Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Халықаралық құқық / International law/ Международное право

МРНТИ 10.19.61 https://doi.org/10.32523/2616-6844-2026-154-1-256-269
Научная статья

Сопоставительный анализ правовых подходов к противодействию deepfake-мошенничеству и социальной инженерии: опыт США, ЕС и Республики Казахстан

А.Б. Сактаганова[1*], И.С, Сактаганова[2], Б.У. Турегелдиев[3]

[1,2,3]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

(E-mail: [1]aridnisssakta.11@gmail.com, [2]aridniss@mail.ru, [3]bagdaulet.turegeldiyev@bk.ru)

Аннотация. В условиях современной цифровой трансформации стремительное развитие deepfake-технологий приводит к появлению новых, более изощренных форм онлайн-мошенничества. Контент, созданный с помощью технологии deepfake, особенно в сочетании с методами социальной инженерии, представляет собой серьезную угрозу правам и законным интересам отдельных лиц, общественной безопасности и институтам цифрового доверия. В этой связи разработка государствами правовых механизмов борьбы с мошенничеством, совершаемым с помощью deepfake, имеет актуальное научное и практическое значение.

В данной статье представлен сравнительно-правовой анализ правовых подходов к противодействию онлайн-мошенничеству и социальной инженерии, осуществляемым с использованием технологий deepfake. Исследование основано на законодательной практике США, Европейского Союза и Республики Казахстан и охватывает ключевые нормативные решения в области уголовно-правового регулирования, контроля цифрового контента, ответственности онлайн-платформ и защиты персональных данных. В частности, анализируются конкретные законодательные инициативы, касающиеся deepfake-контента в США, акты Европейского Союза, направленные на регулирование искусственного интеллекта, а также особенности действующего уголовного и информационного законодательства Республики Казахстан.

В ходе исследования были использованы методы сравнительно-правового, формально-логического и системного анализа. Научная новизна статьи характеризуется комплексным рассмотрением правовых угроз, возникающих на стыке deepfake и социальной инженерии, и выработкой предложений направленных на совершенствование национального законодательства.

Результаты исследования имеют практическое значение в совершенствовании правовой политики Республики Казахстан в области цифровой безопасности и формировании эффективных правовых механизмов борьбы с онлайн-мошенничеством.

Ключевые слова: Deepfake, онлайн-мошенничество, киберпреступность, цифровая безопасность, социальная инженерия, законодательство, правовая политика, правовой анализ.

Поступила: 19.01.2026 Одобрена: 17.03.2026 Доступна онлайн: 30.03.2026

***автор для корреспонденции**

Введение

Стремительное развитие цифровых технологий оказало значительное влияние на все сферы общества, позволив, с одной стороны, оптимизировать социально-экономические процессы, а с другой – открыв путь для возникновения новых угроз. Технологии deepfake, развивающиеся в последние годы на основе искусственного интеллекта, создают сложную и проблематичную ситуацию в области информационной безопасности и правового регулирования. Технологии deepfake позволяют создавать аудио-, видео- и визуальный контент, максимально приближенный к реальности, что, в свою очередь, значительно повышает эффективность методов онлайн-мошенничества и методов социальной инженерии. Данное явление представляет серьезную угрозу правам и законным интересам физических лиц, экономической стабильности, а также институтам цифрового доверия в обществе.

Выбор данной темы исследования обусловлен тем, что технологии deepfake – относительно новое явление, и их правовые последствия еще недостаточно систематически изучены. Как показывает анализ предыдущих исследований, в зарубежной научной литературе технологии deepfake часто рассматриваются с точки зрения информационной безопасности, киберпреступности или этических проблем. В частности, меньшее количество работ рассматривающих правовую практику США, Европейского Союза и Республики Казахстан в сравнительной перспективе, особенно повышает и научную актуальность исследования [1].

Актуальность темы определяется не только широким распространением технологий deepfake, но и полной неподготовленностью законодательства и правоприменительной практики к этому явлению. Во многих штатах мошеннические действия, совершаемые с помощью deepfake, оцениваются в рамках традиционных уголовно-правовых норм, что свидетельствует о неадекватности инновационных правовых ответов на новые технологические угрозы. В этом смысле изучение правовых подходов к противодействию deepfake и социальной инженерии имеет как теоретическое, так и практическое значение.

Объектом исследования является система правового регулирования против мошеннических действий, совершаемых в цифровой среде. Предметом исследования являются правовые подходы к противодействию онлайн-мошенничеству, осуществляемые с использованием технологий deepfake и социальной инженерии. Основная цель исследования – сравнительный анализ моделей правового регулирования против мошенничества и социальной инженерии deepfake на основе опыта США, Европейского Союза и Республики Казахстан и оценка их эффективности.

Для достижения этой цели поставлены следующие задачи: описать правовую природу технологий deepfake и их связь с методами социальной инженерии; проанализировать законодательные и институциональные механизмы борьбы с контентом deepfake в США; раскрыть содержание нормативно-правовых актов Европейского Союза в области искусственного интеллекта и цифровой безопасности; изучить нормы, касающиеся мошенничества с deepfake, в действующем законодательстве Республики Казахстан; выявить пробелы в правовом регулировании и перспективы развития на основе сравнительного анализа.

В исследовании используются сравнительно-правовые, формально-логические, систематические и аналитические методы. Кроме того, применялись методы анализа нормативно-правовых актов и изучения правоохранительной практики. Основная

гипотеза исследования заключается в том, что сочетание технологий deepfake и социальной инженерии снижает эффективность традиционных механизмов уголовного права и требует специального, всеобъемлющего правового регулирования. Эта гипотеза обосновывается и подкрепляется рекомендациями, представленными в статье [2].

Правовые и социальные последствия технологий deepfake активно изучаются в зарубежной научной литературе в последние годы. В ранних фундаментальных работах феномен deepfake рассматривался главным образом с точки зрения информационной безопасности, манипулирования СМИ и угроз демократическим институтам. Эти исследования подтвердили, что контент deepfake увеличивает риск искажения общественного мнения, распространения дезинформации и вторжения в частную жизнь. Однако в указанных работах уголовно-правовые последствия технологий deepfake часто затрагиваются лишь косвенно, а конкретные механизмы правового регулирования недостаточно систематизированы.

В исследованиях американских ученых проблема deepfake часто анализируется в контексте принципов свободы слова, неприкосновенности частной жизни и технологического нейтралитета. В этих работах основное внимание уделяется вопросу о балансе между ограничением контента deepfake и соблюдением конституционных прав. В ряде исследований также отмечается финансовый и репутационный ущерб от мошенничества с deepfake. Однако правовые особенности deepfake-мошенничества в сочетании с методами социальной инженерии редко рассматриваются как самостоятельный объект исследования; при этом комплексная оценка эффективности действующих уголовных норм не дается [3].

В европейской научной литературе технологии deepfake широко изучаются в контексте регулирования искусственного интеллекта. Исследователи уделяют приоритетное внимание этическим и правовым рискам deepfake, анализируя нормативные акты Европейского Союза в области защиты данных, цифровых услуг и искусственного интеллекта. В этих работах широко освещаются вопросы превентивных механизмов, ответственности платформ и алгоритмической прозрачности. Однако конкретные механизмы уголовно-правового противодействия и факторы социальной инженерии часто отходят на второй план, а практическая эффективность регулирования недостаточно раскрывается [4].

В научных исследованиях в странах Азии проблема deepfake рассматривается с точки зрения государственного контроля, кибербезопасности и поддержания общественного порядка. Хотя эти работы подчеркивают необходимость срочного правового реагирования на технологические угрозы, элементы сравнительно-правового анализа ограничены. В частности, редко проводятся исследования, сравнивающие инструменты, используемые различными правовыми системами для борьбы с deepfake и социальной инженерией.

Что касается казахстанской научной литературы, то вопросы технологий deepfake и онлайн-мошенничества все еще находятся на начальной стадии развития. В имеющихся работах вопросы киберпреступности, интернет-мошенничества и информационной безопасности рассматриваются в общих чертах, а сочетание deepfake и социальной инженерии не систематизировано как самостоятельная правовая проблема.

Существующие работы, как правило, рассматривают вопросы киберпреступности, онлайн-мошенничества и информационной безопасности, а сочетание deepfake и социальной инженерии не систематизировано как самостоятельная правовая проблема.

Также наблюдается небольшое количество исследований, которые анализируют национальное законодательство в сравнении с зарубежным опытом, что затрудняет выявление пробелов в правовом регулировании.

Таким образом, обзор литературы показывает, что, хотя проблемы технологий deepfake, онлайн-мошенничества и социальной инженерии были изучены в различных аспектах, комплексного и сравнительного анализа юридических проблем на их стыке недостаточно. В частности, отсутствие работ, рассматривающих опыт США, Европейского Союза и Республики Казахстан как единый объект сравнительно-правового исследования, оценивается как научный пробел. Данное обстоятельство повышает теоретическую и практическую значимость данного исследования и доказывает необходимость нового научного подхода, направленного на выявление эффективных моделей правового регулирования.

Материалы и методы исследования

Методология настоящего исследования направлена на сравнительный анализ правовых подходов к противодействию онлайн-мошенничеству с использованием технологий deepfake и социальной инженерии. Объектом исследования стала система правового регулирования противодействия мошенничеству в цифровой среде США, Европейского Союза и Республики Казахстан. Предметом исследования являются уголовно-правовые, административно-правовые и регулирующие правовые механизмы, применяемые против онлайн-мошенничества, связанного с технологиями deepfake и социальной инженерией.

Основной вопрос исследования: какими правовыми подходами различные правовые системы противодействуют онлайн-мошенничеству, основанному на deepfake и социальной инженерии, и в чем эффективность этих подходов? Чтобы прояснить этот вопрос, были заданы следующие дополнительные исследовательские вопросы: возможна ли криминально-правовая дифференциация мошенничества с использованием технологий deepfake; на каком уровне установлена правовая ответственность онлайн-платформ; насколько развиты механизмы профилактики и оперативного реагирования в национальном законодательстве.

Основная гипотеза исследования заключается в том, что комбинированное использование deepfake и социальной инженерии снижает эффективность правовых механизмов против традиционного онлайн-мошенничества и требует комплексных специальных моделей правового регулирования. Данная гипотеза проверяется с помощью сравнительно-правового анализа.

Исследование проводилось в несколько этапов. На первом этапе был проведен систематический обзор зарубежной и отечественной научной литературы по вопросам технологий deepfake, социальной инженерии и онлайн-мошенничества. На данном этапе сформированы теоретические основы исследования, определены основные понятия и категории. На втором этапе были отобраны и проведен содержательный анализ нормативных правовых актов США, Европейского Союза и Республики Казахстан. На третьем этапе полученные данные систематизировались сравнительно-правовым методом, выявляются сходства и различия правового регулирования. На заключительном этапе обобщаются результаты исследования, формулируются выводы и рекомендации [5, 4].

В ходе исследования были использованы следующие научные методы. Сравнительно-правовой метод использовался для сравнения правовых средств, используемых различными правовыми системами против deepfake-мошенничества, выбор этого метода был обусловлен транснациональным характером исследования. Формально-логический метод применялся с целью анализа содержания правовых норм и определения взаимосвязи правовых понятий. Метод системного анализа позволил рассматривать правовое регулирование как единый механизм. Также для раскрытия особенностей применения нормативных актов использовались методы правового анализа и интерпретации.

В качестве материала исследования были взяты федеральное законодательство США [6], акты Европейского Союза, регулирующие искусственный интеллект и цифровые услуги [7], а также Уголовный кодекс Республики Казахстан [8], Закон об искусственном интеллекте [9] и другие отраслевые законы [10]. При обработке материалов использовались правовые базы данных, официальные государственные порталы и научные электронные базы. Для систематизации и сопоставления правовых текстов использовались средства текстового анализа и программное обеспечение для управления нормативными данными.

С методологической точки зрения преимуществом исследования является применение комплексного и сравнительного подхода, а ограничения – ограниченность судебной практики по deepfake-мошенничеству и тот факт, что некоторые правовые нормы находятся на стадии формирования. Однако эти ограничения не снижают актуальность результатов исследования, а скорее определяют инновационный характер исследования.

Результаты и обсуждение

Результаты проведенного исследования показали, что правовое регулирование онлайн-мошенничества с использованием технологий deepfake и социальной инженерии неоднородно в разных штатах. Сравнительный анализ опыта США, Европейского Союза и Республики Казахстан выявил наличие существенных различий и общих тенденций в понимании правовой природы данного явления, а также в определении механизмов эффективного противодействия.

Согласно результатам исследования, правовые подходы к борьбе с deepfake-мошенничеством в США часто носят фрагментарный характер. Хотя универсальная уголовно-правовая норма, направленная непосредственно на deepfake, еще не сформирована на федеральном уровне, в ряде штатов приняты специальные законодательные акты, касающиеся использования контента deepfake. Эти нормы часто применяются в случаях посягательств на частную жизнь, мошенничества или распространения ложной информации. Результаты показывают, что в правовой системе США основной приоритет отдается принципам свободы слова и избежания ограничений технологических инноваций. В этом смысле противодействие deepfake и социальной инженерии часто опирается на механизмы гражданской ответственности и саморегулирования платформ. Хотя этот подход является гибким, он оценивается как недостаточный с точки зрения защиты жертв [6].

Результаты анализа опыта Европейского Союза показали формирование правового подхода к проблеме deepfake, имеющего системный и превентивный характер. В ЕС

комплексные акты, направленные на регулирование искусственного интеллекта, вводят задачи по установлению, ограничению и контролю контента deepfake, классифицируя его как категорию высокого риска. Результаты исследования показывают, что в этой модели преобладают административно-правовые и регуляторные механизмы, а не уголовно-правовые санкции. Задачи, алгоритмическая прозрачность и средства защиты прав пользователей, возлагаемые на онлайн-платформы, направлены на предотвращение deepfake-мошенничества. Однако анализ показывает, что такой подход также имеет определенные ограничения: хотя превентивные меры ужесточаются, проблема ответственности за конкретные преступные действия не всегда очевидна [7].

Результаты анализа опыта Республики Казахстан показали, что национальное законодательство лишь частично адаптировано к новым угрозам, связанным с технологиями deepfake и социальной инженерией. В то время как действующее уголовное законодательство содержит нормы о мошенничестве, незаконном распространении информации и защите персональных данных, не существует специальных правил, непосредственно охватывающих технологии deepfake. Как было установлено в ходе исследования, данная ситуация создает определенные трудности в правоприменительной практике, поскольку не всегда возможно квалифицировать действия, совершенные с помощью deepfake, в соответствие с традиционными составами преступлений. В результате юридическая реакция задерживается или становится неэффективной [8].

Сравнение полученных результатов с существующими научными исследованиями позволило выявить общие тенденции в отношении проблемы deepfake. В зарубежных исследованиях deepfake часто рассматривается как угроза демократическим процессам, конфиденциальности и информационной безопасности. В этих работах часто отмечается, что темпы технологического развития опережают правовое регулирование. Результаты нашего исследования, подтверждая эти результаты, показали, что сочетание deepfake и социальной инженерии многократно увеличивает юридические риски. Методы социальной инженерии, в частности, использующие психологические уязвимости человека, могут повысить надежность deepfake-контента и позволить обойти механизмы правовой защиты.

Выдвинутая в исследовании гипотеза также в значительной степени подтвердилась. Было установлено, что комбинированное использование deepfake и социальной инженерии снижает эффективность традиционных правовых механизмов борьбы с онлайн-мошенничеством. В то время как в США этот вопрос ограничивается принципами защиты свободы слова, в ЕС преобладает профилактика, но ясность уголовного права недостаточна. В Казахстане основными проблемными факторами являются фрагментация правового регулирования и отсутствие специальных норм.

В ходе обсуждения был выявлен еще один важный результат: во всех трех изученных правовых системах недостаточно только уголовно-правовых подходов в борьбе с deepfake-мошенничеством. Эффективность правового регулирования во многом зависит от институциональной совместимости, ответственности платформ и гибкости правоприменительной практики. Этот вывод согласуется с взглядами зарубежных авторов на превентивные и многоуровневые модели регулирования [11,376].

Также результаты исследования показали необходимость учета национальных особенностей правового регулирования. В то время как модель США направлена на защиту технологических инноваций, модель ЕС отдает приоритет усилению правовой

безопасности и превентивных мер. Для Казахстана важно не механическое копирование этих практик, а адаптация их элементов к национальной правовой системе. Особенно актуальными являются: правовое определение технологий deepfake, уточнение уголовной ответственности, связанной с их использованием, и определение задач онлайн-платформ.

Теоретическая значимость полученных результатов характеризуется обоснованием возможности рассмотрения deepfake и социальной инженерии как единого правового феномена. С практической точки зрения результаты исследования могут служить основой для совершенствования правовой политики в области цифровой безопасности в Республике Казахстан. Эти результаты дополняют пробелы в существующих научных исследованиях и предлагают новый научный подход, направленный на разработку эффективных правовых моделей против deepfake-мошенничества [12].

Таким образом, результаты исследования позволили выявить сильные и слабые стороны правового регулирования с помощью сравнительного анализа правовых действий против deepfake и социальной инженерии. Полученные данные и анализ показали, что только правовые подходы, учитывающие комплексный, многоуровневый характер и темпы технологического развития в этой области, могут дать эффективные результаты.

Заключение

Сегодня цифровые технологии быстро развиваются, и риск того, что инструменты на основе искусственного интеллекта, такие как deepfake, будут использоваться для мошенничества и социальной инженерии, значительно вырос. Технология deepfake позволяет реалистично воссоздавать голос и изображение человека, что создает новые угрозы: подкуп с помощью поддельных видеороликов, обман людей, манипулирование информацией в социальных сетях и экономический ущерб. В этом контексте обеспечение эффективности правовых систем регулирования в борьбе с deepfake стало стратегической задачей современной юриспруденции. Сравнительный анализ показывает, что США и Европейский Союз активно развивают правовые основы в борьбе с deepfake. США вводят особые правовые нормы в отношении deepfake на федеральном уровне. Например, ограничивается использование речевых и видеоматериалов без согласия лиц, при этом мошенничество рассматривается как существенное отягчающее обстоятельство. В странах ЕС, в частности в законе Artificial Intelligence Act, формируются правила в направлении укрепления алгоритмических угроз и безопасности персональных данных [13].

Хотя правовая система Республики Казахстан демонстрирует определенный прогресс в разработке нормативно-правовой базы, направленной на противодействие цифровым угрозам, в ней недостаточно норм, конкретно регулирующих deepfake и социальную инженерию. Действующее законодательство охватывает только классические проявления мошенничества, то есть не в полной мере раскрывает специфику deepfake – механизмы, посредством которых контент, модифицированный искусственным интеллектом, становится правонарушением. Поэтому правовой системе Казахстана необходимы конкретные, четко определенные правовые нормы, соответствующие современным особенностям технологии deepfake.

Ряд важных выводов, полученных в ходе исследования, следующие:

– Правовое определение deepfake, касающееся создания и распространения контента, четко не установлено действующим законодательством. Это точно определяет правонарушение и ограничивает эффективную деятельность правоохранительных органов.

– Уровень уголовной ответственности в отношении элементов deepfake, используемых в мошенничестве и социальной инженерии, низок – это увеличивает шансы киберпреступников воспользоваться ситуацией.

– Обязанности и ответственность платформ для борьбы с контентом deepfake, распространяемым на общественных информационных площадках, социальных сетях и коммерческих платформах, законодательно не определены.

– Международная практика сочетает в себе правовые требования против deepfake, образовательные программы, механизмы технологического контроля, принципы гражданской юридической ответственности. В Казахстане координация в этом направлении осуществляется на более низком уровне [14].

– Действующее законодательство недостаточно предусматривает конкретные процедуры защиты прав юридических и физических лиц (например, удаление контента, требования о компенсации).

В целом, создание эффективных правовых подходов против мошенничества, связанных с deepfake и социальной инженерией, является сложной задачей, требующей как теоретических, так и практических инноваций. В правовой системе Казахстана этот вопрос не до конца изучен и требует системного внедрения лучших практик, полученных из международного опыта. В связи с этим гипотеза исследования – если в регуляторной базе будут внедрены специальные нормы и механизмы против deepfake, усилится ответственность правоохранительной системы и будут эффективно защищены права граждан оно подтверждается данными и сравнительными анализами.

Рекомендации:

1. Поправки к Уголовному кодексу

Мошенничество, совершенное с использованием технологии deepfake

Пункт 1. Мошенничество лица или организации с использованием технологии deepfake, причинение материального или нематериального ущерба путем использования их изображения или голоса без их согласия является уголовным преступлением.

Пункт 2. Проявления данной статьи:

а) распространение deepfake-видео/голосовых материалов в отношении физического лица;

б) использование электронной подписи, документа в качестве поддельного документа с использованием deepfake;

в) использование deepfake на информационных платформах с целью получения финансовых данных физического лица.

Пункт 3. Виды и размеры наказания для обвиняемого по данной статье: от штрафа до ограничения свободы.

Обоснование: Потенциальный вред, причиняемый deepfake обществу и личности, превышает вред, причиняемый классическим мошенничеством, поэтому необходимо ввести для него специальную уголовную категорию.

2. Поправки к Гражданскому кодексу (в сфере частного права)

Право человека на защиту от deepfake

Пункт 1. Каждый имеет право на то, чтобы его изображение, голос или личная информация не изменялись и не распространялись на основе deepfake.

Пункт 2. Устанавливается гражданская ответственность (возмещение ущерба, удаление контента, порядок выплаты компенсации) за нарушение данной статьи.

Пункт 3. Регулятивно устанавливаются сроки и порядок обязывающих каналов распространения (социальные сети, платформы) удалять контент.

Обоснование: Защита прав и достоинства личности является важным элементом в борьбе с deepfake.

3. Поправки к законодательству о регулировании электронных коммуникаций

Обязанности платформ по мониторингу и удалению информации

Пункт 1. Онлайн-платформы (социальные сети, видеохостинги, мессенджеры) обязаны внедрять технические и организационные меры по обнаружению, оценке и удалению контента, созданного с помощью deepfake.

Пункт 2. Устанавливается гражданская ответственность (компенсация ущерба, удаление контента, созданного с помощью deepfake) за нарушение данной статьи.

Пункт 3. Несоблюдение этого обязательства повлечет за собой административную ответственность платформ (штрафы, ограничения на использование сервисов).

Пункт 4. Срок удаления очевидного deepfake-контента составляет не более 24 часов.

Обоснование: Поскольку платформы являются основным каналом распространения deepfake, их обязательства должны быть отражены в законодательстве.

4. Изменения в законодательстве о защите персональных данных

Защита персональных данных, связанных с deepfake

Пункт 1. Обработка персональных данных, собранных для использования в deepfake –материалах, признатся незаконной без согласия субъекта.

Пункт 2. Должны быть установлены специальные меры безопасности для сбора, хранения, обработки и распространения этих данных.

Пункт 3. Должна быть введена административная и уголовная ответственность для лиц, незаконно обрабатывающих персональные данные.

Обоснование: deepfake-материалы часто требуют предоставления персональных данных, поэтому усиление защиты данных является важной частью борьбы с deepfake.

5. Включение в образовательные и профилактические программы

Рекомендация: Правоохранительные органы Республики Казахстан, Министерство науки и высшего образования и ИТ-индустрия должны совместно разрабатывать программы по предотвращению deepfake и повышению информационной грамотности населения.

Включить:

– курсы медиаграмотности

– образовательные стандарты по цифровой безопасности

– программы государственно – частного партнерства

Обоснование: одних правовых норм недостаточно, необходимо повышать информационную культуру и цифровое здоровье общества.

Исследование, анализирующее правовые аспекты deepfake в сфере мошенничества и социальной инженерии, показало следующие важные выводы:

– Отсутствие специальных правовых дефиниций – недостаточно регламентирует правовой статус deepfake; .

– Слабость механизмов ответственности – действующие нормы не охватывают новые технологические риски;

– Задачи платформ и лиц неясны – усложняет работу правоохранительных органов.

Представленные выше конкретные статьи законопроекта укрепляют правовую основу борьбы с deepfake и систематизируют механизмы расследования, правоохранительных органов и гражданской защиты.

Информация о финансировании

Данное исследование было профинансировано научным комитетом Министерства науки и высшего образования Республики Казахстан по теме «Сравнительный анализ законодательства зарубежных стран по противодействию онлайн-мошенничеству с использованием deepfake и социальной инженерии». (AP26103625 «Онлайн-мошенничество с помощью deepfake-технологий и социальной инженерии: проблемы уголовно-правового противодействия, перспективы законодательного регулирования»).

Вклад авторов:

Сактаганова Акмарал Бакытовна – сыграла ключевую роль в подготовке основных выводов, руководила исследовательским процессом и участвовала в доработке рукописи. Она также внесла вклад в улучшение качества и точности окончательной версии.

Сактаганова Индира Советовна – сыграла ключевую роль в разработке концепции и дизайна исследования, сборе и анализе данных, а также интерпретации результатов. Она взяла на себя ответственность за общую целостность работы, решала вопросы, связанные с точностью и полнотой данных статьи, написала рукопись, оценила и доработала критические разделы, а также провела обзор соответствующей литературы.

Турегельдиев Бакдаулет Усербаевич предоставил экспертное руководство, возглавил разработку концепции и методологии исследования. Он рецензировала рукопись и участвовал в переводе исследовательскиех материалов.

Список литературы

1. Apsimet, N.M., 2025. Crimes involving deepfake in online fraud and the challenges of proving them. Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, 3(80), pp. 357–368. Available at: https://vestnik.zqai.kz/index.php/vestnik/article/view/1794 (Accessed: 12 December 2025).

2. Smanova, A.B., Muratova, A.Zh. and Zhumagulova, S.R., 2025. Deepfake technologies and social engineering in online fraud: forms, mechanisms, and legal challenges. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 152(3), pp. 188–211. Available at: https://bullaw.enu.kz/index.php/main/article/view/608 (Accessed: 12 December 2025).

3. Beaver, K., 2025. International and domestic legal frameworks on online fraud and deepfake technologies: a comparative criminal law analysis. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 152(3), pp. 212–228. Available at: https://bullaw.enu.kz/index.php/main/article/view/609 (Accessed: 12 December 2025).

4. Romero-Moreno, F., 2025. Deepfake detection in generative AI: a legal framework proposal to protect human rights. Computer Law & Security Review. Available at: https://www.sciencedirect.com/science/article/pii/S2212473X25000355 (Accessed: 12 December 2025).

5. Lumen, C., 2025. Deepfakes and the limits of law: a comparative analysis of regulatory frameworks in the U.S., EU, and China. Journal of Advanced Artificial Intelligence, 2(3), pp. 1–7. Available at: https://jaaionline.org/archives/volume2/number3/lumen-jaai202550.pdf (Accessed: 12 December 2025).

6. U.S. Congress, 2023–2024. H.R.5586 — Deepfakes Accountability Act, 118th Congress. Available at: https://www.congress.gov/bill/118th-congress/house-bill/5586/text (Accessed: 12 December 2025).

7. European Parliament and Council, 2024. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1 // (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R1689 (Accessed: 12 December 2025).

8. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 01.01.2026 г.). Available at: https://online.zakon.kz/Document/?doc_id=31575252 (Accessed: 01 January 2026).

9. Об искусственном интеллекте Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК. Available at: https://adilet.zan.kz/rus/docs/Z2500000230 (Accessed: 17 January 2026).

10. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 30.11.2025 г.). Available at: https://online.zakon.kz/Document/?doc_id=33885902 (Accessed: 30 November 2025).

11. Ткалина, А. (2025) Правовое регулирование цифровой технологии «deepfake». Цифровые технологии и право, № 1 (3), pp. 360–372. Available at: https://inlibrary.uz/index.php/digteclaw/article/view/135262 (Accessed: 12 December 2025).

12. Geng, S. (2023) Comparing «deepfake» regulatory regimes in the U.S., EU and China. Georgetown Law Technology Review. Available at: https://georgetownlawtechreview.org/wp-content/uploads/2023/01/Geng Deepfakes.pdf (Accessed: 12 December 2025).

13. EU AI Act: first regulation on artificial intelligence. The use of artificial intelligence in the EU is regulated by the AI Act, the world's first comprehensive AI law. Find out how it protects you (2023) Published: 08 June 2023. Last updated: 19 February 2025. Available at: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?utm_source=chatgpt.com (Accessed: 19 February 2025).

14. Ramluckan, T. (2024) Deepfakes: the legal implications. Proceedings of The 19th International Conference on Cyber Warfare and Security (ICCWS 2024), Vol. 19 No. 1, pp. 282–288. Available at: https://papers.academic-conferences.org/index.php/iccws/article/view/2099 (Accessed: 12 December 2025).

Сактаганова А.Б.*[1], Сактаганова И.С.[2], Турегелдиев Б.У.[3]

[1,2,3]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

(E-mail: [1]aridnisssakta.11@gmail.com, [2]aridniss@mail.ru, [3]bagdaulet.turegeldiyev@bk.ru)

Deepfake – алаяқтық пен әлеуметтік инженерияға қарсы іс-қимылдың құқықтық тәсілдеріне салыстырмалы талдау: АҚШ, Еуропалық Одақ және Қазақстан Республикасының тәжірибесі

Аңдатпа. Қазіргі цифрлық трансформация жағдайында deepfake технологияларының қарқынды дамуы онлайн-алаяқтықтың жаңа, күрделі нысандарының пайда болуына әкелуде. Әсіресе әлеуметтік инженерия әдістерімен үйлескен deepfake контенті жеке тұлғалардың құқықтары

мен заңды мүдделеріне, қоғамдық қауіпсіздікке және цифрлық сенім институттарына елеулі қатер төндіреді. Осыған байланысты мемлекеттердің deepfake арқылы жасалатын алаяқтыққа қарсы құқықтық тетіктерді қалыптастыруы өзекті ғылыми және практикалық маңызға ие.

Аталған мақалада deepfake технологияларын пайдалану арқылы жүзеге асырылатын онлайн-алаяқтық пен әлеуметтік инженерияға қарсы іс-қимылдың құқықтық тәсілдеріне салыстырмалы-құқықтық талдау жүргізіледі. Зерттеу АҚШ, Еуропалық Одақ және Қазақстан Республикасының заңнамалық тәжірибесіне негізделеді, қылмыстық-құқықтық реттеу, цифрлық контентті бақылау, онлайн-платформалардың жауапкершілігі және жеке деректерді қорғау салаларындағы негізгі нормативтік шешімдерді қамтиды, атап айтқанда, АҚШ-тағы deepfake контентіне қатысты арнайы заңнамалық бастамалар, Еуропалық Одақтың жасанды интеллектіні реттеуге бағытталған актілері және Қазақстан Республикасының қолданыстағы қылмыстық және ақпараттық заңнамасының ерекшеліктері талданады.

Зерттеу барысында салыстырмалы құқықтық талдау, формальды-логикалық және жүйелік талдау әдістері қолданылды. Мақаланың ғылыми жаңалығы deepfake пен әлеуметтік инженерияның түйіскен тұсында туындайтын құқықтық қатерлерді кешенді түрде қарастыруымен және ұлттық заңнаманы жетілдіруге бағытталған ұсыныстар әзірлеуімен сипатталады. Зерттеу нәтижелері Қазақстан Республикасының цифрлық қауіпсіздік саласындағы құқықтық саясатын жетілдіруге және онлайн-алаяқтыққа қарсы тиімді құқықтық механизмдерді қалыптастыруда практикалық маңызға ие.

Түйін сөздер: deepfake, онлайн-алаяқтық, киберқылмыс, цифрлық қауіпсіздік, әлеуметтік инженерия, заңнама, құқықтық саясат, құқықтық талдау

Saktaganova A.B.*[1], Saktaganova I.S.[2], Turegeldiev B.U.[3]
[1,2,3]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
(E-mail: [1]aridnisssakta.11@gmail.com, [2]aridniss@mail.ru, [3]bagdaulet.turegeldiyev@bk.ru)

Comparative analysis of legal approaches to countering deepfake fraud and social engineering: the experience of the USA, the EU, and the Republic of Kazakhstan

Annotation. In the context of modern digital transformation, the rapid development of deepfake technologies leads to the emergence of new, more sophisticated forms of online fraud. Content created using Deepfake technology, especially when combined with social engineering techniques, poses a serious threat to the rights and legitimate interests of individuals, public safety, and institutions of digital trust. In this regard, the development by States of legal mechanisms to combat fraud committed with the help of deepfakes is of urgent scientific and practical importance.

This article presents a comparative legal analysis of legal approaches to countering online fraud and social engineering carried out using deepfake technologies. The study is based on the legislative practice of the United States, the European Union, and the Republic of Kazakhstan and covers key regulatory decisions in the field of criminal law regulation, digital content control, responsibility of online platforms, and personal data protection. In particular, the article analyzes specific legislative initiatives related to deepfake content in the United States, acts of the European Union aimed at regulating artificial intelligence, as well as the specifics of the current criminal and information legislation of the Republic of Kazakhstan.

In the course of the research, the methods of comparative legal, formal-logical, and system analysis were used. The scientific novelty of the article is characterized by a comprehensive consideration of

the legal threats arising at the junction of deepfake and social engineering, and the development of proposals aimed at improving national legislation. The results of the study are of practical importance in improving the legal policy of the Republic of Kazakhstan in the field of digital security and the formation of effective legal mechanisms to combat online fraud.

Keywords: Deepfake, online fraud, cybercrime, digital security, social engineering, legislation, legal policy, legal analysis

References

1. Apsimet, N.M., 2025. Crimes involving deepfake in online fraud and the challenges of proving them. Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, 3(80), pp. 357–368. Available at: https://vestnik.zqai.kz/index.php/vestnik/article/view/1794 (Accessed: 12 December 2025).

2. Smanova, A.B., Muratova, A.Zh. and Zhumagulova, S.R., 2025. Deepfake technologies and social engineering in online fraud: forms, mechanisms, and legal challenges. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 152(3), pp. 188–211. Available at: https://bullaw.enu.kz/index.php/main/article/view/608 (Accessed: 12 December 2025).

3. Beaver, K., 2025. International and domestic legal frameworks on online fraud and deepfake technologies: a comparative criminal law analysis. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 152(3), pp. 212–228. Available at: https://bullaw.enu.kz/index.php/main/article/view/609 (Accessed: 12 December 2025).

4. Romero-Moreno, F., 2025. Deepfake detection in generative AI: a legal framework proposal to protect human rights. Computer Law & Security Review. Available at: https://www.sciencedirect.com/science/article/pii/S2212473X25000355 (Accessed: 12 December 2025).

5. Lumen, C., 2025. Deepfakes and the limits of law: a comparative analysis of regulatory frameworks in the U.S., EU, and China. Journal of Advanced Artificial Intelligence, 2(3), pp. 1–7. Available at: https://jaaionline.org/archives/volume2/number3/lumen-jaai202550.pdf (Accessed: 12 December 2025).

6. U.S. Congress, 2023–2024. H.R.5586 — Deepfakes Accountability Act, 118th Congress. Available at: https://www.congress.gov/bill/118th-congress/house-bill/5586/text (Accessed: 12 December 2025).

7. European Parliament and Council, 2024. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1 // (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R1689 (Accessed: 12 December 2025).

8. Ugolovnyj kodeks Respubliki Kazahstan ot 3 ijulja 2014 goda № 226-V (s izmenenijami i dopolnenijami po sostojaniju na 01.01.2026 g.). Available at: https://online.zakon.kz/Document/?doc_id=31575252 (Accessed: 01 January 2026).

9. Ob iskusstvennom intellekte Zakon Respubliki Kazahstan ot 17 nojabrja 2025 goda № 230-VIII ZRK. Available at: https://adilet.zan.kz/rus/docs/Z2500000230 (Accessed: 17 January 2026).

10. Zakon Respubliki Kazahstan ot 24 nojabrja 2015 goda № 418-V «Ob informatizacii» (s izmenenijami i dopolnenijami po sostojaniju na 30.11.2025 g.). Available at: https://online.zakon.kz/Document/?doc_id=33885902 (Accessed: 30 November 2025).

11. Tkalina, A. (2025) Pravovoe regulirovanie cifrovoj tehnologii «deepfake». Cifrovye tehnologii i pravo, № 1 (3), pp. 360–372. Available at: https://inlibrary.uz/index.php/digteclaw/article/view/135262 (Accessed: 12 December 2025).

12. Geng, S. (2023) Comparing «deepfake» regulatory regimes in the U.S., EU and China. Georgetown Law Technology Review. Available at: https://georgetownlawtechreview.org/wp-content/uploads/2023/01/Geng-Deepfakes.pdf (Accessed: 12 December 2025).

13. EU AI Act: first regulation on artificial intelligence. The use of artificial intelligence in the EU is regulated by the AI Act, the world's first comprehensive AI law. Find out how it protects you (2023) Published: 08 June 2023. Last updated: 19 February 2025. Available at: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?utm_source=chatgpt.com (Accessed: 19 February 2025).

14. Ramluckan, T. (2024) Deepfakes: the legal implications. Proceedings of The 19th International Conference on Cyber Warfare and Security (ICCWS 2024), Vol. 19 No. 1, pp. 282–288. Available at: https://papers.academic-conferences.org/index.php/iccws/article/view/2099 (Accessed: 12 December 2025).

Information about authors:

Saktaganova A.B. **–** corresponding author, PhD, Senior Lecturer, Department of criminal law disciplines, L.N. Gumilyov Eurasian National University, 2A Satpayev str., 010000, Astana, Kazakhstan.

Saktaganova I.S. **–** Doctor of Law, Professor, Department of Constitutional and Civil Law, L.N. Gumilyov Eurasian National University, 2A Satpayev str., 010000, Astana, Kazakhstan.

Turegeldiev B.U. **–** doctoral student, Faculty of Law, L.N. Gumilyov Eurasian National University, 2A Satpayev str., 010000, Astana, Kazakhstan.

Сактаганова А.Б. **–** хат-хабар авторы, PhD, аға оқытушы, қылмыстық-құқық кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 010000, Сәтпаев көшесі 2А, 010000, Астана, Қазақстан.

Сактаганова И.С. – заң ғылымдарының кандидаты, профессор, конституциялық және азаматтық құқық кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 010000, Сәтпаев көшесі 2А, 010000, Астана, Қазақстан.

Турегелдиев Б.У. **–** докторант, заң факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 010000, Сәтпаев көшесі 2А, 010000, Астана, Қазақстан.

Сактаганова А.Б. **–** автор для корреспонденции, PhD, старщий преподаватель, кафедра уголовно-правовых дисциплин, Евразийский Национальный университет имени Л.Н. Гумилева, Сатпаева 2А, 010000, Астана, Казахстан.

Сактаганова И.С. **–** кандидат юридических наук, профессор, кафедра конституционного и гражданского права, Евразийский Национальный университет имени Л.Н. Гумилева, Сатпаева 2А, 010000, Астана, Казахстан.

Турегелдиев Б.У. – докторант, юридический факультет, Евразийский национальный университет имени Л.Н. Гумилева, Сатпаева 2А, 010000, Астана, Казахстан.