**ПРИМЕНЕНИЕ МЕТОДОВ ПСИХОЛОГИЧЕСКОГО АНАЛИЗА В СОЦИАЛЬНОЙ ИНЖЕНЕРИИ**

**АННОТАЦИЯ**

В данной статье приводится одна из главных проблем современного общества — мошенничество в интернете, а в частности, в социальных сетях. В статье рассмотрены виды и формы социальной инженерии. Приведен анализ различных способов мошенничества в социальных сетях, такие как взлом страниц, переход по ссылке, отправка зараженных файлов и т.д.

**АNNOTATION**

  This article presents one of the main problems of modern society - fraud on the Internet, and in particular on social networks. The article considers the types and forms of social engineering. The analysis of various methods of fraud on social networks, such as hacking pages, clicking on the link, sending infected files, etc.

**Ключевые слова:** социальная инженерия, социальные сети, мошенничество, глобальная сеть, уязвимость.

**Keywords**: social engineering, social networks, fraud, global network, vulnerability.

Информация представляет собой один из наиболее важных ресурсов современного общества, поэтому обеспечение комплексной защиты информации является одной из важных и приоритетных задач в информационной безопасности. С каждым годом информационные системы защиты совершенствуются в связи с постоянным развитием современных технологий. Информационные системы защиты могут продолжительное время функционировать в заданных пределах и решать поставленные задачи, что нельзя сказать о самом человеке. Люди, так и будут оставаться основной уязвимостью, со своими слабостями, предрассудками, являясь наиболее слабым звеном в цепочке информационной безопасности. Глобальная сеть, как основной и самый быстрый источник получения и распространения информационных ресурсов, таит в себе немало угроз [1].

Мошенничество в социальных сетях.

Понятие, как мошенничество, на сегодняшний день, очень распространенное. С законодательной точки зрения, мошенничество представляет собой хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (статья 159 УК РФ) [2]. На сегодняшний день в России мошенничество распространено довольно широко и оно очень разнообразно. Можно сказать, стало массовым явлением.

Уголовный кодекс определяет способы мошенничества, которые заключаются в хищении чужого имущества или приобретении права на чужое имущество одним из двух указанных в нем способов: обман и злоупотребление доверием.

Основная часть видов мошенничества известна уже многие времена. Они могут быть самыми разнообразными. Традиционные виды мошенничества [2]:

- в сфере кредитования;

- при получении выплат;

- с использованием платежных карт;

- в сфере страхование и др..

Мошенничество в глобальной сети, представляет собой самую незащищенную сферу социально-общественных отношений. Вычислить преступников очень сложно, практически невозможно: отсутствует доказательная база по различным видам преступлений в сети. В УК РФ в принципе отсутствует норма, которая могла бы регулировать социально-общественные отношения в Глобальной сети, а, следовательно, предусматривать ответственность за совершение преступных деяний в ней [4].

Таким образом, самое уязвимое место в защите информационной системе от мошенничества это человек. Никакие программно-аппаратные средства не защитят вас, если вы будете неосторожны и невнимательны.

**Список литературы:**

1. ЯКЛАСС. Глобальная сеть Интернет. Общая характеристика, особенности построения инженерия / [Электронный ресурс] – Режим доступа: https://www.yaklass.ru/materiali?mode=

cht&chtid=464/ (Дата обращения: 01.03.2020).

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 18.02.2020)// Мошенничество, 08.12.2003, N 162-ФЗ, статья 159.
2. Статистика социальных сетей в России 2019 / [Электронный ресурс] – Режим доступа: https://livedune.ru/blog/statistika\_socsetej\_v\_rossii/ (Дата обращения: 01.03.2020).
3. Аюпова К.В., Аюпов Р.Ш. Социальная инженерия — современная угроза информационной безопасности // Актуальные проблемы и перспективы инновационного развития современной России.–2014.–С. 125-128.