

КИБЕРМОШЕННИЧЕСТВО В 2021 ГОДУ И СПОСОБЫ ЗАЩИТЫ

Введение

Актуальность выбранной мною темы заключается в том, что для снижения угрозы в Интернет пространстве со стороны мошенников необходимо знать существующие виды этих угроз и меры предотвращения их.

Цель – выявить существующие способы защиты от кибермошенничества в 2021 году.

Задачи:

Определить сущность понятия кибермошенничества;

Охарактеризовать кибермошенничество;

Изучить историю возникновения кибермошенничества;

Выявить существующие способы защиты от кибермошенничества;

Предложить методы по усовершенствованию системы кибербезопасности.

Что такое кибермошенничество?

Кибермошенничество является одним из видов киберпреступления, цель которого – причинение материального или иного ущерба путем хищения личной информации пользователя.

Основные каналы, по которым мошенники могут взаимодействовать со своей жертвой:

- Электронная почта;
- Сайты;
- Соцсети и мессенджеры;
- Программы и приложения;
- Телефонный звонок и СМС



Какие существуют способы преступлений в Интернете?

Киберсквоттинг

Тайпсквоттинг

Ноах – программы

Коммерческие утилиты

Создание искусственного вирусного программного обеспечения

Интернет-магазины

Мошенничество с использованием телекоммуникации



Как появилось кибермошенничество?

- **1 этап (1972-1991 гг.)**

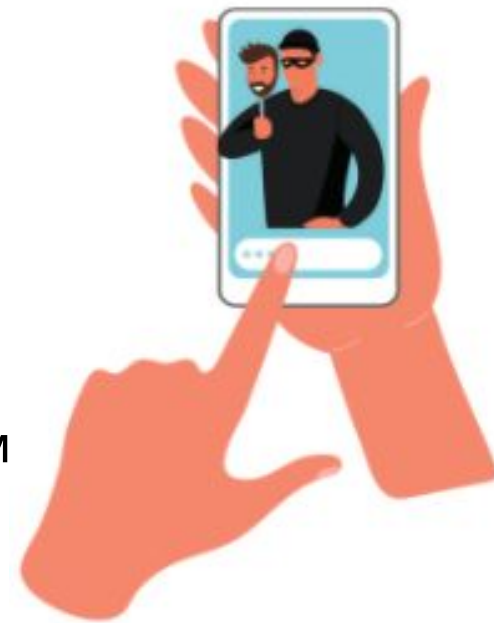
Период характеризуется становлением интернет преступности. Преступления совершаются узким кругом лиц, зарождается специализация компьютерных преступников.

- **2 этап (1991-2001 гг.)**

Интернет становится средой совершения традиционных преступлений. Период характеризуется созданием и внедрением «хакеров».

- **3 этап (2001 г. - настоящее время)**

Интернет преступность приобретает межнациональный характер.



Куда обращаться в случае столкновения с кибермошенничеством?

МВД России



Роспотребнадзор



Банк России



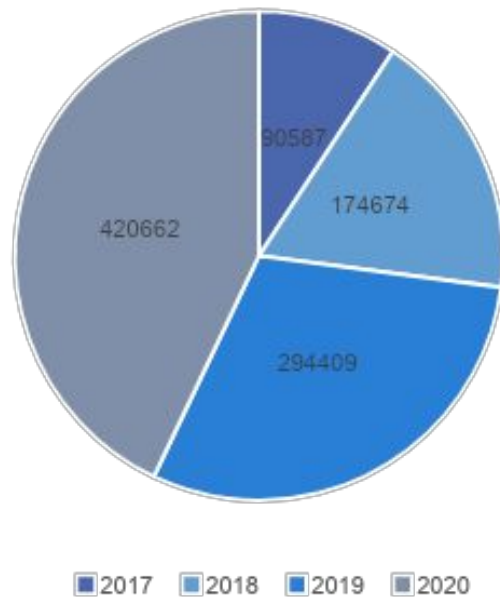
Финансовый
уполномоченный



Прокуратура



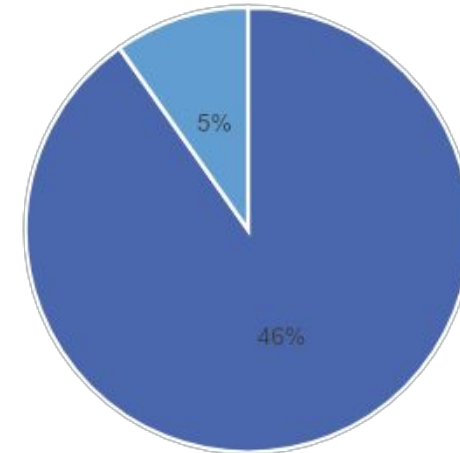
Статистика киберпреступлений



Динамика киберпреступлений показывает беспрецедентный рост. В 2017 году было зарегистрировано 90587 преступлений, в 2018 – 174674 преступлений, в 2019 – 294409, а за январь–октябрь 2020 – 420662. При этом одним из характерных признаков киберпреступлений является довольно низкий процент раскрываемости.

Почему киберпреступления имеют низкую раскрываемость?

- Специалистов, которые одновременно обладали бы знаниями компьютерной техники и технологий с одновременным пониманием юриспруденции, практически, не существуют.
- Низкая осведомленность населения о способах совершения мошеннических действий.
- Низкий уровень информационной безопасности.



■ Обычные преступления ■ Киберпреступления

Как можно усовершенствовать безопасность в Интернете?

- Необходимо больше специалистов, обладающих знаниями в сфере информационных технологий, вычислительной техники, связи
- Нужна четкая единая методическая база, которая будет действительно эффективна при раскрытии дистанционных мошенничеств
- Необходимо обобщать и анализировать данные для использования полученной информации при выработке мер противодействия и в целях предупреждения киберпреступлений



Памятка по безопасности в Интернете

- Никогда не распространяйте в социальных сетях информацию о ваших личных данных
 - Нельзя разглашать информацию ваших банковских карт
 - Используйте сложные пароли для персональных страниц
 - Всегда используйте антивирусную программу
 - Не скачивайте из Интернета непроверенные файлы
 - Никогда не сохраняйте пароли в браузере
- Не встречайтесь с людьми, с которыми вы познакомились в Интернете
 - Регулярно просматривайте операции с банковскими картами
 - Будьте предельно осторожны к письмам



Заключение

Таким образом – кибермошенничество — как и технический прогресс — не стоит на месте, а идет в ногу со временем. Изобретаются все новые способы хищения чужого имущества.

Сегодня для защиты прав граждан от кибермошенников существуют правовые статьи, специальные органы, памятки по предотвращению вреда. Однако несмотря на это, статистика свидетельствует об увеличении мошенничества в Интернете. Органы власти различных стран должны предпринять ряд мер для ее устранения, чтобы защитить население своих государств.



СПАСИБО ЗА ВНИМАНИЕ!
