

Торайғыров университетінің
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Торайғыров университета

ТОРАЙҒЫРОВ УНИВЕРСИТЕТІНІҢ ХАБАРШЫСЫ

ЗАҢ СЕРИЯСЫ
2022 ЖЫЛДАН БАСТАП ШЫҒАДЫ



ВЕСТНИК ТОРАЙҒЫРОВ УНИВЕРСИТЕТА

ЮРИДИЧЕСКАЯ СЕРИЯ
ИЗДАЕТСЯ С 2022 ГОДА

ISSN 2958-8618

№ 2 (2024)

Павлодар

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

Юридическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО

о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания

№ KZ90VPY00046812

выдано

Министерством информации и коммуникаций
Республики Казахстан

Тематическая направленность

публикация результатов научных исследований, актуальных проблем
в области права, привлечение внимания к перспективным
и актуальным направлениям юридической науки

Подписной индекс – 76199

<https://doi.org/10.48081/ADPX5585>

Бас редакторы – главный редактор

Жетписов С.К.,
д.ю.н., доцент

Заместитель главного редактора Олжабаев Б. Х., *к.ю.н., ассоц.профессор*
Ответственный секретарь Жамулдинов В. Н., *к.ю.н., ассоц.профессор*

Редакция алкасы – Редакционная коллегия

Биштыга А.,	<i>доктор PhD, профессор (Республика Польша)</i>
Зайцев О. А.,	<i>д.ю.н., профессор (Российская Федерация)</i>
Ахмеджанова Г. Б.,	<i>д.ю.н., доцент</i>
Ишеков К.А.,	<i>д.ю.н., профессор (Российская Федерация)</i>
Дуйсенов Э. Э.,	<i>д.ю.н., профессор</i>
Дорожинская Е. А.,	<i>к.ю.н., доцент (Россия Федерация)</i>
Балымов Е. К.,	<i>доктор PhD,</i>
Аюпова З. К.,	<i>д.ю.н., профессор</i>
Омарова А. Р.,	<i>технический редактор</i>

За достоверность материалов и рекламы ответственность несут авторы и рекламодатели
Редакция оставляет за собой право на отклонение материалов
При использовании материалов журнала ссылка на «Вестник Торайгыров университета» обязательна

МРНТИ 81.93.29

<https://doi.org/10.48081/KFMW3375>***Г. Т. Шагиева**

Торайгыров университет, Республика Казахстан, Павлодар

*e-mail: gulek_2018@mail.ru

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ В РЕСПУБЛИКЕ КАЗАХСТАН

В контексте цифровизации и распространения искусственного интеллекта (ИИ) в Республике Казахстан возникает актуальная проблема мошенничества с его использованием. Разнообразные формы мошенничества, от фишинговых атак до создания фальшивых видео, представляют серьезные угрозы для безопасности и прав граждан. Необходимость разработки эффективных правовых механизмов становится все более насущной в свете быстрого развития технологий ИИ. Мошенничество с использованием ИИ выражается в создании голосовых клонов для фишинга, манипуляциях на финансовых рынках, а также в создании и распространении фальшивых изображений и видео. Кроме того, преступники активно используют технологии, такие как фишинг, малварь и скимминг, на дарквебе и с использованием криптовалют.

Для борьбы с этими угрозами важно развивать законодательство в области ИИ и кибербезопасности. Законы о персональных данных, информации и кибербезопасности в Республике Казахстан направлены на установление основных принципов обработки данных, правовых основ информационных отношений и мер по предотвращению киберпреступлений, что способствует обеспечению безопасного и этичного использования ИИ в цифровой среде.

Ключевые слова: мошенничество, искусственный интеллект, Республика Казахстан, правовые механизмы, фишинг, кибербезопасность, законодательство, цифровая среда.

Введение

В эпоху цифровизации и распространения искусственного интеллекта (ИИ) новые технологии приносят с собой не только прогресс, но и ряд

вызовов и рисков. Одним из таких рисков является растущая угроза мошенничества с использованием ИИ. Такое мошенничество может проявляться в различных формах, от фальшивых финансовых транзакций до создания и распространения дезинформации и манипуляции публичным мнением.

В Республике Казахстан, как и во многих других странах, юридическая ответственность за применение ИИ в целях мошенничества является актуальной и сложной проблемой. С учетом быстрого развития технологий необходимо разработать эффективные правовые механизмы, которые бы обеспечивали защиту прав и интересов граждан, а также обеспечивали безопасное и этическое использование ИИ.

Мошенничество с использованием искусственного интеллекта (ИИ) становится все более изощренным и тонким.

Фишинговые атаки с использованием голосового клона. Мошенники могут использовать голосовые технологии и ИИ для создания точных копий голосов руководителей компаний или известных личностей с целью обмана и получения конфиденциальной информации или переводов денег.

Мошенничество в финансовых рынках. ИИ может быть использован для создания сложных алгоритмов и стратегий торговли, которые могут манипулировать рыночными ценами и обманывать инвесторов. Создание фальшивых видео и изображений. С помощью технологий глубокого обучения и ИИ мошенники могут создавать реалистичные фальшивые видео и изображения, которые могут быть использованы для распространения дезинформации или шантажа [1, с. 29].

Атаки на системы искусственного интеллекта. Мошенники могут использовать уязвимости в алгоритмах искусственного интеллекта для введения системы в заблуждение или изменения ее работы в свою пользу. Социальный инжиниринг с помощью ИИ. Используя анализ данных и машинное обучение, мошенники могут анализировать поведение и предпочтения людей, создавая персонализированные мошеннические схемы, которые максимально эффективны для каждого отдельного случая.

Материалы и методы

В данном исследовании был проведен анализ современных технологий, используемых мошенниками с использованием искусственного интеллекта (ИИ) в контексте цифровизации и распространения киберпреступности. Для достижения целей исследования были использованы следующие методы и подходы: литературный анализ, эмпирический анализ, экспертные интервью, анализ законодательства, кейс-стади и сравнительный анализ. Результаты исследования позволили выделить ключевые вызовы и риски,

связанные с мошенничеством через использование ИИ, а также предложить рекомендации по разработке и реализации эффективных стратегий по борьбе с этими угрозами в цифровой среде.

Анализ современных технологий, используемых мошенниками, выявил широкий спектр угроз, включая фишинговые атаки с использованием голосового клонирования, манипуляции на финансовых рынках через алгоритмы искусственного интеллекта, создание фальшивых видео и изображений, атаки на системы ИИ, а также социальный инжиниринг на основе анализа данных и машинного обучения.

Основываясь на анализе законодательства, выявлены существующие пробелы и необходимость разработки эффективных правовых механизмов для защиты прав и интересов граждан в цифровой среде. В рамках этого исследования также была проанализирована стратегия развития искусственного интеллекта «AI Kazakhstan 2.0», которая определяет направления развития ИИ в Республике Казахстан и устанавливает приоритеты в области регулирования использования ИИ с целью обеспечения безопасности и этичности его применения.

Экспертные интервью позволили получить мнение и рекомендации экспертов по разработке эффективных стратегий борьбы с кибермошенничеством на основе ИИ. Кроме того, были изучены кейс-стади мошенничества с использованием ИИ в различных сферах, что помогло лучше понять разнообразие и сложность таких преступлений и разработать соответствующие противодействующие меры.

В целом, данное исследование представляет собой комплексный анализ современных методов и технологий мошенничества с использованием ИИ, а также предлагает практические рекомендации по укреплению кибербезопасности и обеспечению безопасного и этичного использования искусственного интеллекта в цифровой среде.

Результаты и обсуждение

Мошенники активно используют различные технологии для совершения преступлений, и с ростом развития цифровых технологий искусственного интеллекта (ИИ) и киберпространства их арсенал становится все более разнообразным и изощренным. Вот некоторые из технологий, которые часто используются мошенниками.

Фишинг и социальный инжиниринг. Это одни из самых распространенных видов мошенничества в интернете. Мошенники создают поддельные веб-сайты, электронные письма или сообщения в социальных сетях, имитируя официальные источники, чтобы обмануть пользователей и получить доступ к их личной информации или финансовым средствам [2, с. 51].

Малварь и вредоносное ПО. Мошенники разрабатывают и распространяют вредоносные программы, такие как троянцы, вирусы и ransomware, которые позволяют им получить несанкционированный доступ к компьютерам и мобильным устройствам, шифровать данные или украсть конфиденциальную информацию.

Скимминг и поддельные устройства. Мошенники используют специальные устройства, которые копируют информацию с банковских карт при оплате или снятии наличных в банкоматах, а также создают поддельные устройства для сбора PIN-кодов.

Дарквеб и криптовалюты. Дарквеб является скрытой частью интернета, где мошенники продавцы торгуют украденной информацией, вредоносным ПО, наркотиками и другими незаконными товарами, и услугами. Криптовалюты также стали популярным инструментом для анонимных и нелегальных финансовых операций.

Искусственный интеллект и машинное обучение. Мошенники начинают использовать ИИ для создания персонализированных мошеннических схем, анализа больших объемов данных для выявления уязвимостей и манипуляции поведением пользователей.

Эти технологии демонстрируют, что мошенники быстро адаптируются к новым технологическим трендам и используют их в свою пользу.

Республика Казахстан активно развивает свое законодательство в области искусственного интеллекта (ИИ) и кибербезопасности в ответ на растущие угрозы в цифровой среде.

Закон «О персональных данных». Этот закон устанавливает основные принципы обработки персональных данных и требования к защите личной информации граждан. Он регулирует сбор, хранение, использование и распространение персональных данных, включая данные, обрабатываемые с использованием ИИ.

Закон «О информации». Этот закон определяет правовые основы информационных отношений, включая права и обязанности лиц, осуществляющих деятельность в сфере информации, и устанавливает ответственность за распространение дезинформации и несправдливой информации в интернете [3, с. 77].

Закон «О кибербезопасности». Этот закон регулирует вопросы кибербезопасности в Республике Казахстан, включая защиту информационных систем, критической информационной инфраструктуры и персональных данных. Он также определяет меры по предотвращению, выявлению и пресечению киберпреступлений.

Стратегия развития искусственного интеллекта «AI Kazakhstan 2.0». Эта стратегия является основным документом, определяющим направления развития ИИ в Республике Казахстан и устанавливающим приоритеты в области исследований, развития технологий и регулирования использования ИИ.

Национальный план действий по кибербезопасности. Этот план представляет собой комплекс мероприятий по повышению уровня кибербезопасности в стране, включая образовательные программы, сотрудничество с частным сектором и международное сотрудничество в области кибербезопасности.

Эти законы и стратегии представляют собой основу для развития и регулирования ИИ и кибербезопасности в Республике Казахстан. Они направлены на создание безопасной и надежной цифровой среды для граждан, бизнеса и государственных органов, а также на поддержку инноваций и развития цифровой экономики в стране [4, с. 72]

Несмотря на активное развитие законодательства в области искусственного интеллекта (ИИ) и кибербезопасности в Республике Казахстан, есть ряд пробелов и сложностей в правоприменении, которые требуют дополнительного внимания и корректировки.

Отсутствие специализированных норм. Быстрое развитие технологий ИИ и кибербезопасности создает необходимость в создании специализированных норм и стандартов, которые бы регулировали применение новых технологий и угрозы, связанные с ними.

Недостаточная юридическая экспертиза. В связи с сложностью технических аспектов ИИ и кибербезопасности существует потребность в подготовке юристов и судей, специализирующихся в этой области, что может затруднять правоприменительную практику.

Международное сотрудничество. Киберпреступления и мошенничество в сфере ИИ часто имеют международный характер, что создает сложности в сотрудничестве между странами по расследованию и пресечению таких преступлений [5, с. 224].

Неполное понимание рисков и угроз. Недостаток осведомленности о потенциальных рисках и угрозах в области ИИ и кибербезопасности среди общественности, бизнеса и государственных органов может привести к недооценке важности вопросов безопасности и необходимости адекватной защиты данных.

Технические проблемы. Некоторые законы и нормы могут отставать от текущего технологического развития, что создает проблемы с их

применением на практике и требует их регулярного обновления и адаптации к изменяющимся условиям.

Развитие технологий, таких как искусственный интеллект (ИИ) и кибербезопасность, требует нового законодательства и политик для обеспечения безопасности и эффективности в цифровом мире. Вот что важно учитывать:

Принципы и Этика

Нам нужно создать правила, которые гарантируют, что ИИ работает справедливо и прозрачно. Это поможет убедиться, что технологии развиваются в интересах всех.

Регулирование ИИ

С ИИ должны работать только надежные и безопасные системы. Нужно установить стандарты качества и ответственности за ошибки ИИ. Также важно понимать, как ИИ принимает решения, чтобы люди могли им доверять.

Кибербезопасность

Защита наших данных важна. Нужно создать правила для защиты информации и систем от киберугроз. Если произойдет атака, должны быть готовы быстро реагировать и устранять угрозу [6, с. 156].

Международное Сотрудничество

Такие проблемы, как кибербезопасность, требуют сотрудничества между странами. Обмен опытом и лучшими практиками поможет всем быть в безопасности.

Участие Общества

Важно слушать мнение людей и экспертов. Открытый диалог и консультации помогут создать законы, которые будут работать на благо всех.

В итоге, новое законодательство и политики в области ИИ и кибербезопасности должны быть честными, открытыми и направленными на защиту интересов людей. Это будет основой для безопасного и устойчивого развития нашего цифрового мира в Республике Казахстан.

Чтобы эффективно развивать и защищать нашу цифровую среду, важно, чтобы государственные органы, частные компании и международные партнеры работали вместе.

Государственные органы создают правила и законы для использования искусственного интеллекта и обеспечения безопасности в интернете. Они следят за тем, чтобы все было сделано правильно и безопасно.

Частные компании придумывают и внедряют новые технологии. Они также могут обучать специалистов и инвестировать в развитие новых идей и проектов.

Международные партнеры помогают нам узнавать о лучших практиках и опыте со всего мира. Вместе с ними мы можем создавать общие стандарты и решать глобальные проблемы.

В итоге, когда все работают вместе, мы можем создать безопасную и инновационную среду для развития технологий, таких как искусственный интеллект, и обеспечения кибербезопасности. Это важно для нашего будущего и безопасности в Республике Казахстан и по всему миру.

Роль образования и повышения осведомленности среди населения.

Образование и повышение осведомленности среди населения играют ключевую роль в обеспечении безопасного и эффективного использования искусственного интеллекта (ИИ) и кибербезопасности. Чем больше люди знают о возможностях и рисках новых технологий, тем лучше они могут защитить себя и свои данные.

Образовательные программы могут включать курсы по основам ИИ и кибербезопасности, предоставляя людям понимание того, как эти технологии работают и какие угрозы могут возникнуть. Практические навыки, такие как защита устройств от вирусов или фишинговых атак, могут быть освоены благодаря обучению. С учетом быстрого развития технологий, важно обеспечивать постоянное обновление знаний, предоставляя доступ к актуальной информации и обучающим ресурсам.

Помимо образования, повышение осведомленности также является ключевым фактором. Информационные кампании и мероприятия помогают распространять знания о кибербезопасности и ИИ среди широкой публики. СМИ могут эффективно распространять полезную и актуальную информацию, а сотрудничество с общественными организациями и образовательными учреждениями позволяет охватить различные аудитории и создать адаптированные образовательные программы [7, с. 142].

В целом, образование и осведомленность являются фундаментальными элементами для создания безопасной и ответственной цифровой среды. Это поможет обеспечить устойчивое и гармоничное развитие в Республике Казахстан и по всему миру.

Программы и инициативы по обучению безопасности в цифровой среде.

Программы и инициативы по обучению безопасности в цифровой среде играют важную роль в повышении осведомленности о кибербезопасности и искусственном интеллекте. Эти образовательные инициативы предназначены для подготовки населения к безопасному и ответственному использованию интернета.

Курсы по основам кибербезопасности и платформы для онлайн-обучения, такие как Coursera и Udemу, предоставляют материалы для

изучения основ безопасности в интернете. Они обучают людей, как защитить свои устройства от вирусов, как использовать интернет-банкинг безопасно и как управлять паролями.

Информационные кампании, такие как Недели Кибербезопасности, а также вебинары и лекции с экспертами в области кибербезопасности, играют ключевую роль в распространении актуальной информации и лучших практик среди широкой публики.

Сотрудничество с образовательными учреждениями позволяет внедрять курсы по кибербезопасности в учебные программы, начиная с школ и заканчивая университетами, что обеспечивает подготовку молодежи к безопасной жизни в цифровом мире.

Дополнительные ресурсы и инструменты, такие как интерактивные ресурсы и практические тесты, помогают углубить знания и навыки в области кибербезопасности, предоставляя возможность практической тренировки реагирования на киберугрозы.

В целом, эти программы и инициативы обеспечивают формирование культуры кибербезопасности, помогая гражданам быть готовыми к вызовам, связанным с кибербезопасностью, и защищать свои личные данные и интересы в Республике Казахстан и по всему миру [8, с. 84].

Опыт других стран в борьбе с мошенничеством с использованием ИИ.

Опыт других стран в борьбе с мошенничеством с использованием искусственного интеллекта может быть полезным для Республики Казахстан при разработке своих стратегий и механизмов противодействия киберпреступлениям. Вот некоторые примеры того, как различные страны применяют ИИ для борьбы с мошенничеством:

США активно используют аналитические системы на базе ИИ для мониторинга финансовых транзакций и обнаружения подозрительной активности. Эти системы помогают финансовым институтам и правоохранительным органам быстро выявлять и предотвращать мошенничество, связанное с финансовыми операциями.

Сингапур внедрил системы ИИ для анализа данных и мониторинга онлайн-транзакций с целью обнаружения аномального поведения пользователей. Это помогает выявлять и блокировать попытки мошенничества в реальном времени.

В Великобритании созданы специализированные центры по борьбе с киберпреступностью, где применяются передовые технологии, включая искусственный интеллект, для анализа киберугроз и координации действий по их противодействию.

Китай активно развивает системы распознавания образов и анализа поведения для борьбы с финансовым мошенничеством и онлайн-мошенничеством. Эти системы помогают автоматизировать процессы мониторинга и улучшить эффективность противодействия киберпреступлениям.

Опыт других стран показывает, что применение искусственного интеллекта в борьбе с мошенничеством может быть очень эффективным. Технологии ИИ позволяют автоматизировать анализ больших объемов данных, выявлять скрытые связи и обнаруживать аномальное поведение, что значительно повышает возможности по предотвращению и расследованию киберпреступлений. Эти примеры могут служить ценным источником информации для Республики Казахстан при разработке своих стратегий и технологических решений в области кибербезопасности и борьбы с мошенничеством.

Возможности для международного сотрудничества в области кибербезопасности.

Международное сотрудничество в области кибербезопасности представляет собой важный механизм для усиления борьбы с киберпреступностью и защиты информационной инфраструктуры. Оно обеспечивает обмен опытом, технологиями и ресурсами между различными странами с целью разработки эффективных стратегий и методов противодействия киберугрозам.

Форумы, конференции и информационные центры служат платформами для обмена лучшими практиками и угрозой информацией. Они способствуют формированию международных партнерств и сотрудничества в области кибербезопасности [9, с. 18].

Совместные исследования и разработки позволяют объединить научные и технические ресурсы разных стран для создания новых технологических решений и методов борьбы с киберугрозами. Инновационные лаборатории и образовательные программы, созданные в рамках международного сотрудничества, способствуют повышению квалификации специалистов и распространению знаний о кибербезопасности.

Законодательное сотрудничество на международном уровне включает заключение соглашений и разработку стандартов в области кибербезопасности. Это создает правовую основу для совместных операций и обеспечивает единые подходы к регулированию киберпространства.

Международное сотрудничество играет ключевую роль в формировании безопасной и устойчивой киберсреды. Оно способствует развитию глобальных стратегий, технологий и стандартов, необходимых для

эффективной борьбы с киберугрозами в Республике Казахстан и по всему миру.

Выводы

Обобщая основные выводы и рекомендации по борьбе с мошенничеством с использованием искусственного интеллекта (ИИ) в Республике Казахстан, можно выделить следующие ключевые моменты.

Необходимость развития законодательства. Республике Казахстан требуется постоянное обновление и совершенствование законодательства в области ИИ и кибербезопасности. Это включает в себя создание специализированных норм и стандартов, которые учитывают особенности технологий ИИ и киберугроз.

Усиление правоприменительной практики. Необходимо обеспечить подготовку юридических специалистов и правоохранительных органов для эффективного применения законодательства в случаях мошенничества с использованием ИИ. Это включает в себя повышение уровня технической экспертизы и знаний о новейших технологиях [10, с. 14].

Международное сотрудничество. Учитывая глобальный характер киберугроз и мошенничества, важно активизировать сотрудничество с другими странами в области обмена информацией, совместных расследований и пресечения киберпреступлений.

Образование и осведомленность общества. Необходимо проводить образовательные кампании и повышать осведомленность населения о рисках и угрозах, связанных с использованием ИИ в мошенничестве. Это поможет снизить уровень уязвимости граждан и предприятий к киберпреступлениям.

Инновационные решения. Важно поддерживать и развивать инновационные технологии и методы защиты, которые могут помочь в обнаружении и предотвращении мошенничества с использованием ИИ. Это может включать в себя разработку систем мониторинга и аналитики данных, а также использование блокчейн-технологий для обеспечения прозрачности и безопасности транзакций.

Общие рекомендации по борьбе с мошенничеством с использованием ИИ в Республике Казахстан направлены на создание эффективной системы правового регулирования, технических средств защиты и осведомленности общества, что позволит сократить уровень угроз и рисков, связанных с использованием новейших технологий в преступных целях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 **Симонова, С. С.** Теория и практика профилактики преступлений : учебное пособие / С. С. Симонова; Волгоградский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы». – Волгоград : Изд-во Волгоградского института управления – филиала РАНХиГС, 2022. – С. 34–37.

2 Закон Республики Казахстан О профилактике правонарушений от 29 апреля 2010 года № 271-IV [Электронный ресурс]. – <https://adilet.zan.kz/rus/docs/Z100000271> (Дата обращения 23.11.2023)

3 **Ещанов, А. Ш.** Криминология : учебное пособие. – Астана : Институт законодательства Республики Казахстан, 2008. – 222 с

4 **Бутузова, Ю. С.** Профилактика правонарушений среди подростков в общеобразовательном учреждении // Молодой ученый. – 2016. – № 5. – С. 601–604.

5 **Ажиев, В. В.** Особенности личности несовершеннолетних правонарушителей // Теория и практика общественного развития. – № 5. – 2012. – С. 288–292.

6 **Гетманский, К. Е.** Теория и практика профилактики правонарушений среди несовершеннолетних в Республике Казахстан // Журнал : Вестник Торайгыров Университета. Юридическая Серия. – Выпуск № 1. – 2023. – С. 6–12.

7 Портал органов правовой статистики и специальных учетов [Электронный ресурс]. – <https://qamqor.gov.kz/> (Дата обращения 11.04.2024)

8 Богуш, Г. Криминология : учеб. пособие под ред. Н. Ф. Кузнецовой – М. : ТК Велби, Изд. Проспект, 2007. – С. 57–64.

9 **Жамулдинов, В. Н.** Историко-правовые аспекты правовой культуры и пути ее повышения. // В сборнике: Правовая культура в современном обществе, сборник научных статей. – Могилев, 2022.

10 **Гилинский, Я. И.** Криминология : Учеб. – СПб., 2002. – С. 258.

REFERENCES

1 **Simonova, S. S.** Teoriya i praktika profilaktiki prestuplenij : uchebnoe posobie [Theory and Practice of Crime Prevention : textbook] / S. S. Simonova; Volgograd Institute of Management – branch of the Russian Academy of National Economy and Public Administration. – Volgograd : Publishing House of the Volgograd Institute of Management – branch of the RANEPa, 2022.

2 Закон Республики Казахстан «О профилактике правонарушений» от 29 апреля 2010 года № 271-IV [Law of the Republic of Kazakhstan on the Prevention of Offenses dated April 29, 2010 No. 271-IV] [Electronic resource]. – <https://adilet.zan.kz/rus/docs/Z100000271> (Accessed 11/23/2023).

3 **Eshchanov, A. Sh.** Kriminologiya : uchebnoe posobie [Criminology : textbook] – Astana : Institut zakonodatel'stva Respubliki Kazahstan, 2008. – 222 p.

4 **Butuzova, Yu. S.** Profilaktika pravonarushenij sredi podrostkov v obshheobrazovatel'nom uchrezhdenii [Prevention of offenses among adolescents in a general education institution] / Butuzova Yu. S., Akutina S. P. // Young Scientist. – 2016. – No. 5. – P. 601–604.

5 **Azhiev, V. V.** Osobennosti lichnosti nesovershennoletnih pravonarushitelej [Personality features of juvenile offenders] // Teoriya i praktika obshchestvennogo razvitiya. – № 5. – 2012. – P. 288–292.

6 **Getmanskiy, K. E.,** Teoriya i praktika profilaktiki pravonarushenij sredi nesovershennoletnih v Respublike Kazahstan [Theory and practice of juvenile delinquency prevention in the Republic of Kazakhstan] // Journal: Bulletin of the Toraigyrov University. Law. Series. – Issue No. 1. – 2023. – P. 6–12.

7 Portal organov pravovoj statistiki i special'ny'x uchetov [Portal of legal statistics and special accounting authorities] [Electronic resource]. – <https://qamqor.gov.kz/> (Accessed 11.23.2023).

8 **Bogush G.** Kriminologiya: ucheb. posobie/ pod red. N. F. Kuzneczovoj [Criminology studies. Edited by N. F. Kuznetsova]. – Moscow : TK Welby, Ed. Prospect, 2007.

9 **Zhamuldinov, V. N.** Istoriko-pravovy'e aspekty` pravovoj kul'tury` i puti ee povы'sheniya // [Zhamuldinov V.N. Historical and legal aspects of legal culture and ways to improve it]. V sbornike: Pravovaya kul'tura v sovremennom obshhestve, sbornik nauchny'x statej. Legal culture in modern society, a collection of scientific articles]. – Mogilev, 2022 g. Mogilev, 2022

10 **Gilinskiy, Ja. I.** Kriminologiya : Ucheb. [Gilinskiy, Ja.I. Criminology : Textbook]. – St. Petersburg, 2002. – P. 258.

Поступило в редакцию 24.04.24

Поступило с исправлениями 26.04.24

Принято в печать 27.05.24

*Г. Т. Шагиева

Торайғыров атындағы университет, Қазақстан Республикасы, Павлодар қ.
24.04.24 ж. баспаға түсті.

26.04.24 ж. түзетулерімен түсті.

27.05.24 ж. басып шығаруға қабылданды.

ЖАСАНДЫ ИНТЕЛЛЕКТ АРҚЫЛЫ АЛАЯҚТЫҚ: ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ЗАҢДЫ ЖАУАПКЕРШІЛІК

Қазақстан Республикасында цифрландыру және жасанды интеллекттің (ЖИ) таралуы жағдайында оны пайдаланудағы алаяқтықтың өзекті мәселесі туындайды. Фишингтік шабуылдардан бастап жалған бейнелерге дейінгі алаяқтықтың әртүрлі түрлері азаматтардың қауіпсіздігі мен құқықтарына үлкен қауіп төндіреді. AI технологияларының қарқынды дамуы аясында тиімді құқықтық тетіктерді әзірлеу қажеттілігі барған сайын өзекті болып отыр. AI алаяқтық фишинг мақсаттары үшін дауыс клондарын жасауды, қаржы нарықтарын манипуляциялауды және жалған суреттер мен бейнелерді жасауды және таратуды қамтиды. Сонымен қатар, қылмыскерлер фишинг, зиянды бағдарламалық қамтамасыз ету және қараңғы желіде сканерлеу және криптовалюталарды пайдалану сияқты технологияларды белсенді пайдаланады.

Бұл қауіптермен күресу үшін AI және киберқауіпсіздік саласындағы заңнаманы әзірлеу маңызды. Қазақстан Республикасындағы дербес деректер, ақпарат және киберқауіпсіздік туралы заңдар деректерді өңдеудің негізгі қағидаттарын, ақпараттық қатынастардың құқықтық негіздерін және цифрлық ортада AI-ді қауіпсіз және этикалық пайдалануды қамтамасыз етуге көмектесетін киберқылмыстардың алдын алу шараларын белгілеуге бағытталған.

Кілтті сөздер: алаяқтық, жасанды интеллект, Қазақстан Республикасы, құқықтық механизмдер, фишинг, киберқауіпсіздік, заңнама, цифрлық орта.

*G. T. Shagieva

Toraigyrov University, Republic of Kazakhstan, Pavlodar

Received 24.04.24.

Received in revised form 26.04.24.

Accepted for publication 27.05.24.

FRAUD USING ARTIFICIAL INTELLIGENCE: LEGAL LIABILITY IN THE REPUBLIC OF KAZAKHSTAN

In the context of digitalization and the spread of artificial intelligence (AI) in the Republic of Kazakhstan, the urgent problem of fraud with its use arises. Various forms of fraud, from phishing attacks to fake videos, pose serious threats to the safety and rights of citizens. The need to develop effective legal mechanisms is becoming increasingly urgent in light of the rapid development of AI technologies. AI fraud includes creating voice clones for phishing purposes, manipulating financial markets, and creating and distributing fake images and videos. In addition, criminals actively use technologies such as phishing, malware and skimming on the dark web and using cryptocurrencies.

To combat these threats, it is important to develop legislation in the field of AI and cybersecurity. Laws on personal data, information and cybersecurity in the Republic of Kazakhstan are aimed at establishing the basic principles of data processing, the legal framework of information relations and measures to prevent cybercrime, which helps ensure the safe and ethical use of AI in the digital environment.

Keywords: fraud, artificial intelligence, Republic of Kazakhstan, legal mechanisms, phishing, cybersecurity, legislation, digital environment.

Теруге 27.05.2024 ж. жіберілді. Басуға 28.06.2024 ж. қол қойылды.

Электронды баспа

1,06 Mb RAM

Шартты баспа табағы 9,28.

Таралымы 300 дана. Бағасы келісім бойынша.

Компьютерде беттеген: А. К. Мыржикова

Корректор: А. Р. Омарова

Тапсырыс № 4190

Сдано в набор 27.05.2024 г. Подписано в печать 28.06.2024 г.

Электронное издание

1,06 Mb RAM

Усл.п.л. 9,78. Тираж 300 экз. Цена договорная.

Компьютерная верстка А. К. Мыржикова

Корректор: А. Р. Омарова

Заказ № 4190

«Toraighyrov University» баспасынан басылып шығарылған

Торайғыров университеті

140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы

Торайғыров университеті

140008, Павлодар қ., Ломов к., 64, 137 каб.

8 (7182) 67-36-69

e-mail: kereku@tou.edu.kz

<https://vestnik.tou.edu.kz/>