# Киберпреступность

# Введение

- Мы храним огромные объемы информации в компьютерах и часто хотим эту информацию скрыть. Сегодня, как никогда ранее, актуальна проблема защиты личных и конфиденциальных данных. По мере роста развития информационных технологий и развития систем безопасности, растет и количество киберпреступлений. Невозможно создать идеальную систему безопасности. В любой системе есть уязвимость

- **Цель**: изучить способы профилактики киберпреступности и способы борьбы с ней

- **Гипотеза**: Я считаю, что знание о киберприступниках и киберпреступлениях необходимо для работы с информацией в современном мире.

# Задачи

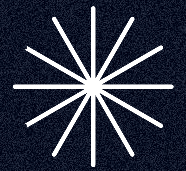
**01.** Выяснить что такое киберприступность

**02.** Изучить виды киберприступности

**03.** Выяснить как избежать обмана

# Киберпреступность

Киберпреступностью является любая преступная активность в виртуальном пространстве (киберпространстве). В некоторых киберпреступлениях осуществляются прямые атаки на компьютеры или другие устройства с целью вывода их из строя. В других киберпреступлениях компьютеры используются киберпреступниками для распространения вредоносных программных кодов, получения незаконной информации, хищения личных данных с целью мошенничества.



# категории киберпреступлений:

## Насильственный

или иные потенциально опасные (угроза физической расправы, киберпреследование, детская порнография, киберэкстремизм, кибертерроризм);

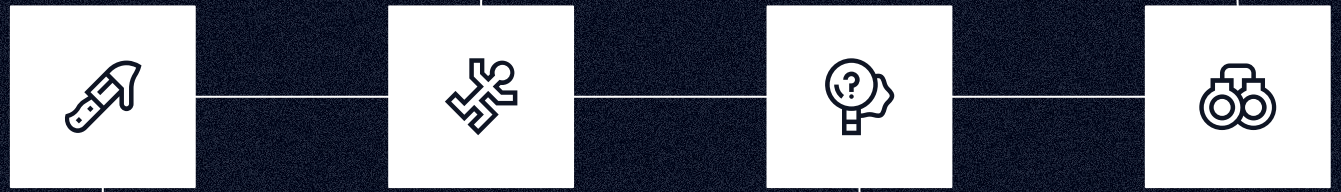
## Ненасильственный

противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество, реклама услуг проституции в сети Интернет, незаконный оборот наркотиков с использованием сети Интернет, азартные игры в сети Интернет, отмывание денег с помощью электронного перемещения, деструктивные киберпреступления и другие киберпреступления).

# Существует четыре наиболее распространенных способа, которыми пользуются киберпреступники:

DDOS атаки: создание огромного количества запросов к серверу или службе с использованием коммуникационных сетевых протоколов с целью вывода из строя объекта воздействия.

незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д.



использование вредоносных программ, которое базируется на злоупотреблении компьютерами и сетями.

комбинация социальной инженерии и вредоносного кода: жертву принуждают к определенным действиям что впоследствии приводит к заражению системы при помощи первого метода

# Группы Правонарушения

**Нарушение авторского права**

Незаконное копирование и распространение произведения, а также плагиат.

**Спам**

Массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получать.

**Социальные и политически мотивированные киберпреступления**

изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей

**Преступления на почве ненависти и домогательства**

домогательства и рассылка оскорбительных сообщений и вброс ложных новостей, касающихся определенной группы лиц.

# Группа правонарушений

**Терроризм**

Комплекс незаконных действий, создающих угрозу государственной безопасности, личности и обществу.

**Кибербуллинг**

намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации

**Груминг**

Тактический подход взрослого человека к несовершеннолетнему, как правило, с сексуальными целями

**Шпионаж**

Хакеры распространяют вирусы в сети

# 01. Для собственной безопасности следует

1.Используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;
2.Установите антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и другую технику;
3.Не загружайте файлы из непроверенных источников;
4.Не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;
5.Не сообщайте никому свои пароли и личные данные;
6.Откажитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги;
7.Используйте сложные пароли, состоящие из комбинаций цифр и букв ИЛИ ИНЫХ СИМВОЛОВ;
8.Воздержитесь от паролей -— дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

# Вывод

Сегодня преступления в сфере информационных технологий стали опасными для общественности. Несмотря на то, что компьютерные преступления появились сравнительно недавно, они быстро развиваются. Слабая подготовка правоохранительных органов по расследованию такого рода преступлений и высокий уровень скрытности преступников, способствует развитию киберпреступлениям и привлекает все больше и больше людей

К вопросу о киберпреступности нужно отнестись очень серьезно. Технологии в современном мире не стоят на месте и быстро развиваются, что дает новые возможности для совершения нового рода киберпреступлений. Правительственным органам нужно довольно серьезно заняться решением проблемы киберпреступности, иначе это может привести к необратимым последствиям