлома компьютерных систем, вирусных атак, программных закладок;
- Утечка секретной информации в открытый доступ;
- Распространение дезинформации с помощью захваченных каналов СМИ;
- Нарушение работы каналов связи.



Как защитить себя

- Не доверять всем непонятным сообщениям, в которых содержится просьба предоставить личные данные;
- Быть аккуратными при совершении онлайн - покупок, выбирать для этого сайты, обеспечивающие безопасность сделок и конфиденциальность личных данных;
- Использовать антивирусные программы и сложные уникальные пароли для каждой службы;
- Ограничение личной информации в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона и т.д.;
- Регулярно проводите беседы с детьми о правилах поведения в интернете, особенно в соцсетях. Ваши дети должны знать о недопустимости любого негативного воздействия на них и необходимости сообщить родителям о подобных инцидентах;
- Никогда не открывайте письма на электронной почте, если не уверены в отправителе;
- Не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут;
- Не предоставляйте возможность физического доступа к вашим устройствам. Относитесь к вашим устройствам, как к кошельку с кучей денег, потому что так оно и есть на самом деле – информация стоит дорого;
- Проверяйте аккаунт пользователя, прежде чем добавлять его в друзья.