НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

К 145-летию со дня основания
Томского государственного университета

МИР ЧЕЛОВЕКА В ФОКУСЕ ПСИХОЛОГИЧЕСКИХ МЕТАПРАКТИК

МАТЕРИАЛЫ
VIII СИБИРСКОГО ПСИХОЛОГИЧЕСКОГО ФОРУМА

Томск
Издательство Томского государственного университета
2022

совладающего поведения» (Р. Лазарус); миссисипская шкала (МШ) посттравматического стрессового расстройства (ПТСР) (Н.М. Кеан, Дж.М. Кэддел, К.Л. Тэйлор).

Вторым этапом психокоррекционной групповой работы стал психолого-педагогический тренинг. Задачи и цели ГКП были представлены авторами в трех основных программных блоках. По результатам исследования на третьем этапе была осуществлена посттренинговая психодиагностика.

Результаты исследования. Для определения эффективности психолого-педагогической коррекционной программы были выявлены индикаторы оценки адаптационных возможностей человека. Показатель положительной динамики и улучшение психоэмоционального состояния испытуемых свидетельствовали о правильности подобранного инструментария в психокоррекционной работе. Статистическая обработка проходила с использованием коэффициента ранговой корреляции Спирмена, U-критерия Манна–Уитни и т-теста с использованием пакета SPSS Statistics 22.0. Далее был проведен корреляционный анализ и представлены его результаты. Исследование обнаружило обратную взаимосвязь между формированием личностного адаптационного потенциала и уровнями тревожности и депрессии.

В заключение отметим, что цель проведения групповой психокоррекционной программы достигнута, выполнены все задачи, которые были на нее возложены, а также доказана эффективность ее практического использования.

Литература

1. Василюк Ф.Е. Психология переживания. М. : Инфра-М, 2017. 214 с.
2. Конопкин О.А. Психологические механизмы регуляции деятельности. М. : Наука, 2010. 186 с.
3. Линехан М. Руководство по тренингу навыков при терапии пограничного расстройства личности. СПб. : Диалектика, 2020. 336 с.
4. Тарабрина Н.В. Практикум по психологии посттравматического стресса. СПб. : Питер, 2001. 272 с.
5. Формы и методы кризисной психотерапии: методические рекомендации. М. : М-во здравоохранения РСФСР, 1987. 21 с.

УДК 159.9:33

УЯЗВИМОСТИ В ПСИХОЛОГИЧЕСКОЙ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА В ЦИФРОВОЙ СРЕДЕ И ОСНОВНЫЕ ВИДЫ МОШЕННИЧЕСТВА

Марина Вячеславовна Рыжкова, Михаил Владимирович Чиков, Ирина Евгеньевна Розынко
Томский государственный университет, Томск, Россия

Развитие цифровых технологий обусловливает появление ряда серьезных проблем и угроз для человека в двухкомпонетной реальности (онлайн и офлайн): этические проблемы, проблема автономности, свободы выбора и воли, физического здоровья, размывания границ виртуального и реального, киборгизация и др. В условиях инерционности институциональных систем высокая скорость технологических изменений порождает целый ряд отрицательных внешних эффектов (манипулирование пользователем, высокий уровень финансового мошенничества, сопротивление цифровизации и др.) и ставит перед человеком проблему личной безопасности в цифровой среде.

Экспоненциальный рост мошенничества в цифровой среде – один из наиболее существенных негативных эффектов текущего этапа цифровизации [1]. Скорость, с которой внедряются цифровые технологии, оказывает значительное давление на психологическую устойчивость человека и создает оптимальные условия для мошенников, поскольку борьба с уязвимостью цифровых процессов и внедрение комплексных защитных систем для многих пока не являются приоритетной задачей.

Для построения комплексных систем психологической и финансовой защиты необходимо выявить все существующие каналы уязвимостей, где человек в большей мере подвержен риску стать жертвой мошенников, поэтому основная цель нашего исследования состояла в типологизации основных видов мошенничества в Интернете. Эволюция мошенничества протекает лавинообразными темпами, вследствие чего методы и формы обмана совершенствуются ежедневно, что вызывает необходимость актуального мониторинга новых форм обмана, совершаемого через Интернет, в том числе с использованием новейших методов анализа данных [2, 3].

Для достижения поставленной цели необходимо было решить следующие задачи:

1. Провести онлайн-опрос среди студентов об актуальных видах мошенничества в сети Интернет.
2. Обработать полученные результаты онлайн-опроса.
3. Представить обобщенную типологизацию основных видов мошенничества в сети Интернет.

На первом этапе исследования мы подготовили и разослали гугл-форму для неанонимного опроса студентов, куда включили следующие открытые вопросы:

1. С какими мошенническими действиями сталкивались вы или ваши знакомые / родственники в последнее время в Интернете?
2. Какие новые финансовые / психологические / прочие угрозы возникли за период пандемии или за последний год?
3. Экзотические виды мошенничеств в Интернете в последнее время – опишите известные вам случаи.
4. Особое мнение – любые соображения, которые вы хотели бы сообщить по теме «Мошенничество с использованием современных цифровых технологий».
5. Считаете ли вы, что государство должно контролировать Интернет? И в какой степени и формах?

Всего опрос прошли 94 студента экономических специальностей 1–2-го курсов. Опрос проходил с 10 по 12 декабря 2021 г. В результате обработки ответов мы получили обобщенную сборку видов мошенничества в сети Интернет по различным каналам уязвимостей.

1. Обман по номеру телефона:
- анонимные звонки с просьбой о помощи;
- звонки из «банка» с информацией о взломе / краже данных карточки;
- звонки с сообщением о выигрыше (Столото, лотерея и т.д.).

2. Обман через личные аккаунты:
- кража аккаунта в социальной сети «ВКонтакте» с вымогательством / просьбой проголосовать / перевести деньги / помочь материально (похороны, болезнь и т.д.);
- кража аккаунта на платформе Steam;
- кража почты (mail.ru, gmail.com) или данных телефона (icloud).

3. Обман через сервисы для продажи товаров (Юла / Авито):
- отправка товаров через сервис доставки;
- мнимый перевод с подделкой чека;
- продажа несуществующего / испорченного товара.

4. Обман через популярные аккаунты в социальных сетях:
- покупка в онлайн-магазине, которого по факту не существует;
- гайды и онлайн-курсы;
- гадания и раскладывания карт таро, гивы;
- ставки, прогнозы и каперство, раскрутка счета, предложение войти в бизнес.

5. Обман через рекламные каналы:
- ролики с призывом помочь больному / умирающему ребенку;

- реклама ненадежных онлайн-казино;
- подделка брендовых вещей (утверждают, что со скидкой или напрямую от поставщика).

6. Обман через фишинг:
- сайт, копирующий ввод данных с клавиатуры;
- подделка реальных сайтов.

7. Обман через сервисы по поиску работы:
- предложение зарабатывать на дому крупные суммы денег;
- перед устройством на работу просят отправить личные данные;
- внести предоплату перед устройством на работу.

8. Обман через сделки в Интернете:
- сделки на платформе Binance;
- вывод денег из букмекерской конторы;
- продажа внутриигровой валюты / предметов.

Таким образом, признак, который мы положили в основу группировки основных видов мошенничества, – это канал уязвимости (тип технологии), через который осуществляется мошенничество.

Также важно отметить, что большинство опрошенных считают, что государство должно осуществлять контроль за интернет-пространством (84% респондентов за контроль в определенных рамках), но при условии сохранения законности и основных прав граждан. Контроль прежде всего должен проводиться над финансовыми операциями, действиями пользователей для выявления следов незаконной активности. Интересно, что респонденты указывают на принципиальную недостижимость анонимности и защиты персональных данных в современном цифровом мире и неизбежную вследствие этого слежку за их действиями со стороны как государства, так и злоумышленников.

Литература

1. Al-Hashedi K.G., Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019 // Computer Science Review. 2021. Vol. 40. Art. 100402.
2. Kemp S. Fraud reporting in Catalonia in the Internet era: Determinants and motives // European Journal of Criminology. 2022. Vol. 19 (5). P. 994–1015.
3. Wang L., Cheng H., Zheng Z., Yang A., Zhu X. Ponzi scheme detection via oversampling-based Long Short-Term Memory for smart contracts // Knowledge-Based Systems. 2021. Vol. 228. Art. 107312.

УДК 159.95

ВЫРАЖЕННОСТЬ АГА-ПЕРЕЖИВАНИЯ В ИНСАЙТНЫХ ЗАДАЧАХ И ИНСАЙТНЫХ РЕШЕНИЯХ

Анна Джумберовна Савинова, Александра Валерьевна Чистопольская, Наталья Юрьевна Лазарева

Ярославский государственный университет им. П.Г. Демидова, Ярославль, Россия

Исследование выполнено при финансовой поддержке гранта РНФ 22-18-00358.

Согласно теории изменения репрезентации, ага-переживание как внезапное появление яркой позитивной эмоции в конце решения возникает при изменении репрезентации. Изменение репрезентации – атрибут инсайтных задач, сконструированных так, чтобы для нахождения правильного ответа требовалось посмотреть на задачу под другим углом. Со временем представление о прочной связи ага-переживания и инсайтных задач начало давать трещину, поскольку инсайтные задачи могут решаться без изменения репрезентации и ага-переживания [3, 4], а неинсайтные задачи могут получать высокие оценки инсайтности [1, 4]. В связи с этим