**УДК 004.056.5**

# ПРОТИВОДЕЙСТВИЕ КИБЕРОБМАНУ: ПСИХОЛОГИЯ ЗАЩИТЫ В ЭПОХУ ЦИФРОВЫХ УГРОЗ.

Скачкова А.И., студент гр. ИБт-221, III курс, Бритова Н.Н., студент гр. ИБт-221, III курс, Луцык Е.М., студент гр. ИБт-221, III курс
Научный руководитель: Коротин В.О
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

Мошенничество продолжает оставаться одной из самых актуальных проблем современного общества, требующей глубокого анализа и системного подхода к ее решению. Понимание психологических механизмов, делающих людей уязвимыми к манипуляциям, играет ключевую роль в предотвращении обмана. В данной статье мы проанализируем основные факторы, способствующие успеху мошенников, и предложим стратегии защиты от их уловок.

Мошенничество в современном мире представляет собой значительную угрозу, требующую тщательного изучения и анализа в контексте информационной безопасности. Для завладения чужими финансами мошенники активно используют психологические приемы и техники нейролингвистического программирования.

## Как нас обманывают в сети: Психологические уловки мошенников

Человеческая психология играет ключевую роль в восприимчивости к обману. Мошенники искусно используют базовые инстинкты, такие как доверие, стремление к выгоде или страх потери. Эти внутренние механизмы часто затмевают критическое мышление, особенно в стрессовых ситуациях.

Один из основных принципов, используемых мошенниками, — это создание ложного чувства безопасности. Они представляются надежными людьми, предлагают "выгодные" сделки или ссылаются на авторитетные источники. Это заставляет жертву поверить в легитимность предложения. Кроме того, мошенники активно манипулируют эмоциями: страхом, тревогой, стыдом или даже эйфорией. Эмоциональное состояние снижает способность анализировать ситуацию, подталкивая к поспешным и не обдуманным решениям.

## Социальные факторы и контекст

Социальный контекст также оказывает значительное влияние на вероятность попадания в сети мошенников. Феномен "социального доказательства" — когда человек принимает решение, основываясь на действиях других, — широко используется мошенниками. Например, если

жертва видит положительные отзывы о сомнительном предложении, она с большей вероятностью доверится ему.

Кроме того, социальная изоляция и недостаток поддержки увеличивают уязвимость человека. В таких условиях человек теряет доступ к ресурсам, которые могли бы помочь распознать обман. Особенно опасны ситуации, связанные с повышенным стрессом, когда люди становятся менее склонными к критическому анализу.

**Цифровая эпоха: новые возможности для мошенников**

С развитием информационных технологий мошенничество приобрело новые формы и масштабы. Кибермошенники используют сложные схемы, такие как фишинг, поддельные сайты и вредоносные программы. Даже образованные и технически подкованные люди могут стать жертвами из-за недостатка знаний о современных угрозах мошенничества.

Одним из распространенных приемов является создание чувства экстренной необходимости. Жертве говорят, что время на принятие решения истекает, что вынуждает ее действовать спонтанно, не задумываясь о дальнейших последствиях. Этот метод основан на психологическом явлении "принуждение к действию", когда давление времени подавляет способность критически оценивать ситуацию.

**Внутренние факторы уязвимости**

Психологическая предрасположенность также играет важную роль. Люди с низкой самооценкой, желанием угодить другим или склонностью к избеганию конфликтов более восприимчивы к манипуляциям. Мошенники могут использовать чувство вины или стыда, чтобы заставить жертву действовать против здравого смысла.

Интересно отметить эффект "иллюзии невосприимчивости". Многие люди считают, что они менее подвержены мошенничеству, чем окружающие. Это заблуждение может привести к игнорированию большинства предупреждающих знаков.

**Методы защиты от мошенничества**

1. Обучение критическому мышлению

Развитие навыков анализа информации и осознание своих уязвимостей — первый шаг к защите. Школы, университеты и общественные организации могут проводить программы по повышению финансовой грамотности и информационной безопасности.

2. Распознавание фишинговых атак

Умение выявлять подозрительные электронные письма, сообщения и сайты помогает избежать многих мошеннических схем. Простые правила, такие как проверка отправителя письма и отказ от перехода по подозрительным ссылкам, могут спасти от серьезных последствий.

3. Создание безопасного цифрового пространства

Использование надежных паролей, двухфакторной аутентификации и регулярное обновление программного обеспечения помогают защитить личные данные.

4. Создание групп для людей, которые подверглись на мошеннические уловки.

5. Проверка источников информации

Перед тем как доверять кому-либо или совершать действия, связанные с деньгами или личными данными, важно проверять надежность источника.

Используйте официальные сайты компаний, звоните на горячие линии или обращайтесь напрямую в организацию, чтобы убедиться в подлинности запроса.

Будьте осторожны с незнакомыми номерами телефонов, особенно если звонящий представляется сотрудником банка, службы безопасности или правоохранительных органов.

6. Избегание эмоциональных решений

Мошенники часто используют психологическое давление: создают ощущение срочности, страха или радости ("победили в лотерею", "счет заблокирован").

Прежде чем действовать, сделайте паузу и проанализируйте ситуацию. Спросите себя: "Почему это происходит именно сейчас?" и "Что я могу потерять, если соглашусь?".

Если вы чувствуете тревогу или волнение, обсудите ситуацию с близкими или друзьями — они могут помочь взглянуть на нее объективно.

7. Ограничение публичной информации в интернете

Мошенники часто собирают информацию о своих жертвах через социальные сети, форумы и другие открытые источники.

Ограничьте доступ к личной информации (фото, адрес, номер телефона, место работы) в социальных сетях.

Не делитесь своими планами, финансовыми данными или другими конфиденциальными сведениями в публичных постах или сообщениях.

8. Использование технологий для защиты

Установите антивирусное программное обеспечение и регулярно обновляйте его. Это поможет защитить устройства от вредоносных программ.

Включите функции блокировки подозрительных звонков и SMS в смартфоне. Многие операторы связи предлагают такие услуги.

Используйте менеджеры паролей для создания и хранения сложных уникальных паролей.

9. Финансовая осмотрительность

Никогда не переводите деньги незнакомцам или компаниям, чья репутация не проверена.

Будьте осторожны с предложениями, которые кажутся слишком выгодными ("гарантированный доход", "легкие деньги").

Храните важные финансовые документы в безопасном месте и регулярно проверяйте состояние своих счетов на предмет несанкционированных операций.

10. Обращение в правоохранительные органы

Если вы стали жертвой мошенников, немедленно сообщите об этом в полицию или соответствующие службы. Чем быстрее вы обратитесь за помощью, тем больше шансов минимизировать ущерб.

Сохраняйте все доказательства (переписки, скриншоты, записи разговоров), чтобы облегчить расследование.

Оказание помощи пострадавшим, включая финансовую и психологическую поддержку, является важной частью борьбы с мошенничеством. Создание поддерживающих сообществ позволяет жертвам делиться опытом и предостерегать других.

## Заключение

Борьба с мошенничеством — задача, требующая многоуровневого подхода, который объединяет действия отдельных людей, общества в целом и современные технологии. Важно повышать уровень осведомленности населения о методах психологического воздействия, развивать навыки критического анализа информации и укреплять цифровую грамотность. Эти меры способны существенно сократить количество пострадавших от мошеннических схем. Лишь совместными усилиями мы сможем сформировать защищенное информационное пространство, где каждый сможет безопасно и уверенно пользоваться преимуществами цифровых технологий.

Мошенничество остается одним из главных вызовов современности, требующим осознания как технических аспектов, так и глубинных психологических механизмов, делающих нас уязвимыми. Понимая эти механизмы, мы можем разработать эффективные методы противодействия и минимизировать риски стать жертвой обмана. Основные рекомендации включают развитие критического мышления, повышение осведомленности о современных угрозах и использование проверенных методов цифровой безопасности. Только через совместные усилия общества, государства и частных лиц возможно создать надежную систему защиты от мошенничества в цифровую эпоху.

## Список литературы:

1. Основы цифровой грамотности и кибербезопасности: учебное пособие / Т.А. Бороненко, В.С. Федотова, И.Н. Пальчикова [и др.]. – Санкт-Петербург : ЛГУ им.А.С.Пушкина, 2021. – 431 с.

2. Стрижов Е.Ю. Психология нравственной надежности и мошенничества: Монография / Е.Ю. Стрижов. – москва : ЮНИТИ-ДАНА: Закон и право, 2009. – 305 с.