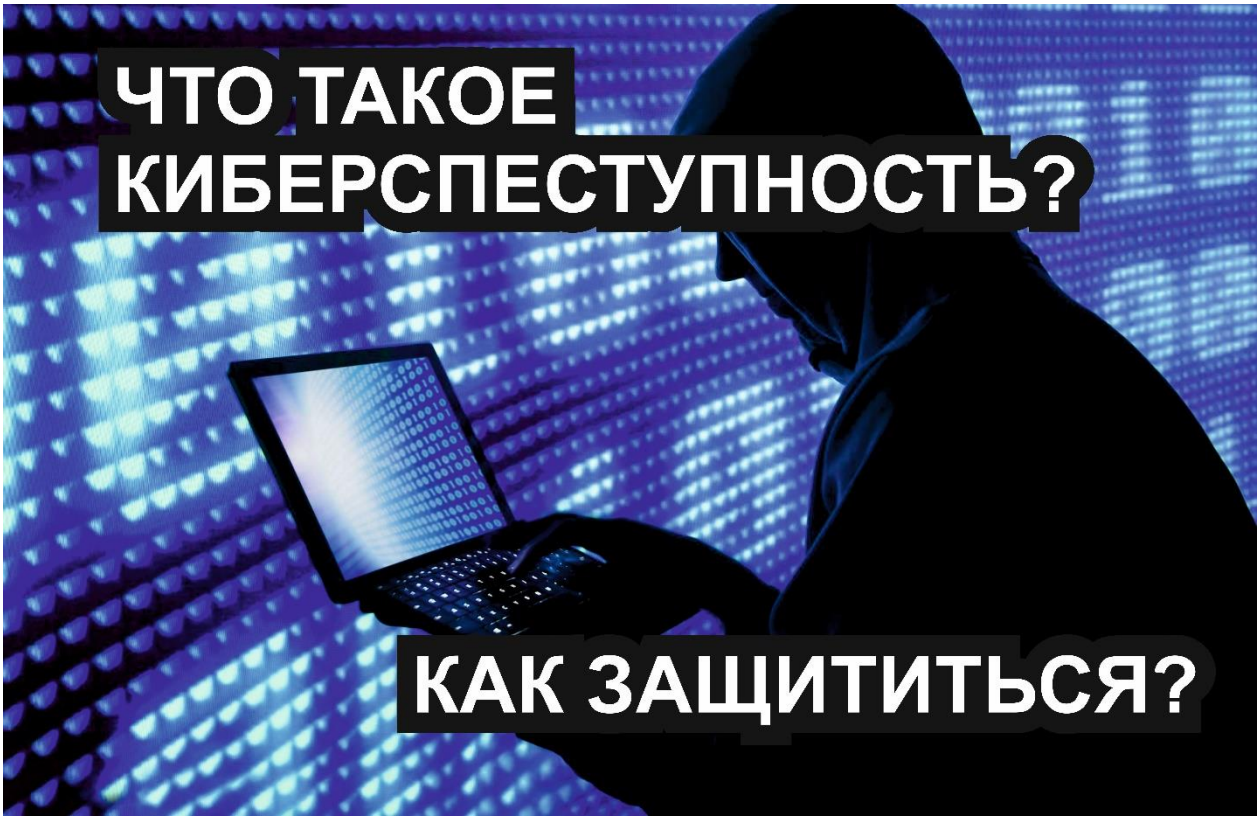

КИБЕРПРЕСТУПНОСТЬ – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство.
Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров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

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ

Мошенничество с использованием электронной почты и интернета
Кража цифровой личности (хищение и использование личных данных)
Кибер-кража финансовых данных или данных о платежах по картам
Хищение и перепродажа корпоративных данных
Кибершантаж (вымогательство денег под угрозой атаки)
Атаки компьютерных программ-вымогателей
Криптоджекинг (майнинг криптовалют с использованием чужих ресурсов)
Кибершпионаж (несанкционированный доступ 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
Заражение компьютеров вредоносным ПО, чтобы повредить устройства или остановить их работу
DoS-атака на веб-сайт, компьютерную сеть или программные сервисы (отказ в обслуживании)
Атаки на критически важную инфраструктуру
Распространение вредоносного ПО, запрещенной информации или изображений в интернете
Фишинг (рассылка электронных писем с целью заставить получателей сделать что-то, что подрывает их безопасность)
Смишинг (SMS-фишинг) и вишинг (голосовой фишинг), использующие SMS и телефонные звонки вместо электронной почты
Платформы Crime-as-a-Service (CaaS) - это торговые площадки в темном Интернете, предлагающие приобрести готовые наборы программ-вымогателей, фишинговые кампании, дампы учетных данных и DDoS-атаки по найму

КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРПРЕСТУПНОСТИ

1. Регулярно обновляйте программное обеспечение и операционную систему

2. Используйте антивирусное программное обеспечение и постоянно обновляйте его

3. Используйте надежные пароли

4. Никогда не открывайте вложения в спам-письмах

5. Не переходите по ссылкам в спам-письмах или на ненадежных сайтах

6. Не разглашайте личную информацию, если она не защищена

7. Обращайтесь напрямую к компаниям по поводу подозрительных запросов

8. Обратите внимание на URL-адреса веб-сайтов, которые вы посещаете

9. Следите за своими банковскими выписками

ПРОКУРАТУРА ИНФОРМИРУЕТ ВСЕХ ГРАЖДАН!

БУДЬТЕ БДИТЕЛЬНЫМИ!

disk.yandex.ru/i/WaxOnz8z...

disk.yandex.ru/i/VgQM6cWL...;

disk.yandex.ru/i/I06gdo2q...;

disk.yandex.ru/i/VieGq2HB...

disk.yandex.ru/i/WaxOnz8z...