УДК 159.9:001.891; 159.9:001.891.57; 159.9:007; 343.3/.7
МРНТИ 15.01.77; 10.77.51

Т.Г. Маханов, Н.К. Мырзабаев
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

НАУЧНО-ПРАКТИЧЕСКИЙ АНАЛИЗ ДИАЛОГОВ ИНТЕРНЕТ-МОШЕННИКОВ С ПРИМЕНЕНИЕМ ИНСТРУМЕНТОВ ПСИХОЛОГИЧЕСКОГО И НЕЙРОЛИНГВИСТИЧЕСКОГО ПРОГРАММИРОВАНИЯ

Аннотация. Статья посвящена анализу диалогов интернет-мошенников с позиций психолингвистики, нейролингвистического программирования и криминалистики. Актуальность исследования обусловлена стремительным ростом киберпреступлений, совершаемых с помощью методов социальной инженерии, которые представляют угрозу национальной безопасности. Эмпирическую базу составили 530 аудиозаписей телефонных разговоров злоумышленников с операторами Антиколл-центра (общей продолжительностью более 105 часов). Методологически работа опирается на дискурс-анализ, контент-анализ и структурно-функциональный подход. В результате выявлены ключевые манипулятивные паттерны: стратегии установления авторитета через имитацию официального статуса и профессиональный жаргон; психологические триггеры дефицита, страха и бесплатности; техники рефрейминга для получения SMS-кодов; приемы введения в трансовое состояние и эмоциональных качелей. Отдельно проанализированы способы сопротивления жертв – логический аудит, юмор и доведение до абсурда. Рассмотрен зарубежный опыт регулирования ИИ и синтетического контента (ЕС, Великобритания, Сингапур, Китай, Индия). Сформулированы практические рекомендации для граждан, правоохранительных органов, банков и разработчиков систем цифровой безопасности.

Ключевые слова: интернет-мошенничество; социальная инженерия; нейролингвистическое программирование; манипулятивная стратегия; дипфейк; когнитивный иммунитет; цифровая безопасность.

Т.Ғ. Маханов, Н.Қ. Мырзабаев
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

ПСИХОЛОГИЯЛЫҚ ЖӘНЕ НЕЙРОЛИНГВИСТИКАЛЫҚ БАҒДАРЛАМАЛАУ ҚҰРАЛДАРЫ НЕГІЗІНДЕ ИНТЕРНЕТ-АЛАЯҚТАРДЫҢ ДИАЛОГТАРЫНА ҒЫЛЫМИ-ПРАКТИКАЛЫҚ ТАЛДАУ

Аннотация. Мақалада интернет-алаяқтардың диалогтары психолингвистика, нейролингвистикалық бағдарламалау және криминалистика тұрғысынан талданады. Зерттеудің өзектілігі ұлттық қауіпсіздікке қауіп төндіретін әлеуметтік инженерия әдістерімен жасалған киберқылмыстардың қарқынды өсуіне байланысты. Зерттеудің эмпирикалық базасын шабуылдаушылар мен Антиколл-орталық операторлары арасындағы телефон сөйлесулерінің 530 аудиожазбасы (жалпы ұзақтығы 105 сағаттан астам). Әдістемелік тұрғыдан жұмыс дискурстық талдауға, контенттік талдауға және құрылымдық-функционалдық тәсілге негізделген. Нәтижесінде негізгі манипуляциялық заңдылықтар анықталды: ресми мәртебеге еліктеу және кәсіби жаргон арқылы беделге негізделген ықпал ету стратегиялары; тегін ұсынысқа негізделген психологиялық триггерлер; SMS-кодтарды алу үшін рефрейминг әдістері; эмоциялық ауытқуларды басқару тәсілдері. Жәбірленушілерге қарсы тұру тәсілдері, яғни логикалық талдау, әзіл және абсурдқа дейін жеткізу тәсілі де бөлек талданады. Жасанды интеллект пен синтетикалық мазмұнды реттеудің шетелдік тәжірибесі қарастырылды (ЕО, Ұлыбритания, Сингапур, Қытай, Үндістан).

Азаматтарға, құқық қорғау органдарына, банктерге және цифрлық қауіпсіздік жүйелерін әзірлеушілерге арналған практикалық ұсынымдар тұжырымдалған.

Түйінді сөздер: интернет-алаяқтық; әлеуметтік инженерия; нейролингвистикалық бағдарламалау; манипулятивтік стратегия; дипфейк; когнитивті иммунитет; цифрлық қауіпсіздік.

T.G. Makhanov, N.K. Myrzabayev
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, the Republic of Kazakhstan

SCIENTIFIC AND PRACTICAL ANALYSIS OF INTERNET FRAUDSTER DIALOGUES USING PSYCHOLOGICAL AND NEURO-LINGUISTIC PROGRAMMING TOOLS

Abstract. The article analyzes the dialogues of Internet scammers from the perspective of psycholinguistics, neuro-linguistic programming and criminology. The relevance of the study is due to the rapid growth of cybercrimes committed by social engineering methods that pose a threat to national security. The empirical base consisted of 530 audio recordings of telephone conversations between intruders and Anti-Call Center operators (with a total duration of more than 105 hours). Methodologically, the work is based on discourse analysis, content analysis, and a structural and functional approach. As a result, key manipulative patterns were identified: strategies for establishing authority through imitation of official status and professional jargon; psychological triggers of scarcity, fear, and gratuitousness; reframing techniques for receiving SMS codes; techniques for inducing a trance state and emotional swings. The methods of victim resistance are analyzed separately – logical audit, humor and bringing to the point of absurdity. The foreign experience of regulating AI and synthetic content (EU, UK, Singapore, China, India) is considered. Practical recommendations are formulated for citizens, law enforcement agencies, banks and developers of digital security systems.

Keywords: Internet fraud; social engineering; neuro-linguistic programming; manipulative strategie; deepfake; cognitive immunity; digital security.

DOI: 10.52425/25187252_2026_40_143

Введение. Стремительное развитие информационно-коммуникационных технологий сопровождается не только позитивными социально-экономическими эффектами, но и ростом новых форм противоправной деятельности. Одной из наиболее динамично прогрессирующих угроз является интернет-мошенничество.

На последнем заседании Национального курултая Президент Казахстана Касым-Жомарт Токаев заявил, что «распоясавшиеся мошенники превратились в реальную угрозу национальной безопасности»[1].

Преступное явление в последние годы приобрело масштабы транснационального феномена. По данным международных организаций (FATF, UNODC, Интерпол), темпы прироста числа киберпреступлений, совершаемых с использованием методов социальной инженерии (далее – СИ), ежегодно составляют 15-20%. По прогнозам, к 2027 году киберпреступность обойдется миру в 23 триллиона долларов (рост на 175% по сравнению с 2022 г.)[2]. При этом значительная доля таких преступлений остается латентной. Потерпевшие не всегда осознают факт психологического манипулирования либо не обращаются в правоохранительные органы из-за чувства стыда или неверия в раскрытие преступления.

Особую тревогу вызывает то обстоятельство, что современные интернет-мошенники все чаще отказываются от традиционных массовых фишинговых рассылок в пользу персонализированных, многокомпонентных атак. В основе этих атак лежат не столько технические уязвимости программного обеспечения, сколько уязвимости когнитивной и

[1] Опубликован полный текст выступления Токаева на Национальном курултае [Электронный ресурс] – Режим доступа: https://tengrinews.kz/kazakhstan_news/opublikovan-polnyiy-tekst-vyistupleniya-tokaeva-natsionalnom-590731/ (дата обращения: 15.02.2026).

[2] 250+Cybercrime Statistics for 2026 [Электронный ресурс] – Режим доступа: https://www.brightdefense.com/resources/cybercrime-statistics/#fl-main-content (дата обращения: 14.05.2026).

эмоциональной сферы человека. Злоумышленники целенаправленно используют механизмы доверия, страха, авторитета, срочности и взаимности – ключевые рычаги воздействия, изученные в социальной психологии и нейролингвистическом программировании (далее – НЛП).

Несмотря на обилие криминологических и уголовно-правовых исследований, посвященных интернет-мошенничеству, анализ непосредственно диалоговой ткани преступной коммуникации остается недостаточно разработанным.

Большинство работ фокусируется либо на статистической характеристике деяний, либо на описании типовых схем «развода» без погружения в лингвистическую и психотехническую структуру разговора. Между тем именно в диалоге, в его речевых паттернах, метапрограммах, предикатах, якорях и стратегиях присоединения скрыт ключ к пониманию того, почему вполне рациональные, критически мыслящие люди добровольно переводят деньги незнакомцам.

Настоящее исследование направлено на восполнение указанного пробела посредством анализа диалогов интернет-мошенников с использованием инструментов психологии и НЛП. Подобный анализ предполагает не только теоретическую реконструкцию применяемых техник, но и выявление признаков (маркеров) манипулятивного воздействия, имеющих значение для правоприменительной практики.

Актуальность исследования обусловлена тремя основными факторами:

- высокими темпами роста количества интернет-мошенничеств в странах постсоветского пространства, включая Республику Казахстан (далее – РК), где дистанционная деятельсность на протяжении длительного времени и цифровизация финансовых услуг создали благоприятную среду для атак СИ;
- недостаточной разработанностью методик выявления и доказывания фактов психологического манипулирования в рамках уголовного судопроизводства;
- необходимостью создания научно обоснованных алгоритмов противодействия, учитывающих не только техническую, но и коммуникативную составляющую преступления.

Цель исследования – осуществить многоуровневый анализ диалогов интернет-мошенников, выявить наиболее эффективные психолингвистические паттерны, а также разработать практические рекомендации для профилактики преступности данной категории.

Научная новизна работы заключается в том, что впервые на материале русско- и казахскоязычных диалогов проводится систематическое сопоставление заявленных мошенниками ролей (легенд) с конкретными языковыми маркерами НЛП.

Материалы и методы. Эмпирическую базу исследования составили уникальные полевые материалы, собранные авторами за период 2023-2025 гг. Теоретико-методологический каркас работы базируется на синтезе классических и современных научных трудов по психологии влияния, СИ и «человеческому хакингу», НЛП, психолингвистике архетипов и речевой манипуляции. Для анализа цифровой трансформации мошенничества привлекались научные работы последних лет.

Методологическую основу исследования составили общенаучные и специальные методы познания: логический и сравнительный методы; метод правового моделирования; контент-анализ; метод дискурс-анализа; метод лингвистического профилирования; анализ виктимного поведения.

Результаты, обсуждение. На основе проведенного анализа фонограмм разговоров обозначены следующие критериальные признаки НЛП[3], психологического инструментария и прагматических установок, используемых злоумышленниками в процессе телефонного взаимодействия.

I. Стратегии установления авторитета и социального доверия

[3] Нейролингвистическое программирование (НЛП) – это метод практической психологии, направленный на моделирование эффективного поведения, саморазвитие и конструктивное общение через изменение мышления и эмоций.

В ходе изучения аудиозаписей установлено, что мошенники активно используют имитацию официального статуса, присваивая себе роли сотрудников социально значимых институтов (ЦОН, Казпочта, поликлиника, налоговая служба, организации жилищно-коммунального хозяйства (таких как электросети) или финансовых учреждений (банков)):

- использование профессионального жаргона: для придания веса своим словам злоумышленники оперируют такими терминами, как «диспансеризация», «иммунологический анализ», «лицензия на продажу алкоголя», «внеплановая поверка электросчетчика» и «финансовый мониторинг»;

- ссылка на нормативные акты: для подавления критического мышления используются ссылки на «постановления Минздрава», «новые порядки продления лицензий», «подачу налоговой декларации» и «требования управления транспорта».

II. Психологические триггеры и инструменты НЛП , в т.ч. боевого

В диалогах прослеживаются четкие паттерны[4] манипуляции, направленные на создание стрессовой ситуации или чувства долга:

- триггер[5] дефицита и срочности: жертву убеждают, что запись в поликлинику «забита на месяцы», «курьер приедет в течение часа», «срок сдачи декларации истек» или «лицензия перестанет действовать с 1 января». В коммунальных сценариях используется легенда об «аварии на подстанции», из-за которой якобы горят электроприборы;

- триггер страха за здоровье, тревоги: активно используется тема эпидемий («вспышки метапневмовируса», «гонконгский грипп», «серьезные осложнения на легкие») для принуждения к прохождению рентгена или сдачи анализов. В сценариях с налогами или коммунальными службами используются угрозы «штрафов», «ареста счетов» или «порчи имущества из-за скачков напряжения»;

- триггер «бесплатности» и выгоды: мошенники снижали критическое восприятие, подчеркивая, что предлагаемые услуги абсолютно бесплатны в рамках государственных программ (в сфере медицины – «бесплатная томография/УЗИ по новой программе», в сфере услуг – продление лицензии «без повторной оплаты», в ЖКХ – компенсация за сгоревшую технику при условии получения «акта поверки»);

- использование «да-сетов»[6]: спрашивая о самочувствии или подтверждая личные данные (ФИО, дата рождения), мошенники добиваются от жертвы серии утвердительных ответов, что снижает психологический барьер перед финальной просьбой.

III. Техники рефрейминга[7] и обработки возражений

Ключевым этапом мошенничества является получение SMS-кода. Когда жертва выражает сомнение, мошенники используют рефрейминг – переименование опасного действия в безопасное:

- фокусы языка: код подтверждения от государственных сервисов (например, 1414, eGov или uchet.kz) называют «номером талона», «номером электронной очереди», «номером акта» или «кодом подтверждения отказа»;

- минимизация значимости: жертву убеждают, что код «не несет юридической силы» и нужен лишь для «закрепления гарантии» или «внесения в журнал посещений»;

- логическая ловушка «двух лиц»: используется псевдоправовой скрипт: «Я являюсь

[4] Паттерн (от англ. pattern – «шаблон», «образец», «узор») – это повторяющаяся схема, модель или структура, используемая для решения типовых задач в различных областях.

[5] Триггер (от англ. trigger – «спусковой крючок») – это стимул, событие, слово или образ, вызывающий автоматическую, часто мгновенную и сильную эмоциональную, психологическую или поведенческую реакцию.

[6] «Да-сеты» (или ставки «Да» в сетах) – это вид пари в букмекерских конторах на теннис, означающий, что конкретный игрок выиграет как минимум один сет в матче.

[7] Рефрейминг (от англ. reframe – «вставить в новую рамку ту же картину», «по-новому сформулировать») – это метод изменения восприятия ситуации, проблемы или поведения путем смены контекста или смысла, через которую они рассматриваются.

первым лицом (отправителем), вы вторым лицом (получателем), третьим лицам код не говорите, а мне – можно».

IV. Нейролингвистический анализ отказа и сопротивления

Аудиозаписи демонстрируют различные уровни сопротивления жертв (операторов), от легкого сомнения до механизма боевого НЛП:

- технические препятствия как форма защиты: жертвы (операторы) часто ссылаются на «плохую связь», «заполненную память телефона» или отсутствие очков, что дезориентирует мошенника и заставляет его терять контроль над сценарием;
- логический аудит: некоторые жертвы (операторы) задают вопросы, на которые у мошенников нет готовых скриптов, например, о связи «1414» с электросетями или о том, почему маска не защищает от запаха, но защищает от вируса;
- юмор и доведение до абсурда: в ряде случаев жертвы (операторы) начинают подыгрывать, приглашая «врача» на блины с медом или прося денег в долг, что приводит к агрессии или прекращению звонка со стороны мошенника.

Дополнительно стоит отметить, что использование знакомых системных уведомлений (1414, eGov, uchet.kz) служит лингвистическим «якорем» доверия, т.к. эти сервисы официально используются в повседневной жизни.

Таким образом, исследование показывает, что современный телефонный мошенник – это не просто технический специалист, а обученный манипулятор, использующий СИ[8]. Они детально прорабатывают легенды, адаптируясь под текущую новостную повестку (эпидемии, изменения в законодательстве и т.д.).

Основные признаки манипуляции в диалогах:

1. Навязывание услуги, о которой жертва не просила (анализы, поверки).
2. Требование продиктовать код из SMS, даже если в самом сообщении написано «никому не передавать».
3. Переход на личности или агрессивный тон при попытке жертвы уточнить данные руководства.

Таким образом, современное мошенничество с использованием информационно-телекоммуникационных технологий (далее – ИТТ) представляет собой организованную форму преступной деятельности, приобретающую массовый характер. В этой связи в рамках настоящего исследования был проведен анализ научных публикаций психологов, специализирующихся в области изучения данного вида преступлений.

Так, Е.В. Зотина определяет данный феномен как «хищение чужого имущества путем обмана или злоупотребления доверием, совершаемое в результате взаимодействия преступника и жертвы с применением технологий сбора и обработки информации» [1, 16 стр.].

А.А. Калиев утверждает, что «интернет-мошенничество сочетает в себе традиционные формы преступности с новыми технологиями и психологическими приемами, составляющими основу социальной инженерии» [2, 295 стр.].

Эмпирические данные, полученные А.Е. Кулакаевой, свидетельствуют о том, что «значительная часть жертв мошенничества (35,6%) подвергается выраженному психологическому стрессу» [3, 385 стр.].

Ключевым механизмом совершения таких преступлений выступает СИ, определяемая как криминальное манипулирование и целенаправленное воздействие на эмоционально-волевую сферу жертвы посредством психолого-речевых приемов.

С.П. Баранцев и другие ученые характеризуют этот процесс как «взлом» человеческого

[8] Социальная инженерия – психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации.

сознания» [4, 21 стр.]. При этом Е.А. Полтаева подчеркивает, что «методы НЛП-воздействия в мошенничестве направлены непосредственно на подсознание, снижая критичность восприятия информации» [5, 45 стр.].

По словам И.В. Салынцева, «основной механизм НЛП, которым пользуются мошенники – речевая подстройка под клиента. Особенно подвержены воздействию НЛП люди истерического, художественного или сангвинического склада.

При этом противостоят гипнозу дискретики, недоверчивые люди мыслительного склада, склонные к анализу. Именно они начинают сомневаться в честности и достоверности «сказочных» предложений, а уточняющими вопросами разрывается цепочка внушений – команд мошенника»[9].

Анализ научной литературы свидетельствует о том, что интернет-мошенничество представляет собой не только имущественное преступление, совершаемое с использованием информационно-коммуникационных технологий, но и сложное психологическое воздействие на личность потерпевшего. В отличие от традиционных форм хищения, основным инструментом преступника выступает не техническое средство само по себе, а способность манипулировать сознанием человека посредством методов социальной инженерии, речевого внушения, установления доверительного контакта и воздействия на эмоционально-волевую сферу.

В рамках изучения теоретического базиса психологии воздействия были верифицированы психологические и дискурсивные механизмы, лежащие в основе формирования манипулятивных стратегий.

1. Психолингвистический подход к анализу диалогов позволяет выявить арсенал методов воздействия на сознание жертвы. В научной литературе выделяются следующие механизмы:

- подмена языковой картины мира: Л.А. Тугай и А.А. Миронова указывают, что «в процессе диалога мошенник создает воображаемую модель реальности, выгодную для него, что ведет к отключению критического мышления жертвы» [6, 110 стр.];

- использование архетипов: А.А. Миронова и Л.А. Тугай рассматривают «речевую манипуляцию как актуализацию архетипических схем («Великая мать», «Божественный ребенок», «Мудрец», «Герой»), которые выступают «спусковым крючком» для запуска неконтролируемых действий» [7, 55 стр.];

- перлокутивный эффект: в рамках теории речевых актов Л.А. Тугай переносит акцент на «результат воздействия – перлокуцию. Основными типами вызываемых реакций в мошенническом дискурсе являются: страх и паника, чувство вины и ответственности, иллюзия срочности и спешки, а также ложное доверие» [8, 492 стр.].

2. Инструментарий НЛП и речевые тактики в диалогах. Исследователи выделяют специфические техники и тактики, используемые преступниками для дестабилизации жертвы:

- техника перегрузки: С.П. Баранцев описывает ее как «метод, основанный на превышении лимита восприятия поступающей информации, что ведет к иррациональному поведению» [4, 43 стр.];

- коммуникативная подстройка и «отзеркаливание»: мошенник присоединяется к лексике жертвы и использует аудиальные предикаты («услышала?», «я говорил»). Л.А. Тугай и А.А. Миронова отмечают «варьирование обращений от официально-деловых до дружеских для создания атмосферы «экстремальной откровенности» [7, 57 стр.];

- ритмизация и временные границы: преступник задает жесткий ритм диалога в рамках «здесь и сейчас» («до одиннадцати успеваете?»), создавая искусственный цейтнот;

- эмоциональные качели: как отмечает Л.А. Тугай, «мошенники прибегают к резкому

[9] Как не попасть под гипноз телефонных мошенников (интервью врача) [Электронный ресурс] – Режим доступа: https://www.zakon.kz/sovety/5059278-kak-ne-popast-pod-gipnoz-telefonnyh.html (дата обращения: 14.05.2026).

изменению статуса жертвы (от повышения до занижения) и переходу от отношений кооперации к конфронтации» [8, 493 стр.];

- наведение трансового состояния: Согласно С.П. Баранцеву, «стадии наведения включают фиксацию внимания, депотенциализацию установок сознания и гипнотический отклик» [4, 51 стр.].

3. Трансформация тактик в условиях цифровизации. Современные исследования указывают на криминальную экспансию технологий искусственного интеллекта. Е.В. Зотина выделяет использование:

- «дипфейков» (видео и аудио): для имитации голоса и внешности близких людей;
- чат-ботов: для рассылки фишинговых сообщений, имитирующих индивидуальный стиль письменной речи, что повышает правдоподобность атак [1, 26 стр.].

Исследование психологических, психолингвистических и дискурсивных механизмов воздействия показывает, что современное интернет-мошенничество представляет собой высокоорганизованную систему манипулятивного влияния на сознание человека, основанную на использовании закономерностей восприятия, мышления и принятия решений. Преступники целенаправленно:

- конструируют искусственную картину реальности;
- активизируют архетипические модели поведения;
- вызывают необходимые эмоциональные состояния;
- формируют у потерпевшего иллюзию самостоятельного принятия решений.

Эффективность такого воздействия достигается посредством комплекса речевых техник, включающих информационную перегрузку, коммуникативную подстройку, создание искусственного дефицита времени, эмоциональную дестабилизацию и введение жертвы в состояние сниженного критического контроля.

На основании проведенного исследования необходимо сделать вывод о том, что диалог с интернет-мошенником – это сложная манипулятивная система. Она сочетает лингвистические инструменты (речевые акты, семантические повторы) и психологические методы (НЛП-техники, архетипы), направленные на введение жертвы в трансовое состояние и лишение ее способности к рациональной оценке ситуации.

Как мы уже отметили, современная научная литература рассматривает СИ не просто как технический метод взлома, а как «человеческий хакинг», т.е. искусство манипулирования людьми для получения конфиденциальной информации или доступа к системам.

Зарубежные исследователи подчеркивают, что человек остается самым слабым звеном в цепи кибербезопасности, поскольку злоумышленники эксплуатируют фундаментальные психологические черты: доверие, страх и любопытство.

К. Митник в своей работе «Искусство обмана» определил СИ как использование влияния и убеждения для введения жертвы в заблуждение [9]. Его классический цикл атаки (сбор информации, выстраивание доверия, эксплуатация, выход) остается фундаментальным для исследователей.

Р. Чалдини и его принципы влияния (авторитет, дефицит, взаимность, социальное доказательство) часто цитируются как основа психологических триггеров, используемых мошенниками [10, 145 стр.].

Исследовательские организации, такие как Verizon, в своих отчетах (DBIR) подтверждают, что до 82% всех утечек данных включают человеческий фактор, где СИ является основным методом[10].

[10] Data Breach Investigations Report [Электронный ресурс] – Режим доступа: https://www.verizon.com/business/resources/reports/2022-dbir-data-breach-investigations-report.pdf (дата обращения: 14.05.2026).

А.Б. Сманова и другие указывают на качественный скачок угроз из-за использования ИИ для клонирования голоса и создания видео, что делает схемы мошенничества (например, имитацию руководства в видеозвонках) почти неотличимыми от реальности [11, 207 стр.].

Ша Жу Пан отмечает долгосрочные психологические манипуляции в романтических или инвестиционных схемах, где жертву «откармливают» доверием перед окончательным финансовым «убоем» [12].

Аналитик Д. Тейлор выделяет новый тренд, когда пользователи, следуя инструкциям злоумышленников, неосознанно сами активируют вредоносный код или передают данные, считая это рутинной проверкой безопасности [13].

Наряду с этим зарубежный опыт основывается на сочетании жесткого законодательного регулирования и продвинутых технологических решений (таблица 1).

Европейский союз (Закон об ИИ / AI Act)	Первая в мире комплексная правовая база, которая классифицирует системы ИИ по уровню риска и вводит обязательную маркировку синтетического контента (дипфейков), чтобы пользователи могли распознать подделку[11].
Великобритания (Online Safety Act)	Закон возлагает на платформы ответственность за своевременное удаление мошеннического контента и вводит персональную ответственность руководителей компаний за несоблюдение норм безопасности[12].
Сингапур (Computer Misuse Act)	Обновленное законодательство криминализирует психологические манипуляции и «несанкционированный доступ через обман», признавая СИ самостоятельным составом преступления [14, 799 стр.].
Китай (Administrative Provisions on Deep Synthesis)	Введено обязательное уведомление пользователей об использовании технологий синтеза и строгая верификация личностей создателей контента [15, 49 стр.].
Индия	Использование систем UEBA (аналитика поведения пользователей и сущностей) позволяет ИИ выявлять аномалии (например, вход в систему из необычного места или странные финансовые транзакции) и автоматически блокировать аккаунты до подтверждения личности [16].

Таблица 1. Регуляторные стратегии ведущих юрисдикций в сфере ИИ и защиты пользователей от злоупотреблений

Таким образом, для эффективной защиты от взлома зарубежные исследователи предлагают применять следующие подходы:

- многофакторная аутентификация (MFA) – использование физических токенов или биометрии (FIDO2), которые сложнее скомпрометировать методами СИ, чем пароли из SMS [13];
- фильтрация контента – внедрение ИИ-фильтров для электронной почты (как в Gmail), которые блокируют до 99,9% вредоносных сообщений на основе лингвистического анализа [16];
- регулярное обновление ПО – патчинг уязвимостей, которые могут быть использованы в качестве «претекста» для атаки (например, фальшивые уведомления об обновлении браузера) [17];

[11] EU AI Act unpacked #8: New rules on deepfakes [Электронный ресурс] – Режим доступа: https://technologyquotient.freshfields.com/post/102jb19/eu-ai-act-unpacked-8-new-rules-on-deepfakes (дата обращения: 14.05.2026).

[12] Ofcom's approach to implementing the Online Safety Act [Электронный ресурс] – Режим доступа: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation (дата обращения: 14.05.2026).

- создание культуры здорового скептицизма, где поощряется перепроверка любых необычных запросов от руководства или финансовых служб через альтернативные каналы связи [13];

- политика чистого экрана и стола, а также строгий контроль физического доступа для предотвращения «следования по пятам» (tailgating)[13].

В конечном итоге исследователи сходятся во мнении, что технологии сами по себе не могут полностью остановить СИ. Только сочетание технологических барьеров с развитием цифровой грамотности и психологической устойчивости пользователей может создать надежную защиту.

Проведенный анализ зарубежных исследований позволяет сделать вывод о том, что противодействие социальной инженерии должно основываться на комплексной модели безопасности, сочетающей технические, организационные и психологические меры защиты.

Следовательно, современная система защиты от мошенничества должна рассматриваться как человеко-ориентированная модель кибербезопасности, в которой основным объектом защиты выступают не только информационные ресурсы, но и когнитивные процессы принятия решений пользователями.

Заключение. Проведенное исследование позволяет сформулировать комплекс практических рекомендаций, направленных на повышение эффективности профилактики, выявления и пресечения преступлений с использованием ИТТ.

I. Рекомендации для граждан (потенциальных жертв)

1. Формирование «когнитивного иммунитета» (разъяснять населению, что любые звонки, связанные с угрозами, срочностью, страхом и финансовыми операциями, являются потенциально мошенническими; формировать устойчивую установку: «Срочность + страх + просьба о коде = мошенничество»).

2. Запрет на передачу SMS-кодов в любых ситуациях (закрепить на уровне информационных кампаний абсолютное правило – SMS-коды, полученные от 1414, eGov, банков и иных сервисов, не передаются никому, включая сотрудников организаций; разъяснять, что реальные сотрудники никогда не запрашивают коды подтверждения).

3. Распознавание лингвистических ловушек (обучать граждан выявлять подмену понятий («номер талона», «номер акта», «регистрационный код»), ложную юридическую аргументацию («первое лицо – второе лицо – третьи лица»), псевдобюрократическую лексику; разъяснять, что любая попытка переименовать SMS-код – признак мошенничества).

4. Прерывание диалога как основная форма защиты, т.е. формировать поведенческий алгоритм (прервать разговор; самостоятельно перезвонить в банк или госорган по официальному номеру; сообщить о попытке мошенничества).

5. Использование защитных коммуникативных стратегий с одновременным обучением граждан приемам (затягивания диалога; постановки уточняющих вопросов; логической проверки легенды; намеренного нарушения сценария мошенника).

II. Рекомендации для правоохранительных органов

1. Использовать психолингвистическое профилирование (внедрить лингвистический анализ диалогов как элемент криминалистической характеристики интернет-мошенничества; использовать маркеры (псевдоюридический язык, жесткая ритмизация речи, повторяющиеся скрипты, речевые формулы давления).

2. Создать единый реестр типовых речевых сценариев мошенников (например: «сотрудник банка», «врач», налоговый инспектор», «электросети», «служба доставки», «родственник в

[13] Social Engineering [Электронный ресурс] – Режим доступа: https://www.cmu.edu/computing/safe/secure-your/dont-take-the-bait/social-engineering.html (дата обращения: 14.05.2026).

беде»).

3. Активно привлекать судебных лингвистов, психолингвистов, специалистов по речевому профилированию (для анализа аудиозаписей диалогов и идентификации мошеннических групп).

4. Обучать сотрудников Антифрод-центров путем включения в учебные программы основы НЛП-манипуляций, распознавания трансовых техник, методы разрушения мошеннических скриптов в режиме реального времени.

III. Рекомендации для банков и финансовых организаций

1. Включать в тексты SMS-кодов жесткие формулировки, психологические «якоря» опасности – «НИКОМУ НЕ СООБЩАЙТЕ КОД. СОТРУДНИКИ БАНКА НИКОГДА НЕ СПРАШИВАЮТ ЭТИ ДАННЫЕ».

2. При подозрительных операциях внедрять обязательную задержку транзакций (30-60 минут), дополнительные подтверждения.

3. Использовать ИИ-модели, фиксирующие резкие переводы средств, нетипичные сценарии операций, поведенческую аномалию.

IV. Рекомендации в сфере цифровой безопасности и ИИ

1. Противодействие дипфейкам (разработать систему распознавания синтетической речи, алгоритмов выявления дипфейк-аудио и видео; информирование населения о существовании дипфейк-аудио и видео голосов родственников).

2. Контроль чат-ботов (мониторинг массовых фишинговых рассылок; использование НЛП-фильтров для выявления мошеннических шаблонов).

На основании проведенного научно-практического анализа следует заключить, что противодействие интернет-мошенничеству требует комплексного подхода, сочетающего психолингвистическую диагностику, когнитивную профилактику, цифровую аналитику, институциональное взаимодействие.

Эффективное противодействие данному виду преступности возможно лишь при условии формирования психологической резистентности населения, обеспечения технологического превосходства над криминальной средой и систематической актуализации криминалистических методик.

Список использованной литературы:

1. Зотина, Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: автореф. дис. ... канд. юрид. наук: 5.1.4. Уголовно-правовые науки / Е.В. Зотина. – Казань, 2024. – 33 с.
2. Калиев, А.А. Отдельные аспекты расследования интернет-мошенничества / А.А.Калиев // Вестник Института законодательства и правовой информации РК. – 2025. – № 2. Том 80. – С. 294-301.
3. Кулакаева, А.Е. Оценка угроз мошенничества в мобильных телекоммуникационных сетях / А.Е. Кулакаева // Труды Карагандинского технического университета. – 2025. – № 3 (100). – С. 385-392.
4. Психологические аспекты противодействия телефонному мошенничеству в финансовой сфере: методические материалы / Авторы-составители: С.П. Баранцев, О.В. Медяник, Н.А. Низовских, О.А. Николаева. – Киров, Управление Министерства внутренних дел Российской Федерации по Кировской области области, 2024. – 60 с.
5. Полтаева, Е.А. Использование психологического воздействия рекламы в целях мошенничества / Е.А. Полтаева // Научные междисциплинарные исследования. – 2020. – № 3-2. – С. 42-47.
6. Тугай, Л.А. Психолингвистический подход к исследованию текстов мошеннического дискурса / Л.А. Тугай, А.А. Миронова // Вестник ЧелГУ. – 2024. – № 5 (487). – С. 107-113.
7. Миронова, А.А. Способы манипулирования как архетипическая схема в мошенническом дискурсе / А.А. Миронова, Л.А. Тугай // Этнопсихолингвистика. – 2025. – № 1 (20). – С. 42-59.
8. Тугай, Л.А. Мошеннический дискурс (перлокутивный эффект) / Л.А. Тугай // МНКО. – 2025. – № 1 (110). – С. 490-493.
9. Mitnick, K. The Art of Deception: Controlling the Human Element of Security / K. Mitnick, S. William. – Hoboken, New Jersey: John Wiley & Sons, Inc., 2002. – 368 p.

10. Naz, A. A comprehensive survey on social engineering-based attacks on social networks / A. Naz, et al. // International Journal of Advanced and Applied Sciences. – 2024. – № 11. – Pp. 139-154.

11. Smanova, A.B. Deepfake technologies and social engineering in online fraud forms, mechanisms, and legal challenges / A.B. Smanova, A.Zh. Muratova, Sh.R. Zhumagulova // Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия: Право. – 2025. – Т. 152. № 3. – С. 188-211.

12. Whittaker, J.M. Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘) / J.M. Whittaker, S. Lazarus, T. Corcoran // Journal of Economic Criminology. – 2024. – № 3. – 100052.

13. J. Taylor. Scam Yourself attacks: How social engineering is evolving [Электронный ресурс] – Режим доступа: https://www.helpnetsecurity.com/2025/01/21/scam-yourself-attacks/ (дата обращения: 14.05.2026).

14. Purwadi, M. Exploring The Policy Crisis and Legal Accountability of Cybercrime Perpetrators Employing Social Engineering-Based Phishing Techniques / M. Purwadi, A. Jamaludin // Research Horizon. – 2025. – № 5 (3). – Pp. 797-806.

15. Filipova, I.A. Legal Regulation of Artificial Intelligence: Experience of China / I.A. Filipova // Journal of Digital Technologies and Law. – 2024. – Vol. 2. No. 1. – Pp. 46-73.

16. Tiwari, S. Social Engineering Attacks: Trends, Psychological Triggers, and AIdriven Prevention [Электронный ресурс] / S. Tiwari // Preprints 2025. – Режим доступа: https://doi.org/10.20944/preprints202510.0663.v1 (дата обращения: 14.05.2026).

17. Salahdine, F. Social Engineering Attacks: A Survey [Электронный ресурс] / F. Salahdine, N. Kaabouch // Future Internet. – 2019. – Режим доступа: https://doi.org/10.3390/fi11040089 (дата обращения: 14.05.2026).

References:

1. Zotina, E.V. Moshennichestvo s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij i priemov social'noj inzhenerii: kriminologicheskoe issledovanie: avtoref. dis. ... kand. jurid. nauk: 5.1.4. Ugolovno-pravovye nauki / E.V. Zotina. – Kazan', 2024. – 33 s.

2. Kaliev, A.A. Otdel'nye aspekty rassledovanija internet-moshennichestva / A.A.Kaliev // Vestnik Instituta zakonodatel'stva i pravovoj informacii RK. – 2025. – № 2. Tom 80. – S. 294-301.

3. Kulakaeva, A.E. Ocenka ugroz moshennichestva v mobil'nyh telekommunikacionnyh setjah / A.E. Kulakaeva // Trudy Karagandinskogo tehnicheskogo universiteta. – 2025. – № 3 (100). – S. 385-392.

4. Psihologicheskie aspekty protivodejstvija telefonnomu moshennichestvu v finansovoj sfere: metodicheskie materialy / Avtory-sostaviteli: S.P. Barancev, O.V. Medjanik, N.A. Nizovskih, O.A. Nikolaeva. – Kirov, Upravlenie Ministerstva vnutrennih del Rossijskoj Federacii po Kirovskoj oblasti oblasti, 2024. – 60 s.

5. Poltaeva, E.A. Ispol'zovanie psihologicheskogo vozdejstvija reklamy v celjah moshennichestva / E.A. Poltaeva // Nauchnye mezhdisciplinarnye issledovanija. – 2020. – № 3-2. – S. 42-47.

6. Tugaj, L.A. Psiholingvisticheskij podhod k issledovaniju tekstov moshennicheskogo diskursa / L.A. Tugaj, A.A. Mironova // Vestnik ChelGU. – 2024. – № 5 (487). – S. 107-113.

7. Mironova, A.A. Sposoby manipulirovanija kak arhetipicheskaja shema v moshennicheskom diskurse / A.A. Mironova, L.A. Tugaj // Jetnopsiholingvistika. – 2025. – № 1 (20). – S. 42-59.

8. Tugaj, L.A. Moshennicheskij diskurs (perlokutivnyj jeffekt) / L.A. Tugaj // MNKO. – 2025. – № 1 (110). – S. 490-493.

9. Mitnick, K. The Art of Deception: Controlling the Human Element of Security / K. Mitnick, S. William. – Hoboken, New Jersey: John Wiley & Sons, Inc., 2002. – 368 p.

10. Naz, A. A comprehensive survey on social engineering-based attacks on social networks / A. Naz, et al. // International Journal of Advanced and Applied Sciences. – 2024. – № 11. – Pp. 139-154.

11. Smanova, A.B. Deepfake technologies and social engineering in online fraud forms, mechanisms, and legal challenges / A.B. Smanova, A.Zh. Muratova, Sh.R. Zhumagulova // Vestnik Evrazijskogo nacional'nogo universiteta imeni L.N. Gumileva. Serija: Pravo. – 2025. – T. 152. № 3. – S. 188-211.

12. Whittaker, J.M. Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘) / J.M. Whittaker, S. Lazarus, T. Corcoran // Journal of Economic Criminology. – 2024. – № 3. – 100052.

13. J. Taylor. Scam Yourself attacks: How social engineering is evolving [Jelektronnyj resurs] – Rezhim dostupa: https://www.helpnetsecurity.com/2025/01/21/scam-yourself-attacks/ (data obrashhenija: 14.05.2026).

14. Purwadi, M. Exploring The Policy Crisis and Legal Accountability of Cybercrime Perpetrators Employing Social Engineering-Based Phishing Techniques / M. Purwadi, A. Jamaludin // Research Horizon. – 2025. – № 5 (3). – Pp. 797-806.

15. Filipova, I.A. Legal Regulation of Artificial Intelligence: Experience of China / I.A. Filipova // Journal of Digital Technologies and Law. – 2024. – Vol. 2. No. 1. – Pp. 46-73.

16. Tiwari, S. Social Engineering Attacks: Trends, Psychological Triggers, and AIdriven Prevention [Jelektronnyj

resurs] / S. Tiwari // Preprints 2025. – Rezhim dostupa: https://doi.org/10.20944/preprints202510.0663.v1 (data obrashhenija: 14.05.2026).

17. Salahdine, F. Social Engineering Attacks: A Survey [Jelektronnyj resurs] / F. Salahdine, N. Kaabouch // Future Internet. – 2019. – Rezhim dostupa: https://doi.org/10.3390/fi11040089 (data obrashhenija: 14.05.2026).

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Талғат Ғабитұлы Маханов – Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының Ведомствоаралық ғылыми-зерттеу институты Қылмыстық процесс проблемаларын зерттеу орталығының бас ғылыми қызметкері, заң ғылымдарының магистрі, e-mail: makhanov1986@mail.ru.

Маханов Талгат Габитович – главный научный сотрудник Центра исследования проблем уголовного процесса Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юридических наук, e-mail: makhanov1986@mail.ru.

Makhanov Talgat Gabitovich – Chief Researcher at the Center for Criminal Procedure Research Interdepartmental Research Institute of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Master of Law Sciences, e-mail: makhanov1986@mail.ru.

Нұрланәлі Қошқарұлы Мырзабаев – Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының Ведомствоаралық ғылыми-зерттеу институты Ғылыми превенция және ведомствоаралық өзара іс-қимылды үйлестіру орталығының жетекші ғылыми қызметкері, e-mail: nurlanali_myrzabaev86@mail.ru.

Мырзабаев Нурланали Кошкарович – ведущий научный сотрудник Центр научной превенции и координации межведомственного взаимодействия Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: nurlanali_myrzabaev86@mail.ru.

Myrzabayev Nurlanali Koshkaruly – Leading Researcher at the Center for Scientific Prevention and Interagency Coordination Interdepartmental Research Institute of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, e-mail: nurlanali_myrzabaev86@mail.ru.