DOI: 10.51634/2307-5201_2026_1_71
УДК 343.102:351.745.7; 34.03:[002:004]

ЭВОЛЮЦИЯ И ТРАНСФОРМАЦИЯ МОШЕННИЧЕСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

А.Ш. ЕЩАНОВ, д.ю.н., профессор кафедры общеюридических дисциплин Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан (Республика Казахстан, г. Косшы), e-mail: 7340207@prokuror.gov.kz

М.Б. САДЫКОВ, доктор философии (PhD), старший преподаватель кафедры специальных юридических дисциплин Академии правоохранительных органов при Генеральной прокуратуре Республика Казахстан (Республика Казахстан, г. Косшы), e-mail: mukhtar.sadykov@gmail.com

В статье исследуется эволюция мошенничества в условиях цифровизации как социально-правового феномена, отражающего трансформацию доверия в цифровой среде. Цель работы заключается в анализе философско-правовых закономерностей и институциональных механизмов противодействия цифровому мошенничеству в Республике Казахстан. Методологическая база объединяет философско-правовой, социотехнический и сравнительно-правовой подходы.

Эмпирическая база сформирована на основе статистических и нормативных материалов, характеризующих развитие цифровой инфраструктуры и практик противодействия киберпреступности. Авторы показывают, что обман становится элементом архитектуры коммуникации, а не только действием субъекта. Республика Казахстан формирует экосистему цифрового доверия, включающую профилактику, антифрод-инфраструктуру и развитие цифровой грамотности. Делается вывод о необходимости перехода к концепции цифрового правового гуманизма, где технологическая эффективность сочетается с сохранением человеческого достоинства.

Ключевые слова: цифровое мошенничество, доверие, искусственный интеллект, профилактика, кибербезопасность, цифровой гуманизм, философия права, антифрод-инфраструктура, цифровая грамотность.

Введение

Цифровая трансформация сегодня уже не сводится к ускорению обмена информацией и удобству сервисов. Она перестраивает само устройство социального доверия и тем самым затрагивает основания юридической ответственности, способы правового контроля и практики доказывания. В цифровой среде доверие все чаще формируется через интерфейсы, платформы, процедуры дистанционной идентификации и алгоритмические решения. Пользователь доверяет не конкретному собеседнику, а технической оболочке взаимодействия и ее обещанию подлинности.

Эта перестройка прямо влияет на характер мошенничества. Если классические модели обмана опирались на личный контакт и относительно прозрачную причинно-следственную связь между намерением и действием, то цифровое мошенничество чаще приобретает многоуровневую структуру. Оно выглядит не как единичный эпизод, а как воспроизводимая стратегия воздействия на восприятие и выбор человека, где убедительность создается не только речью и психологией, но и инфраструктурными эффектами достоверности. В результате размывается граница между субъектом, инструментом и средой совершения деяния, а привычные для права категории вины, контроля над способом совершения, причинения вреда требуют более точной интерпретации в условиях распределенности действий и сетевой анонимности.

Актуальность темы подтверждается и эмпирически. Данные Комитета по правовой статистике и специальным учётам Генеральной прокуратуры Республики Казахстан о распространенности интернет-мошенничества в Казахстане и связанном с ним материальном ущербе указывают не просто на рост эпизодов, но на качественный сдвиг в способах эксплуатации доверия [1; 2]. Поэтому исследование целесообразно выводить за рамки узко уголовно-правового описания и дополнять философско-правовым анализом, позволяющим раскрыть доверие как нормативную и ценностную категорию, уязвимую в цифровой среде.

Если для классического мошенничества типичным был прямой обман конкретного лица в ситуации личного контакта, то в цифровой среде уязвимость чаще возникает иначе. Обман опирается на доверие не к человеку, а к техническому контуру взаимодействия, к интерфейсу приложения, к привычному дизайну сервиса, к статусу аккаунта, к «официальному» каналу связи. В рамках настоящего исследования мы исходим из того, что здесь меняется не только способ коммуникации, но и сама логика формирования доверия. Достоверность как будто подтверждается инфраструктурой, и именно поэтому манипуляция все чаще становится функцией среды, через которую человек принимает решения.

Эту особенность можно интерпретировать шире как проявление напряжения внутри модерного проекта, когда рационализированные системы, призванные снижать неопределенность, порождают новые формы риска и новые зоны уязвимости. В таком прочтении цифровое мошенничество выступает симптомом кризисной динамики модерна, о которой писали Ю. Хабермас и У. Бек, но проявляется она на прикладном уровне через конкретные механизмы симуляции доверия и через институциональные ограничения реагирования. Поэтому в статье мы рассматриваем цифровое мошенничество не только как совокупность эпизодов, а как социотехническую схему, где технические признаки легитимности используются для переноса доверия и для сокращения критической проверки со стороны потерпевшего [3], [4].

Это поднимает более общий вопрос о пределах юридической ответственности в цифровой среде. В цифровой среде действие нередко оказывается распределенным. Коммуникация, убеждение, перевод в нужный канал и получение выгоды могут быть разнесены по разным участникам и техническим слоям. След при этом фиксируется не в одном месте, а фрагментами, у платформы, у оператора связи, у банка, на устройстве потерпевшего. Именно поэтому в работе я ставлю вопрос не о том, заменяет ли машина человека, а о том, как меняются условия, в которых право связывает намерение, действие и причинение вреда.

Для описания этой трансформации мы используем несколько теоретических оптик. У Хабермаса важно то, что доверие и легитимность держатся на правилах коммуникации и признании процедур [3]. У Бека принципиальна логика риска, когда рационализированные системы создают новые уязвимости и требуют иных режимов ответственности [4]. Концепция сетевого общества Кастельса помогает увидеть, как власть и воздействие распределяются по сетям и узлам, а не по единичным субъектам [5]. У Флориди значимо представление об информации как среде существования, в которой нормативные границы проходят иначе, чем в офлайн контуре [6]. В совокупности эти подходы позволяют рассматривать право, как открытую систему, которая способна адаптироваться, но только при условии более точной настройки категорий обмана, доверия и информации под цифровую реальность.

Цель настоящего исследования состоит в выявлении философско-правовых закономерностей эволюции мошенничества в эпоху цифровизации и в анализе организационно правовых практик противодействия этому явлению в Республике Казахстан, которая находится на этапе формирования правового режима цифрового доверия.

Материалы и методы

Методологическая основа исследования объединяет философско-правовой, социологический и сравнительно-правовой подходы. Такой междисциплинарный ракурс позволяет рассматривать цифровое мошенничество не только как уголовно правовую категорию, но и как социотехнический феномен, который меняет способы взаимодействия человека, права и технологии. Теоретическая рамка работы опирается на идеи рефлексивной модернизации У. Бека [4], концепцию сетевого

общества М. Кастельса [5], философию коммуникативного действия Ю. Хабермаса [3] и информационную онтологию Л. Флориди [6]. В совокупности эти подходы помогают трактовать цифровизацию как процесс, в котором доверие, ответственность и правовое регулирование становятся гибридными и зависят от инфраструктурных условий цифровой среды. В этой логике право рассматривается как система, способная к адаптации, а не как неизменный набор предписаний, поскольку цифровое пространство задает собственные режимы скорости, анонимности и распределенности действий.

Эмпирическая база сформирована на основе статистических и нормативных материалов, отражающих развитие цифровой инфраструктуры и практик противодействия киберпреступности. Использованные источники позволяют описать и сопоставить институциональные меры предупреждения и пресечения цифрового мошенничества. В работе применяются системный, аксиологический и герменевтический анализ. Это дает возможность выявить связь между распространением цифровых технологий и изменением правовых инструментов реагирования, включая профилактические механизмы и режимы ответственности. Выбранная методология обеспечивает целостное рассмотрение цифрового мошенничества как процесса, который затрагивает не только уголовно правовую квалификацию, но и основания современной правовой культуры и ее представления о доверии и ответственности.

Результаты

Онтология цифрового мошенничества: от обмана к алгоритмической симуляции

Цифровое мошенничество в настоящем исследовании рассматривается не как перенос классического хищения в онлайн среду, а как форма обмана, где манипуляция осуществляется через саму инфраструктуру коммуникации и передачи ценности. Это проявляется в устойчивых практиках, включая фишинговые рассылки и копии сайтов, подмену QR кодов, фиктивные онлайн займы, использование поддельных видеозаписей и клонов голоса [7]. Общий механизм сводится к переносу доверия с личности на технические признаки легитимности, канал связи и дизайн сервиса, вследствие чего видимость подлинности может быть воспроизведена злоумышленником как стандартный сценарий взаимодействия [8]. Инструменты искусственного интеллекта усиливают этот эффект правдоподобия и масштабируемость воздействия, поскольку позволяют имитировать голос, визуальные образы и поведенческие паттерны [9].

Под симуляцией доверия в работе понимается воспроизведение внешних сигналов надежности и официальности, которые обычно поддерживаются средствами аутентификации, интерфейсными решениями и процедурами подтверждения, но в мошеннических схемах используются как средство убеждения [8]. Под распределенностью действия понимается конфигурация, при которой воздействие на потерпевшего разнесено по нескольким каналам и участникам, а результат достигается цепочкой взаимосвязанных шагов в сетевой среде [5]. Под нестабильностью цифрового следа понимается фрагментарность доказательственных признаков, которые распределяются между банками, операторами связи и платформами, из за чего реконструкция события зависит от доступности и согласуемости данных [5].

Эта постановка выводит к уточнению правовых категорий вины, контроля над способом совершения деяния и причинной связи, а также к вопросу о должной осмотрительности субъектов цифрового взаимодействия. Теоретически она соотносится с пониманием легитимности процедур коммуникации у Ю. Хабермаса [3], с логикой общества риска У. Бека [4] и с трактовкой цифровой среды как инфосферы у Л. Флориди [6]. Дополнительное объяснение дает концепт симулякра у Ж. Бодрийяра, описывающий подмену подлинности знаками достоверности [10], а также подход Э. Гоффмана к социальному взаимодействию как к роли и фасаду, что позволяет точнее описывать практики имитации доверия в цифровых контактах [11].

Формирование экосистемы цифрового доверия в противодействии мошенничеству в международно-правовом контексте

Для сравнительного анализа международных моделей цифрового доверия в контексте противодействия мошенничеству в настоящем разделе используются три критерия. Первый критерий

распределение ответственности за доверие и безопасность цифрового взаимодействия между государством, платформами и пользователями. Второй критерий режим идентификации и верификации, который определяет, насколько легко симулировать легитимность и вводить потерпевшего в заблуждение через технические признаки достоверности. Третий критерий организационная инфраструктура профилактики, включая межсекторальный обмен данными и скорость реагирования на антифрод сигналы.

По первому критерию европейская модель опирается на юридически закрепленную подотчетность платформ и прозрачность цифрового взаимодействия. Регламент о цифровых услугах 2022 года и Регламент об искусственном интеллекте 2024 года формируют нормативный режим, в котором доверие поддерживается через обязанность платформ управлять рисками, раскрывать информацию и обеспечивать контролируемость алгоритмических решений [12;13]. В странах Восточной Азии ответственность за доверие чаще проектируется институционально и реализуется через стандарты и управленческие рамки. Сингапурский подход Trust by Design переносит акцент на архитектуру сервисов, где надежность и идентификация задаются на этапе проектирования [14]. В Южной Корее Cyber Trust Framework закрепляет совместное участие государства и частного сектора в поддержании доверия к цифровым услугам [15]. В Китайской Народной Республике доверие обеспечивается преимущественно через государственный контроль и сертификацию платформ, а также через централизованные решения в сфере цифровой идентичности [16]. В обобщенном виде Организация экономического сотрудничества и развития рассматривает доверие как общественный капитал и базовую ценность цифрового общества, требующую институциональной поддержки и согласованных принципов политики [17].

По второму критерию различия проявляются в том, каким образом подтверждается легитимность участника и канала взаимодействия. Европейский подход нацелен на ограничение рисков через правила ответственности и процедурные требования, которые стимулируют платформы устранять источники системной уязвимости и обеспечивать прослеживаемость решений [12;13]. Восточноазиатские модели чаще усиливают доверие через стандартизацию идентификационных процедур и через внедрение принципа надежности в технологический дизайн [14;15]. Китайский подход дополнительно демонстрирует стремление к унифицированным государственным контурам идентичности, что повышает управляемость доверия, но одновременно усиливает зависимость доверия от централизованного контроля [16]. В логике ОЭСР идентификация и доверие должны поддерживаться так, чтобы цифровая среда сохраняла предсказуемость для общества и для экономики, не подрывая базовые права субъектов [17].

По третьему критерию ключевым становится наличие инфраструктуры раннего предупреждения и устойчивых каналов обмена данными. Европейская модель ориентируется на системное снижение рисков и повышение прозрачности поведения цифровых посредников, что создает условия для профилактики, но требует развитого комплаенса и правоприменительных процедур [12;13]. Восточноазиатские модели, особенно в Сингапуре и Южной Корее, усиливают профилактику через проектирование надежности и через совместимые организационные рамки взаимодействия государства и рынка [14;15]. Китайская модель в большей степени опирается на вертикально организованный контроль и сертификацию, что упрощает централизацию антифрод мер, но ставит вопрос о балансе между эффективностью и гарантиями правовой защиты [16].

Казахстанский подход формируется на пересечении указанных направлений и демонстрирует движение к профилактической логике. Создание Антифрод центра при Национальном банке и развитие киберполиции CyberPol отражают ориентацию на раннее выявление угроз и предотвращение ущерба в цифровой среде [18]. Для Казахстана прикладную ценность имеют два элемента международного опыта. Первый элемент институциональная координация и быстрый межсекторальный обмен данными по антифрод сигналам. Второй элемент стандарты дистанционной идентификации и единые требования к подтверждению легитимности канала взаимодействия. Риск состоит в том, что усиление контроля и расширение обмена данными при недостаточно четких процедурах и гарантиях может снижать доверие к цифровым сервисам и формировать конфликт между задачами безопасности и защитой прав субъектов. В этом смысле формирование экосистемы цифрового доверия требует не только расширения полномочий и технических инструментов, но и

выстраивания прозрачных режимов ответственности и подотчетности, которые делают профилактику устойчивой и социально приемлемой.

Обсуждение

Проведенный анализ показывает, что противодействие цифровому мошенничеству в Казахстане постепенно смещается от преимущественно реактивного реагирования к профилактической модели, где ключевым ресурсом становится управление цифровым доверием. В практическом плане это означает, что государственные меры ориентируются не только на наказание за уже совершенный эпизод, но и на снижение вероятности успешной манипуляции на уровне каналов связи, процедур идентификации и пользовательского поведения. Такой поворот требует согласованной связки правовых норм, организационных процедур и технологических инструментов, поскольку мошеннические схемы используют именно разрывы между этими уровнями.

На нормативном уровне важным направлением остается уточнение ответственности за распространение ложной и манипулятивной информации в сети, включая фишинговые предложения и рекламные материалы, которые создают видимость легитимности. В обсуждаемой проблематике это не частная деталь, а элемент правовой определенности цифровых отношений. Пока ответственность посредников и владельцев площадок очерчена нечетко, мошеннические коммуникации сохраняют высокую масштабируемость, а профилактика оказывается заведомо слабее, чем требуется по уровню риска.

Профилактическое направление усиливается за счет политики правовой грамотности и публичных коммуникаций. Концептуальные документы на 2025–2030 гг. закрепляют превенцию и повышение правовой культуры как приоритет, и это соответствует природе цифрового мошенничества, где исход часто решается в первые минуты контакта и зависит от того, распознает ли человек подделку [19]. В отличие от традиционного криминального эпизода, здесь значительная часть ущерба предотвращается не следственными действиями, а снижением уязвимости потерпевшего, прежде всего через понимание типовых признаков фишинга, поддельных сайтов, подмены каналов связи и психологического давления. В этой логике цифровая грамотность выступает не вспомогательной мерой, а элементом инфраструктуры доверия.

Отдельного внимания заслуживает профилактика, ориентированная на поведение потенциальной жертвы. Закон «О профилактике правонарушений» от 30 декабря 2025 г. закрепляет направления государственной политики в сфере профилактики и ориентирует систему на защиту прав и законных интересов граждан [20]. При этом виктимологическая профилактика, даже будучи предусмотренной в законе, остается слабо встроенной в практику правоохранительных органов, что создает разрыв между нормативным потенциалом и реальными инструментами снижения ущерба. Для цифрового мошенничества это особенно чувствительно, поскольку мошенники целенаправленно работают с уязвимостями восприятия и с автоматизмами доверия. Следовательно, приоритетность виктимологической профилактики оправдана не общими рассуждениями, а механизмом причинения вреда, который во многих случаях запускается через типовые поведенческие ошибки и через неверную оценку легитимности цифрового канала.

Новой зоной риска выступают манипулятивные медийные технологии, прежде всего deepfake. Платформы и социальные сети становятся средой распространения роликов, где используются визуальные и голосовые образы публичных лиц для вовлечения граждан в сомнительные инвестиционные и торговые схемы. Здесь вред наносится не только через прямое хищение, но и через разрушение доверия к официальным источникам и через формирование эффекта псевдолегитимности, когда ложная информация оформляется в узнаваемой визуальной оболочке. Для правоприменения это означает необходимость расширять профилактику на уровень платформенной среды и медиаграмотности, а также развивать механизмы оперативной фиксации цифровых следов, пока они не исчезли из публичного доступа.

Значимым элементом казахстанской модели становится институциональная инфраструктура, нацеленная на раннее выявление мошеннических схем и на межсекторальную координацию. Развитие антифрод механизмов при участии Национального банка, банковского сектора и профильных подразделений, включая киберполицию, создает основу для выявления подозрительных

транзакций и паттернов до момента необратимого ущерба [18]. Однако эффективность такой инфраструктуры зависит от процедур обмена данными, скорости реагирования и четкого распределения ответственности между участниками. Без единых протоколов и прозрачных регламентов обмена данными профилактика рискует превратиться в набор разрозненных инициатив, которые не дают кумулятивного эффекта.

Международное сотрудничество также приобретает прикладное значение, поскольку значительная часть цифровых схем имеет трансграничный компонент. В то же время внутри страны критичным остается повышение согласованности межведомственных действий и понятных каналов обратной связи для граждан. В цифровых преступлениях задержка по времени часто означает утрату доказательственных данных, поэтому организационная синхронизация становится фактором не меньшей важности, чем формальное ужесточение ответственности.

С учетом указанных результатов обсуждение выводит к уточнению нескольких правовых категорий. Во-первых, границ вины и контроля над способом совершения деяния в ситуации, когда действие распределено между разными каналами и посредниками. Во-вторых, причинной связи между манипулятивной коммуникацией и ущербом, особенно когда ключевую роль играют признаки технической легитимности и доверие к инфраструктуре. В-третьих, критериев должной осмотрительности и распределения ответственности между пользователем, платформой, финансовой организацией и оператором связи. В этих точках требуется не расширение абстрактных формул, а более точная настройка правового режима цифрового доверия.

Ограничения исследования связаны с тем, что анализ опирается на открытые нормативные и статистические материалы и не включает изучение конкретных уголовных дел с ограниченным доступом. Это означает, что выводы ориентированы на типовые механизмы симуляции доверия и на институциональные практики профилактики, а не на реконструкцию отдельных эпизодов.

Заключение

Рассмотрение феномена цифрового мошенничества через призму философско-правового анализа показывает, что его сущность выходит за пределы классического понимания преступления как акта индивидуального обмана. Оно становится системным свойством цифровой среды, в которой доверие не только используется, но и заново конструируется, а обман встраивается в саму архитектуру коммуникации. В этих условиях правовое регулирование уже не может ограничиваться функцией наказания. Оно должно опережать преступное действие, создавая пространство предсказуемости и прозрачности, где доверие становится не следствием, а предпосылкой правопорядка.

Казахстанский опыт демонстрирует постепенный переход от реактивной к превентивной модели противодействия мошенничеству. Создание Антифрод-центра, развитие межбанковских систем мониторинга и внедрение Концепции по продвижению идеологии законности и правопорядка на 2025–2030 гг. отражают стремление государства формировать цифровое доверие как основу устойчивого правопорядка. Эти процессы требуют постоянного взаимодействия между юристами, техническими специалистами и обществом, поскольку защита цифрового пространства невозможна без развития культуры правового и этического поведения в сети. В этом контексте информационная грамотность граждан становится не только инструментом безопасности, но и новой формой гражданской добродетели.

В философско-правовом плане цифровое мошенничество выявляет границы антропоцентрического права. Возникает необходимость переосмысления категорий вины, ответственности и доверия в условиях, когда субъектом взаимодействия становится не только человек, но и алгоритм. Именно здесь проявляется значение концепции цифрового правового гуманизма, ориентированной на сохранение человеческого достоинства в технологически опосредованной среде. Право должно не просто регулировать цифровое поведение, но и сохранять возможность морального выбора, что делает его не средством контроля, а гарантом человеческого присутствия в мире машинной рациональности.

Таким образом, формирующийся правовой режим цифрового доверия в Казахстане представляет собой пример перехода к новому типу правового мышления, основанному на прагматическом гуманизме. Эта модель соединяет нормативную строгость и этическую гибкость, технологическую эффективность

и человеческое измерение закона. Она выражает не только готовность государства к инновационному регулированию, но и стремление сохранить духовные основания права в эпоху цифровизации.

А.Ш. Ещанов, з.ғ.д., профессор, Қазақстан Республикасының Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының жалпы заң пәндері кафедрасының профессоры (Қазақстан Республикасы, Қосшы қ.); М.Б. Садықов, философия докторы (PhD), Қазақстан Республикасының Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының арнайы заң пәндері кафедрасының аға оқытушысы (Қазақстан Республикасы, Қосшы қ.): Цифрландыру жағдайында алаяқтықтың эволюциясы мен трансформациясы: Қазақстан Республикасындағы қарсы іс-қимылдың құқықтық және ұйымдастырушылық аспектілері.

Мақалада цифрландыру жағдайындағы алаяқтықтың әлеуметтік-құқықтық құбылыс ретіндегі эволюциясы қарастырылады. Зерттеудің мақсаты Қазақстан Республикасындағы цифрлық алаяқтыққа қарсы іс-қимылдың философиялық-құқықтық заңдылықтары мен институционалдық тетіктерін талдау болып табылады. Әдіснамалық негіз ретінде философиялық-құқықтық, әлеуметтік-техникалық және салыстырмалы-құқықтық тәсілдер қолданылды. Эмпирикалық база цифрлық инфрақұрылымның даму динамикасын және киберқылмыспен күрес тәжірибесін сипаттайтын статистикалық және нормативтік материалдарға сүйенеді. Авторлар алаяқтықты тек субъектінің іс-әрекеті деп емес, коммуникация архитектурасының құрамдас бөлігі ретінде қарастырады. Қазақстанда алдын алу шараларын жетілдіру, антифрод инфрақұрылымын қалыптастыру және цифрлық сауаттылықты арттыру арқылы цифрлық сенім экожүйесі құрылып келеді. Зерттеу нәтижелері технологиялық тиімділік пен адам қадір-қасиетін сақтау арасындағы тепе-теңдікті қамтамасыз ететін цифрлық құқықтық гуманизм тұжырымдамасына көшу қажеттігін айқындайды.

Түйінді сөздер: цифрлық алаяқтық, сенім, жасанды интеллект, алдын алу, киберқауіпсіздік, цифрлық гуманизм, құқық философиясы, антифрод инфрақұрылымы, цифрлық сауаттылық.

A.Sh. Yechshanov, Doctor of Law, Professor, Professor at the Department of General Legal Disciplines, Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan (Kosshy, Republic of Kazakhstan); M.B. Sadykov, PhD in Law, Master of Public Administration (Nazarbayev University), Senior Lecturer at the Department of Special Legal Disciplines, Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan (Kosshy, Republic of Kazakhstan): Evolution and Transformation of Fraud in the Context of Digitalization: Legal and Organizational Aspects of Counteraction in the Republic of Kazakhstan.

The article examines the evolution of fraud under digitalization as a socio-legal phenomenon reflecting the transformation of trust within the digital environment. The purpose of the study is to analyze the philosophical and legal patterns and institutional mechanisms of countering digital fraud in the Republic of Kazakhstan. The methodological framework integrates philosophical-legal, socio-technical, and comparative-legal approaches. The empirical base relies on statistical and regulatory materials describing the development of digital infrastructure and practices of combating cybercrime. The authors argue that deception becomes an element of the architecture of communication rather than merely a human act. Kazakhstan is forming an ecosystem of digital trust that includes preventive measures, antifraud infrastructure, and the promotion of digital literacy. The study concludes on the need to move toward a concept of digital legal humanism ensuring a balance between technological efficiency and the preservation of human dignity.

Keywords: digital fraud, trust, artificial intelligence, prevention, cybersecurity, digital humanism, philosophy of law, antifraud infrastructure, digital literacy.

Список литературы:

1. Комитет по правовой статистике и специальным учётам Генеральной прокуратуры Республики Казахстан. Статистика преступлений за первый квартал 2025 года. URL: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fqamqor.gov.kz%2Fcrimestat%2F%2Ffiles%2F2025%2F3%2F19%2F202503_1m_00000___ru.xlsx // (10.09.2025).

2. Ущерб от мошенников достиг рекорда: как казахстанцы теряют миллиарды. URL: https://bank.kz/news/finansy-news/ushherb-ot-moshennikov-dostig-rekorda-kak-kazahstanczy-teryayut-milliardy/?ysclid=mgj4729a93572119698 //(08.10.2025).

3. Habermas, J. The Theory of Communicative Action. Volume 1: Reason and the Rationalization of Society. Boston: Beacon Press, 1984.

4. Beck, U. Risk Society: Towards a New Modernity. London: Sage Publications, 1992.

5. Castells, M. The Rise of the Network Society. Cambridge, Mass.: Blackwell Publishers, 1996.

6. Floridi, L. The Philosophy of Information. Oxford: Oxford University Press, 2011.

7. Digital Element. 3 Common Types of Digital Fraud. Atlanta, GA: Digital Element, 2024. URL:: https://www.digitalelement.com/blog/digital-fraud/ (07.10.2025).

8. Challenges in Voice Biometrics: Vulnerabilities in the Age of Deepfakes. ABA Banking Journal, February 2024. URL: https://bankingjournal.aba.com/2024/02/challenges-in-voice-biometrics-vulnerabilities-in-the-age-of-deepfakes/ (15.09.2025).

9. Kelly S., Kaye S.-A., Oviedo-Trespalacios O. What Factors Contribute to the Acceptance of Artificial Intelligence? A Systematic Review. Technology in Society, 2023, Vol. 75, Article 102287.

10. Бодрийяр Ж. Симулякры и симуляция. Рипол Классик, 2013.

11. Goffman E. The Presentation of Self in Everyday Life. Garden City, N.Y.: Doubleday, 1959.

12. Digital Services Act. EUR-Lex. URL: https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html // (01.10.2025).

13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 June 2024 on digital services (Digital Services Act). Official Journal of the European Union. L XXX. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj // (15.10.2025).

14. Online Trust and Safety Research Programme and Centre for Advanced Technologies in Online Safety (CATOS). Ministry of Digital Development and Information (Singapore), 10 January 2024. URL: https://www.mddi.gov.sg/newsroom/online-trust-and-safety-catos // (11.09.2025).

15. National Cybersecurity Strategy, South Korea. International Telecommunication Union (ITU), 2023. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf // (15.09.2025).

16. Сахаров А. Г., Шелепов А. В. Политика Китайской народной республики в сфере регулирования цифровых платформ // Вестник международных организаций: образование, наука, новая экономика. 2024. Т. 19. №. 2. – С. 8.

17. Building Trust and Reinforcing Democracy. OECD Public Governance Reviews. URL: https://www.oecd.org/en/publications/building-trust-and-reinforcing-democracy_76972a4a-en.html // (08.10.2025).

18. Ещанов Алмаз Шукирович. Профилактика мошенничества с использованием информационных систем. Человек и Закон, 20 июня 2025. URL: https://astanazan.kz/?p=7067 // (15.08.2025).

19. Об утверждении Концепции по продвижению в обществе идеологии закона и порядка на 2025–2030 годы. Постановление Правительства Республики Казахстан от 1 апреля 2025 года № 200. URL: https://adilet.zan.kz/rus/docs/P2500000200 // (02.08.2025).

20. О профилактике правонарушений. Закон Республики Казахстан от 30 декабря 2025 года № 245-VIII ЗРК URL: https://adilet.zan.kz/rus/docs/Z2500000245 // (09.01.2025).

References:

1. Komitet po pravovoi statistike i spetsialnym uchetam Generalnoi prokuratury Respubliki Kazakhstan. Statistika prestuplenii za pervyi kvartal 2025 goda. URL: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fqamqor.gov.kz%2Fcrimestat%2F%2Ffiles%2F2025%2F3%2F19%2F202503_1m_00000___ru.xlsx (10.09.2025).

2. Ushcherb ot moshennikov dostig rekorda: kak kazakhstantsy teryayut milliardy. URL: https://bank.kz/news/finansy-news/ushherb-ot-moshennikov-dostig-rekorda-kak-kazahstanczy-teryayut-milliardy/?ysclid=mgj4729a93572119698 (08.10.2025).

3. Habermas J. The Theory of Communicative Action. Vol. 1: Reason and the Rationalization of Society. Boston: Beacon Press, 1984.

4. Beck U. Risk Society: Towards a New Modernity. London: Sage Publications, 1992.

5. Castells M. The Rise of the Network Society. Cambridge, Mass.: Blackwell Publishers, 1996.

6. Floridi L. The Philosophy of Information. Oxford: Oxford University Press, 2011.

7. Digital Element. 3 Common Types of Digital Fraud. Atlanta, GA: Digital Element, 2024. URL: https://www.digitalelement.com/blog/digital-fraud/ (07.10.2025).

8. Challenges in Voice Biometrics: Vulnerabilities in the Age of Deepfakes. ABA Banking Journal, February 2024. URL: https://bankingjournal.aba.com/2024/02/challenges-in-voice-biometrics-vulnerabilities-in-the-age-of-deepfakes/ (15.09.2025).

9. Kelly S., Kaye S.-A., Oviedo-Trespalacios O. What Factors Contribute to the Acceptance of Artificial Intelligence? A Systematic Review. Technology in Society, 2023, Vol. 75, Article 102287.

10. Bodriiiar Zh. Simulyakry i simulyatsiya. Ripol Klassik, 2013.

11. Goffman E. The Presentation of Self in Everyday Life. Garden City, N.Y.: Doubleday, 1959.

12. Digital Services Act. EUR-Lex. URL: https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html (01.10.2025).

13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 June 2024 on Digital Services (Digital Services Act). Official Journal of the European Union, L XXX. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (15.10.2025).

14. Online Trust and Safety Research Programme and Centre for Advanced Technologies in Online Safety (CATOS). Ministry of Digital Development and Information (Singapore), 10 January 2024. URL: https://www.mddi.gov.sg/newsroom/online-trust-and-safety-catos (11.09.2025).

15. National Cybersecurity Strategy, South Korea. International Telecommunication Union (ITU), 2023. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf (15.09.2025).

16. Sakharov A. G., Shelepov A. V. Politika Kitaiskoi Narodnoi Respubliki v sfere regulirovaniya tsifrovykh platform. Vestnik mezhdunarodnykh organizatsii: obrazovanie, nauka, novaya ekonomika, 2024, T. 19, № 2, S. 8.

17. Building Trust and Reinforcing Democracy. OECD Public Governance Reviews. URL: https://www.oecd.org/en/publications/building-trust-and-reinforcing-democracy_76972a4a-en.html (08.10.2025).

18. Eshchanov A. Sh. Profilaktika moshennichestva s ispolzovaniem informatsionnykh sistem. Chelovek i Zakon, 20 iyunya 2025. URL: https://astanazan.kz/?p=7067 (15.08.2025).

19. Ob utverzhdenii Kontseptsii po prodvizheniyu v obshchestve ideologii zakona i poryadka na 2025–2030 gody. Postanovlenie Pravitelstva Respubliki Kazakhstan ot 1 aprelya 2025 goda № 200. URL: https://adilet.zan.kz/rus/docs/P2500000200 (02.08.2025).

20. O profilaktike pravonarusheniy. Zakon Respubliki Kazakhstan ot 30 dekabrya 2025 goda № 245-VIII ZRK. URL: https://adilet.zan.kz/rus/docs/Z2500000245 // (09.01.2025).

Для цитирования и библиографии: Ещанов А.Ш., Садыков М.Б. Эволюция и трансформация мошенничества в условиях цифровизации условиях цифровизации: правовые и организационные аспекты противодействия в Республике Казахстан // Право и государство. № 1(110), 2026. – С. 71-79. DOI: 10.51634/2307-5201_2026_1_71

Материал поступил в редакцию 10.10.2025