**Ю. М. Графова,**
аспирант,
Казанский инновационный университет имени В. Г. Тимирясова

# СИСТЕМА ПРОФИЛАКТИКИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

**Аннотация**. Одной из самых актуальных проблем преступности во все времена является ее рост, напрямую зависящий от периода развития общества и дефицитов, которое оно переживает. Сейчас современное общество переживает мощный период цифровизации, который, как следствие, ведет к снижению логического анализа, происходящего на различных уровнях психики человека. В работе предложена система профилактических действий, направленных на предотвращение мошенничества с использованием социальной инженерии.

**Ключевые слова**: социальная инженерия, мошенничество, преступление, профилактика, уголовная ответственность

# PREVENTION SYSTEM FRAUD USING SOCIAL ENGINEERING

**Abstract**. One of the most pressing problems of crime at all times is its growth, which directly depends on the period of development of society and the deficits that it is experiencing. Now modern society is going through a powerful period of digitalization as a stage of development, which in its negative manifestations is characterized by two deficits: a lack of socialization and a decrease in horizons, which, as a result, lead to a decrease in the level of logical analysis of what is happening at various levels of the human psyche. The paper proposes an author's system of preventive actions aimed at preventing fraud using social engineering.

**Keywords**: social engineering, fraud, crime, prevention, criminal liability

Цифровизация как этап развития общества явилась тем фактором, который позволил сформироваться новому виду преступности – киберпреступности. Известно, что на сегодняшний день преступники, специализирующиеся на цифровых видах преступлений, являются самыми неисследованными с точки зрения психологического и криминологического подходов. В настоящее время недостаточно исследований, позволяющих определить портрет киберпреступника, его психологические особенности, истинный мотив и цель, которые побуждают его к противоправным действиям.

Ввиду отсутствия портрета такого преступника отсутствует возможность для составления полного портрета жертвы подобных преступлений.

Портреты преступника и жертвы являются важной составляющей частью при формировании правил профилактики таких преступлений, однако отсутствуют соответствующие исследования, которые позволяли бы установить четкие цели и причины, побуждающие преступника к совершению преступления.

На сегодняшний день одним из основных видов противоправных деяний в рассматриваемой сфере является мошенничество с использованием социальной инженерии, которая требует более детального изучения в психолого-криминологическом и уголовно-правовом разрезах.

В связи с этим представляется логичным разделить систему профилактических действий, направленных на предотвращение мошенничества с использованием социальной инженерии, на четыре основные группы мер:

1. Образовательно-просветительские меры, направленные на обучение граждан, лиц без гражданства и сотрудников организаций, учреждений, предприятий независимо от форм собственности новым методам противодействия социоинженерным атакам в целях повышения культуры информационной безопасности и поддержания должного уровня цифровой гигиены.

2. Технологические (предупредительно-охранительные) меры, направленные на тщательную проверку входящих ссылок и иной цифровой информации, поступающей на любого рода средства связи, а также не использование повышенной степени защиты своей личной цифровой информации.

3. Правовые меры, направленные на разработку норм, устанавливающих ответственность за такого рода преступления, защиту прав потерпевших лиц, совершенствование имеющегося законодательства, регулирующего правоотношения в указанной сфере, контролирующие исполнение такого законодательства и на разных уровнях его применения.

4. Психологические меры, направленные на профилактику стресса.

Указанные группы мер крайне важны для эффективной выработки профилактических мер противодействия мошенничеству с использованием социальной инженерии.

В подавляющем большинстве преступлений, связанных с передачей личных данных преступникам уровень критического мышления у жертв снижен до минимального значения. Критическое мышление – это умение всесторонне анализировать информацию и делать обоснованные, объективные выводы [1]. Также под критическим мышлением понимают способность ставить под сомнение любую информацию, в том числе собственные убеждения.

Ключевыми признаками критического мышления являются способность наблюдать;  концентрироваться и сохранять внимание и др.

Несмотря на наличие врожденных личностных характеристик, при общих вводных каждый способен увеличить уровень своего критического мышления. Существуют разнообразные способы, в зависимости от темперамента и склонностей человека к усвоению информации, повысить свой уровень критического мышления. Прибегая к давно известным формам обработки информации, можно выделить межличностных подход, включающий в себя дискуссии, обсуждения, и индивидуальный, куда входят самостоятельный поиск и анализ информации, работа с найденной информацией, построение логических рассуждений и выводов, аргументация при дискуссии, обнаружение ошибок в мышлении, в том числе собственных.

Развитие и формирование критического мышления до высокого уровня позволяют оценивать криминогенную обстановку и принимать управленческие решения в целях минимизации последствий и предотвращения социоинженерных атак.

Важным нюансом является тот факт, что главным инструментом преступлений в социальной инженерии является манипуляция на эмоциях и конструирование ситуаций, которые могут выглядеть совершенно реальными.

Формирование достаточного уровня критического мышления увеличит способность жертвы в процессе осознания рисков при контакте с кибермошенниками прежде, чем предоставлять конфиденциальную информацию или совершать финансовые операции.

Завершая рассуждения, подчеркнем, что для эффективной профилактики мошенничества с использованием социальной инженерии предлагаем использовать все четыре меры системно, комплексно и неразрывно. Одновременное использование этих мер позволить снизить вероятность совершения социоинженерной атаки злоумышленниками.

**Список литературы**

1. Садова А.Р., Хиль Ю.С., Пащенко Т.В., Тарасова К.В. Измерение критического мышления взрослых: методология и опыт разработки // Современная зарубежная психология. 2022. Т. 11, № 4. С. 115–116.

**В. В. Денисович,**
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова,
Южно-Уральский государственный университет
(национальный исследовательский университет)

## КРИМИНОЛОГИЧЕСКИЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ МЕТАВСЕЛЕННЫХ

**Аннотация.** Суть использования этических категорий в цифровых правоотношениях сводится к тому, чтобы определить рамки публичных дискуссий относительно содержания на основе идей признания и социальной справедливости. Востребованность концепции этических основ в использовании виртуальных пространств базируется на том, что этика позволяет сформировать направление будущего нормотворчества в области использования метавселенных. Новые нормы морали могут стать основой для формирования современных нормативных актов.

**Ключевые слова:** метавселенные, криминологические риски метавселенных, виртуальное пространство, цифровой аватар человека, метагаллактики

## ETHICAL BASES OF META-UNIVERSES USE

**Abstract.** The essence of the use of ethical categories in digital legal relations comes down to defining the framework of public discussions, regarding the content on the basis of the ideas of recognition and social justice. The demand for the concept of ethical foundations in the use of virtual spaces is based on the fact that ethics allows to form the direction of future normativity in the use of meta-universes. New norms of morality can become the basis for the formation of modern normative acts.

**Keywords:** metavillages, criminological risks of metavillages, virtual space, digital human avatar, metagallactics