Защита от киберпреступности.

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Киберпреступления совершают частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически.

Для примера можно привести некоторые разновидности киберпреступлений:

- мошенничество с использованием электронной почты и интернета;
- кража цифровой личности (хищение и использование личных данных);
- кража данных платежных карт и другой финансовой информации;
- хищение и перепродажа корпоративных данных;
- кибершантаж (вымогательство денег под угрозой атаки);
- атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа);
- криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);
- кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);
- нарушение работы систем с целью компрометации сети;

- нарушение авторских прав;
- незаконное проведение азартных игр;
- онлайн-торговля запрещенными товарами;
- домогательства, изготовление или хранение детской порнографии;

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности:

1) Повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.).

2) Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств.

3) Особая подготовленность преступников, интеллектуальный характер преступной деятельности.

4) Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств.

5) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления.

6) Многоэпизодный характер преступных действий при множественности потерпевших.

7) Неосведомленность потерпевших о том, что они подверглись преступному воздействию.

8) Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

9) Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Киберпреступление всегда подразумевает хотя бы одно из указанного:

- Преступную деятельность с целью *атаки* на компьютеры с использованием вирусов или другого вредоносного ПО.
- Использование компьютеров для совершения других преступлений.

Примеры кибератак:

- атаки с использованием вредоносных программ;

- фишинг (отправка спама (в электронных письмах или по другим каналам), чтобы обманным путем вынудить пользователей сделать нечто, что ослабит их безопасность. Фишинговые сообщения могут содержать зараженные вложения, ссылки на вредоносные сайты или просьбу предоставить конфиденциальную информацию.

- распределенные DoS-атаки (нацелены на вывод из строя какой-либо системы или сети. Иногда для проведения DDoS-атак используются устройства IoT (интернета вещей).

Способы защиты от киберпреступлений:

- регулярное обновление ПО и операционной системы;

- использование антивирусных программ и их регулярное обновление;

- использование надежных паролей;

- привычка не открывать вложенные файлы в письмах;

- привычка не переходить по ссылкам в спам-письмах и на недоверенных веб-сайтах;

- осторожность при передаче личной информации;

- общение по официальным каналам;

- внимательность при посещении веб-сайтов;

- регулярная проверка банковских выписок.