**Отдел по борьбе с противоправным использованием информационно-коммуникационных технологий Главного управления Министерства внутренних дел Российской Федерации по Саратовской области**

# *Противодействие преступлениям в сфере информационно-коммуникационных технологий, о новых способах совершения мошенничеств с применением инструментов социальной инженерии.*

Киберпреступление – это тип криминальной активности, которая включает в себя использование компьютерных сетей (включая Интернет) в качестве основного средства совершения преступления.

## Категории киберпреступлений

| Преступления, направленные на сети или устройства | Преступления, использующие устройства для осуществления преступной деятельности |
|---|---|
| Вредоносное ПО | Фишинг/кража данных |
| Взлом (хакерство) и др. | Запрещенный/незаконный контент |
| Неправомерный доступ | Онлайн мошенничество/кража |
| | Склонение к суициду |
| | Вовлечение в экстремистскую деятельность и др. |

# Мошенничество с использованием информационно-коммуникационных технологий

«Фишинг» - кража идентификационных данных (например, ФИО, пароль и номер банковской карты). Злоумышленники пользуются невнимательностью граждан и завладевают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и соцсетях, электронной рассылки писем. Преступники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные.

- Двойники интернет-магазинов
- Копии сервисов интернет-банкинга
- Фальшивые сайты благотворительности, туроператоров или авиакомпаний

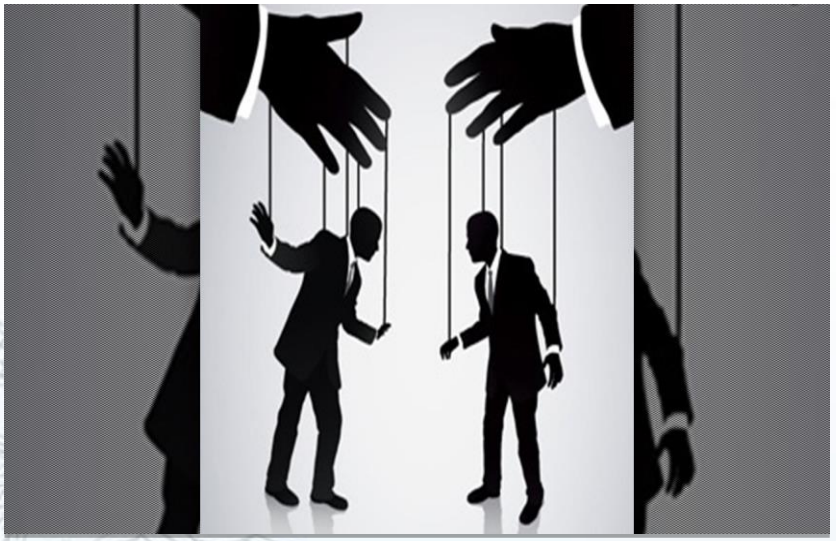
# Мошенничество с использованием информационно-коммуникационных технологий

«Социальная инженерия» - это метод получения необходимого доступа к информации, основанный на особенностях психологии людей.

Родственник попал в аварию, стал соучастником преступления и т.д.

Звонок от представителя силовых структур. Жертву пытаются запугать, вменить вину

Звонки от представителей банка, сервиса «Государственных услуг», различный фондов (пенсионного, социального страхования), мобильного оператора и др



# Мошенничество с использованием информационно-коммуникационных технологий

«Дропы» - подставные лица, которые «прогоняют» по картам похищенные деньги для обналичивания.
Сотрудничают с мошенниками добровольно или по незнанию.

За сбыт средств платежей (банковских карт) предусмотрена ответственность по ст. 187 УК РФ.

С 25 июля 2024 года вступили в законную силу изменения, внесенные в Федеральный закон от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе». Согласно изменениям банк в одностороннем порядке имеет право заблокировать денежные переводы на «сомнительные счета», а также отключить возможность использования онлайн-банкинга.

# С какими мошенническими схемами можно столкнуться в 2024 году?

- Схема 1. Операторы сотовой связи
- Схема 2. Предложения от лжеброкеров
- Схема 3. Общение с работодателем
- Схема 4. Звонки или сообщения от знакомых
- Схема 5. Оплата услуг по фейковому QR-коду
- Схема 6. Звонки и сообщения из банка
- Схема 7. Звонки и сообщения от государственных ведомств

# Мошенничество с использованием информационно-коммуникационных технологий

Статья 20 Уголовного кодекса Российской Федерации.
Уголовной ответственности подлежит лицо, достигшее ко времени совершения преступления 16-летнего возраста.

***ч.2 ст. 20 УК РФ*** — с 14 лет по следующим составам преступлений ст. 105, 111, 112, 126, 131,132, 158, 161, 162, 163, 166, ч.2 ст. 167, 205, 205.3, ч.2 ст. 205.4, ч.2 ст. 205.5, 205.6, 206, 207, ч.2 ст. 208, 211, ч.2 ст.212, ч.2,3 ст. 213, 214, 222.1, 223.1, 226, 229, 267, 277, 360, 361.

# Пропаганда и вовлечение в экстремистскую деятельность

Понятие экстремистской деятельности (экстремизм) закреплено в Федеральном законе от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»

- Распространение в сети Интернет экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, а также предоставление к ним доступа пользователям файлообменных сетей, влечет административную ответственность по **ст. 20.29 КоАП РФ.**
- Распространение материалов, содержащих призывы к осуществлению экстремистской деятельности, возбуждению ненависти либо вражды, а также унижению достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, призывы к осуществлению террористической деятельности или оправдание терроризма может повлечь уголовную ответственность по **ст. ст. 205.2, 280, 282 УК РФ.**

# Суицидальный контент

- **п. «д», ч. 2 ст. 110 УК РФ** предусмотрена ответственность за «Доведение лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего, совершенное в публичном выступлении, публично демонстрирующимся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»).
- **п. «д», ч. 3 ст. 110.1 УК РФ** введена ответственность за «Склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства» а равно Содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению или обещанием скрыть средства или орудия совершения самоубийства, если такое деяние совершено в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»).
- **ч. 2 ст. 110.2 УК РФ** также предусматривает ответственность за «Организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, сопряженное с публичным выступлением, использованием публично демонстрирующегося произведения, средств массовой информации или информационно-телекоммуникационных сетей (включая сеть «Интернет»).

# За киберпреступления предусмотрена ответственность:

- **ст. 128.1 УК РФ – Клевета;**
- **ст. 242 УК РФ – Незаконное распространение порнографических материалов или предметов ( до 6 лет лишения свободы);**
- **ст. 242.1 УК РФ Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (до 10 лет лишения свободы);**
- **п. «г» ч. 3 ст. 158 УК РФ –кража с банковского счёта, а равно в отношении электронных средств платежа ст. 159 УК РФ – Мошенничество (до 10 лет лишения свободы);**
- **ст. 159.6 УК РФ – Мошенничество в сфере компьютерной информации (до 10 лет лишения свободы);**
- **ст. 163 УК РФ – Вымогательство;**
- **ст. 272 УК РФ – Неправомерный доступ к компьютерной информации (до 7 лет лишения свободы);**
- **ст. 273 УК РФ – Создание, использование и распространение вредоносных компьютерных программ (до 5 лет лишения свободы);**
- **ст. 274 УК РФ – Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (до 5 лет лишения свободы).**

## *Неочевидные угрозы социальных сетей*

1. *Сбор и анализ данных.*
2. *Манипулирование общественным мнением.*
3. *Спам и фишинг.*
4. *Кибербуллинг и харассмент.*
5. *Deepfake.*
6. *Продвижение вредных стереотипов.*
7. *Сетевая зависимость.*

## *Как защититься?*

1. *Используйте настройки приватности.*
2. *Не делитесь слишком личной информацией в интернете.*
3. *Используйте сложные пароли.*
4. *Включите двухфакторную аутентификацию.*
5. *Не переходите по подозрительным ссылкам.*
6. *Регулярно обновляйте программное обеспечение.*
7. *Проверяйте настройки безопасности.*

**Управлением по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерством внутренних дел Российской Федерации**

***Создан официальный телеграм-канал***

***Вестник Киберполиции***

**https://t.me/cyberpolice_rus**