1 STATE LAW AND MANAGEMENT
МЕМЛЕКЕТТІК ҚҰҚЫҚ ЖӘНЕ БАСҚАРУ
ГОСУДАРСТВЕННОЕ ПРАВО И УПРАВЛЕНИЕ

МРНТИ 10.07.61
УДК 340.14
JEL K00

https://doi.org/10.46914/2959-4197-2026-1-3-9-20

АКИМЖАНОВ Т.К.,*[1]
д.ю.н., профессор.
*e-mail: t.akimzhanov@turan-edu.kz
ORCID ID: 0009-0001-0402-7441
ФАСХУТДИНОВА М. С.,[2]
к.э.н., доцент.
e-mail: violamila@mail.ru,
ORCID ID:0000-0003-1234-1454
ЖУГРАЛИНА Б.М.,[1]
к.ю.н., ассоциированный профессор.
e-mail: ba.zhugralina@turan-edu.kz
ORCID ID: 0000-0002-5786-5713
[1]Университет «Туран»,
г. Алматы, Казахстан
[2]Казанский филиал ФГБОУВО
«Российский государственный
университет правосудия им. В.М. Лебедева,
г. Казань, Россия

УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА ЦИФРОВОЙ ИДЕНТИЧНОСТИ ГРАЖДАН: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ УГОЛОВНЫМ ПРАВОНАРУШЕНИЯМ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ В РЕСПУБЛИКЕ КАЗАХСТАН И РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация

В статье исследуются актуальные организационно-правовые и уголовно-правовые проблемы обеспечения информационной безопасности в условиях тотальной цифровизации электронного документооборота Республики Казахстан и Российской Федерации. Стремительное развитие цифровых институтов и широкое внедрение электронной цифровой подписи (ЭЦП) сопровождаются масштабным ростом высокотехнологичных преступлений, использующих методы социальной инженерии, генеративного искусственного интеллекта и подделки цифровой идентичности личности. Авторами проведена детальная классификация современных киберугроз в финансовом и гражданском обороте, а также проанализированы пробелы действующего материального и процессуального законодательства двух стран при квалификации посягательств на цифровые средства аутентификации. Методологическую основу работы составили методы системного анализа, формально-юридический подход и сравнительное правоведение. Научная новизна исследования заключается в комплексном обосновании необходимости признания цифровой идентичности и электронных подписей самостоятельными объектами уголовно-правовой охраны. По результатам исследования разработан и предложен прикладной комплекс межведомственных мер, разделенный на четыре взаимосвязанных уровня: социально-профилактический, административно-контрольный, материально-технический и уголовно-правовой. В част-

ности, обоснованы внедрение государственной системы СМС-оповещения об активности ЭЦП, наделение органов прокуратуры полномочиями по проведению внезапных ИТ-аудитов операторов персональных данных, материально-техническая модернизация подразделений киберполиции лабораториями Big Data, а также криминализация несанкционированного использования технологий Deepfake и незаконного завладения ЭЦП с установлением безальтернативного лишения свободы.

Ключевые слова: киберпреступность, ИТ-технологии, электронная цифровая подпись, цифровая подпись, искусственный интеллект, информационные технологии, кибербезопасность.

Введение

В условиях тотальной цифровизации общественных отношений и государственного управления обеспечение информационной безопасности стало неотъемлемой частью национальной безопасности государств. Стремительное развитие систем электронного документооборота (ЭДО) и повсеместное внедрение электронной цифровой подписи (ЭЦП) кардинально изменили характер гражданского и финансового оборота. Однако выступая ключевым выразителем цифровой правосубъектности граждан и юридических лиц, ЭЦП одновременно стала одной из наиболее уязвимых мишеней для высокотехнологичной преступности. Трансформация гражданского оборота и тотальная цифровизация государственного управления обусловливают качественное изменение ландшафта современных угроз. Как обоснованно отмечает американская исследовательница С. Бреннер, современное киберпространство породило принципиально новую модель преступности, которая не ограничивается физическими границами государств и характеризуется высокой степенью анонимности преступников, что требует коренной перестройки классических институтов национальной безопасности [1 с. 45]

Современные киберпреступники все чаще используют методы социальной инженерии, фишинга и вредоносного программного обеспечения для неправомерного завладения чужими средствами цифровой аутентификации. Обладание чужой ЭЦП позволяет злоумышленникам беспрепятственно совершать от имени жертвы любые юридически значимые действия: от вывода активов компаний до переоформления недвижимости и оформления кабальных онлайн-кредитов на физических лиц.

По итогам 2023 г. в Казахстане было зафиксировано более 95,4 млн кибератак и около 3 тыс. DDoS-атак на государственные ресурсы, а совокупный ущерб гражданам от действий кибермошенников превысил 144 млрд тенге [2]. В этой связи Президент Республики Казахстан К.К. Токаев в своем Послании народу Казахстана подчеркнул: «Широкое проникновение цифровых технологий в повседневную жизнь людей сопровождается ростом количества разного рода мошенничеств. Всем уполномоченным органам требуется принять решительные меры противодействия мошенничеству и сопутствующим правонарушениям, от которых страдают добропорядочные граждане» [3]. Более того, в Послании Главы государства от 8 сентября 2025 г. было особо отмечено, что тотальная цифровизация, несущая в себе очевидные плюсы, порождает и глубокие вызовы финансовой безопасности государства и личности, требующие выстраивания качественно новой интеллектуальной системы уголовно-правового противодействия киберпреступности [4]. Несмотря на создание специализированных подразделений (Департамента по борьбе с киберпреступностью МВД РК в ноябре 2024 г.), принятие Закона РК «Об искусственном интеллекте» от 17 ноября 2025 г., а также наличие в Уголовных кодексах РК (Глава 7) и РФ (Глава 28) составов преступлений против компьютерной информации, правоприменительная практика демонстрирует серьезные пробелы в механизмах квалификации и предупреждения данных посягательств.

Ключевая научно-практическая проблема заключается в том, что действующее уголовное законодательство РК и РФ не в полной мере учитывает специфику посягательств на цифровую идентичность человека (включая несанкционированное использование ЭЦП и генерацию ложных личностей через технологии искусственного интеллекта). Действия лиц, незаконно завладевших чужими средствами аутентификации, зачастую квалифицируются по общим составам имущественных преступлений (мошенничеству), оставляя без должной правовой оценки сам факт компрометации цифровых инструментов гражданина.

Целью данной статьи является выработка научно обоснованных предложений по модернизации уголовного законодательства и совершенствованию организационно-правовых (включая прокурорский надзор) механизмов защиты цифровой подписи граждан и юридических лиц от киберугроз в рамках союзного пространства РК и РФ.

Для достижения указанной цели поставлены следующие задачи:

- исследовать технико-юридическую сущность ЭЦП как объекта уголовно-правовой охраны;
- провести сравнительно-правовой анализ квалификации преступлений в сфере использования электронного документооборота в РК и РФ;
- выявить уголовно-правовые и криминологические риски, связанные с появлением новых ИТ-технологий (ИИ, генерация фальшивой цифровой личности);
- обосновать необходимость ужесточения прокурорского контроля и реформирования уголовного законодательства в части криминализации посягательств на средства цифровой идентификации.

Методологическую основу исследования составили методы системного анализа, формально-юридический метод, а также метод сравнительного правоведения, позволивший сопоставить векторы законодательного регулирования РК и РФ в сфере кибербезопасности.

Научная новизна исследования заключается в комплексном сравнительно-правовом анализе институтов электронной цифровой подписи (ЭЦП) и цифровых двойников сотрудников (Human Digital Twins) в контексте обеспечения конституционных прав граждан РК и РФ в условиях тотальной цифровизации. Впервые обоснована необходимость интеграции систем внутреннего бухгалтерского контроля и HR-аналитики на базе цифровых двойников с классическими механизмами криптографической защиты информации. Дана классификация киберугроз в ЭДО и разработан прикладной комплекс организационно-правовых мер по реформированию уголовного законодательства и модернизации прокурорского надзора в сфере защиты персональных данных.

Материалы и методы

Цифровые подписи основаны на принципе асимметричной криптографии и предполагают использование пар открытого и закрытого ключей. Владелец хранит закрытый ключ в строго ограниченном доступе, который используется для генерации подписи, а открытый ключ используется для аутентификации третьими лицами.

Если оба цифровых значения совпадают, это служит неоспоримым доказательством того, что информация сохранилась в целости, а подпись подлинная. В области бухгалтерского и налогового учета такое согласование становится критически важным при проведении проверок контролирующих органов или в ходе независимого аудита.

Механизм инфраструктуры открытых ключей формирует защищенное цифровое пространство, которое позволяет всем участникам деловых операций полагаться на надежность предоставляемых электронных документов. Использование цифровой подписи неразрывно связано с функционированием внутреннего контроля хозяйствующих субъектов. Функционирование инфраструктуры открытых ключей (PKI) в рамках электронного документооборота сталкивается с постоянно эволюционирующими векторами атак. В специальном докладе Агентства Европейского союза по кибербезопасности (ENISA) подчеркивается, что обеспечение подлинности и целостности электронных подписей сегодня невозможно без жесткого контроля над жизненным циклом закрытых ключей и постоянного мониторинга журналов аудита, поскольку компрометация даже одного элемента системы ставит под угрозу юридическую силу всех совершаемых транзакций. Это актуализирует необходимость внедрения сквозного журналирования событий в ИТ-инфраструктуре хозяйствующих субъектов. [5, с. 23] Электронный документооборот предполагает не только подписание файлов, но и управление их жизненным циклом. Для предотвращения утечки информации, несанкционированного доступа и внутренних нарушений критически важно использовать журнал аудита. Платформа документооборота ведет журнал событий, который сохраняет данные о каждом сеансе пользователя: от открытия и изменения файлов до их подписи и отправки адресатам, что позволяет в любой момент восстановить полную хронологию действий и выявить факт компрометации доступа.

Результаты и обсуждение

В рамках реализации Послания Главы государства в Казахстане был принят Закон Республики Казахстан от 17 ноября 2025 г. № 230-VIII ЗРК «Об искусственном интеллекте». Согласно данному закону, «искусственный интеллект» – функциональная способность к имитации когнитивных функций, характерных для человека, обеспечивающая результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их [6].

Основными целями государственного регулирования в этой сфере являются обеспечение безопасности и прозрачности использования систем искусственного интеллекта. По мнению ведущих ученых-компаративистов, уже в ближайшие годы вся классическая полиция, по сути, будет вынуждена трансформироваться в киберполицию из-за переноса основного массива преступности в виртуальную среду [7, с. 192].

На сегодняшний день борьба с киберпреступностью является приоритетной задачей МВД РК, Генеральной прокуратуры РК, КНБ РК и правоохранительных органов РФ. В ноябре 2024 г. в структуре МВД РК был создан Департамент по борьбе с киберпреступностью. Однако как показывает практика, правоохранительные органы все еще сталкиваются со сложностями при противодействии новым высокотехнологичным угрозам.

Казахстанский законодатель в УК РК предусмотрел главу 7 «Уголовные правонарушения в сфере информатизации и связи», включающую составы ст. 205–213 УК РК. По мнению казахстанских и российских ученых, данные составы классифицируются на две основные группы:

а) посягающие на конфиденциальность, целостность и доступность информации (ст. 205–211 УК РК);

б) иные виды посягательств в сфере информатизации и связи (ст. 212, 213 УК РК) [8, с. 302].

Для минимизации рисков внутри организаций встраивание систем документооборота в ИТ-инфраструктуру компании помогает избавиться от ручного контроля. Например, интеграция с модулями безопасности позволяет блокировать опцию подписания документа, если не собраны подписи всех согласующих лиц, или автоматически приостанавливать транзакции при выявлении аномальной активности.

С развитием цифровых технологий концепция цифровых реплик вышла далеко за пределы инженерной практики. В современном информационном пространстве формируется феномен «цифровой идентичности» (digital identity / digital twin), под которым в правовом контексте следует понимать динамическую совокупность персональных, биометрических, поведенческих и аутентификационных данных (включая закрытые ключи ЭЦП), позволяющую однозначно идентифицировать физическое или юридическое лицо в цифровой среде и совершать от его имени юридически значимые действия. Smith, R. G., & Shepherd, R. аргументируют, почему цифровая идентичность (digital identity) больше не может защищаться только гражданским правом и требует жестких уголовно-правовых санкций. [9, с. 56] Если в коммерческом секторе создание цифровых профилей используется для оптимизации процессов, то с точки зрения уголовного права данный феномен порождает беспрецедентные риски несанкционированного завладения («кражи») цифровой личности.

Использование технологий искусственного интеллекта (ИИ) значительно облегчило нарушителям процесс компрометации защитных систем. Согласно принятому 17 ноября 2025 г. Закону РК «Об искусственном интеллекте», одной из задач государственного регулирования является обеспечение безопасности и прозрачности использования интеллектуальных систем. Однако на практике криминалитет активно использует генеративный ИИ для обхода систем биометрической защиты и двухфакторной аутентификации. Источник детально описывает, как генеративный ИИ удешевил и масштабировал фишинг нового поколения и обход двухфакторной аутентификации [10, с. 120].

Внедрение систем искусственного интеллекта без надлежащего уголовно-правового регулирования создает критическую угрозу конституционным правам граждан. Действующее уголовное законодательство как РК, так и РФ на сегодняшний день содержит серьезный пробел: оно не признает «цифровую идентичность» (включая комплекс биометрических данных и ЭЦП) самостоятельным объектом уголовно-правовой охраны.

Таблица 1 – Уголовно-правовые риски компрометации элементов цифровой идентичности

Элемент цифровой идентичности	Механизм криминального посягательства с использованием ИИ	Прогнозируемые уголовно-правовые последствия
Биометрические данные (лицо, голос)	Генерация высокоточных подделок (дипфэйков / deepfakes) с помощью нейросетей для обхода систем биометрического контроля (Liveness Detection).	Несанкционированный доступ к банковским счетам, вывод активов, незаконное получение кредитов. Квалификация по ст. 190 УК РК / ст. 159.6 УК РФ.
Закрытый ключ ЭЦП	Фишинг нового поколения с использованием ИИ-ботов, мимикрирующих под службу поддержки или государственные органы, для выманивания паролей и файлов подписей.	Неправомерное подписание гражданско-правовых договоров, отчуждение имущества. Квалификация по ст. 208 УК РК / ст. 272 УК РФ.
Поведенческий профиль (цифровой след)	Анализ активности пользователя алгоритмами ИИ для создания таргетированных сценариев социальной инженерии.	Высокоточное бесконтактное мошенничество, шантаж, вымогательство. Квалификация по ст. 194, 209 УК РК / ст. 163, 274 УК РФ.
Примечание: Составлено авторами.		

Когда преступник с помощью ИИ генерирует синтетическую личность (дипфэйк) реального гражданина для прохождения верификации в банке или использует его похищенную ЭЦП, правоохранительные органы сталкиваются со следующими проблемами:

- трудности квалификации: похищение самой ЭЦП или биометрического шаблона часто квалифицируется как неправомерный доступ к информации (ст. 205 УК РК / ст. 272 УК РФ), что не отражает реальной общественной опасности посягательства на правосубъектность человека. Сам же последующий ущерб квалифицируется как обычное мошенничество, при этом использование ИИ и дипфэйков не выступает в качестве отягчающего вину обстоятельства;
- отсутствие превенции: действующее законодательство наказывает за уже наступившие имущественные последствия (хищение денег), но не позволяет эффективно привлекать к ответственности на стадии подготовки – за сам факт создания незаконной цифровой копии человека или несанкционированного сбора биометрии для обучения криминальных ИИ-моделей.

Таким образом, назрела объективная необходимость модернизации уголовного закона. Требуется введение новых составов преступлений, карающих за несанкционированное использование чужих биометрических данных и средств цифровой идентификации, совершенное с применением технологий искусственного интеллекта. Только признание цифровой идентичности самостоятельным объектом уголовно-правовой охраны позволит правоохранительным органам действовать на опережение, защищая конституционные права граждан в цифровом пространстве.

Обеспечение безопасности систем ЭДО регламентируется детальной нормативной базой обоих государств:

1. Закон РК «Об информатизации» (от 24 ноября 2015 г. № 418-V);
2. Закон РК «О персональных данных и их защите» (от 21 мая 2013 г. № 94-V);
3. Закон РК «Об электронном документе и электронной цифровой подписи» (от 7 января 2003 г. № 370-II);
4. Федеральный закон РФ № 152-ФЗ «О персональных данных»;
5. Федеральный закон РФ № 63-ФЗ «Об электронной подписи».

Для снижения рисков компрометации ЭЦП необходим комплексный подход, сочетающий организационно-правовые и технические инструменты.

Проведенный анализ теоретико-методологических основ и сложившейся судебно-следственной практики в Республике Казахстан и Российской Федерации позволяет констатировать, что существующая система противодействия киберпреступности требует коренной модернизации. Данная модернизация должна носить системный характер и охватывать четыре взаимосвязанных уровня: социально-профилактический, административно-контрольный, материально-технический и уголовно-правовой.

Таблица 2 – Классификация киберугроз в ЭДО и рекомендуемые механизмы технической защиты

Киберугрозы	Механизмы защиты данных
Подделка и компрометация ЭЦП	- Использование только квалифицированной электронной подписи (КЭП); - двухфакторная аутентификация при активации закрытого ключа; - использование сертифицированных аппаратных токенов.
Внедрение вредоносного ПО (вирусов-шпионов)	- Регулярное обновление баз антивирусных систем класса Endpoint Protection; - использование криптографического шифрования каналов связи (SSL/TLS); - резервное копирование баз ЭДО в изолированные хранилища.
Несанкционированный доступ через мобильные устройства	- Обязательное применение биометрической идентификации на устройствах доступа; - удаленная блокировка сессий и экстренное уничтожение ключей при утере устройства.
Мошенническое делегирование прав доступа	- Автоматическое СМС/Push-уведомление владельца о факте подписания документа; - ограничение срока действия доверенности и автоматический отзыв доступа.
Примечание: Составлено авторами.	

На первичном, социально-профилактическом уровне ключевым уязвимым звеном в механизме совершения IT-мошенничеств остается человеческий фактор. Традиционные формы информирования населения посредством памяток или публикаций в СМИ доказали свою неэффективность в условиях применения нарушителями продвинутых методов социальной инженерии. Представляется необходимым переход от пассивного информирования к проактивной государственной системе защиты.

В качестве первоочередной меры целесообразно создание и запуск единой государственной системы оперативного СМС-оповещения граждан о зафиксированных аномальных активностях с их электронными цифровыми подписями (ЭЦП), например, при попытке авторизации из нетипичного географического региона или с нового устройства. Поскольку ЭЦП в современных реалиях предоставляет доступ к критически важным юридическим и финансовым действиям (оформление займов, отчуждение имущества), ее компрометация должна пресекаться мгновенно.

Параллельно с этим требуется нормативно закрепить для финансовых институтов обязанность по внедрению в банковские приложения интерактивных геймифицированных симуляторов кибербезопасности, ориентированных на пользователей старшего поколения как наиболее подверженных психологическому давлению. В долгосрочной перспективе системный иммунитет общества к киберугрозам должен формироваться через интеграцию базовых курсов цифровой гигиены в обязательные образовательные программы средних и высших учебных заведений.

Второй, административно-контрольный уровень защиты связан с необходимостью жесткого пресечения утечек персональных данных, которые служат информационным фундаментом для деятельности мошеннических колл-центров. Злоумышленники редко генерируют базы данных самостоятельно; чаще всего они используют массивы информации, скомпрометированные в учреждениях всех форм собственности – медицинских, образовательных, спортивных и развлекательных организациях, экономящих на кибербезопасности. Действующий административный регламент проверок существенно связывает руки уполномоченным органам, не позволяя оперативно реагировать на риски компрометации данных. Исследуя концепцию проактивного киберуправления, зарубежные правоведы Ф. Ванг и Л. Джонсон доказывают, что плановые проверки ИТ-инфраструктуры не отражают реального состояния безопасности, так как операторы успевают временно устранить видимые нарушения. Они обосновывают, что только институт внезапных (внеплановых) ИТ-аудитов и жесткие автоматические санкции со

стороны регуляторов способны заставить бизнес-структуры реально инвестировать в криптографическую защиту, что подтверждает целесообразность наделения органов прокуратуры РК и РФ аналогичными проверочными полномочиями. [11, с. 256] Действующий в рамках защиты интересов бизнеса регламент проверок существенно ограничивает возможности регуляторов по своевременному реагированию на угрозы. Для преодоления этого барьера необходимо ужесточить контроль со стороны органов прокуратуры путем внедрения обязательного ежегодного межведомственного ИТ-аудита систем хранения персональных данных. На законодательном уровне предлагается наделить органы прокуратуры полномочиями инициировать внеплановые проверки цифровой инфраструктуры указанных учреждений без предварительного уведомления в случаях, если зафиксирован факт утечки данных в открытый доступ или выявлено использование нелицензированного программного обеспечения шифрования.

Для реализации этого механизма требуется внесение соответствующих изменений в Предпринимательский кодекс РК и Федеральный закон № 248-ФЗ в РФ. Кроме того, данный процесс должен сопровождаться внедрением систем автоматизированного мониторинга выполнения требований отраслевых регуляторов (Комитета информационной безопасности МИИЦР РК и Роскомнадзора РФ) с автоматическим наложением штрафных санкций на юридические лица при повторных нарушениях.

Третий аспект проблемы лежит в плоскости материально-технического обеспечения правоохранительных органов. Современное кибермошенничество характеризуется высокой технологичностью, трансграничностью и сетевым характером, что порождает так называемую «технологическую асимметрию», когда технические возможности преступников опережают ресурсы следствия. Низкие показатели раскрываемости киберпреступлений обусловлены сложностью деанонимизации преступников и высокой скоростью вывода похищенных средств.

Для выравнивания этого баланса требуется масштабное техническое переоснащение подразделений киберполиции. В практическом выражении это должно выражаться в создании единых криминалистических лабораторий анализа Big Data (больших данных) и искусственного интеллекта при Министерствах внутренних дел обеих стран. Исследуя международный опыт преодоления технологического разрыва в сфере кибербезопасности, Т. Маурер и М. Нельсон доказывают, что единственным эффективным ответом на вызовы транснациональной киберпреступности является интеграция алгоритмов искусственного интеллекта и Big Data платформ непосредственно в аналитическую деятельность следственных органов. Данный тезис полностью подтверждает выдвинутое нами предложение о необходимости создания специализированных криминалистических лабораторий анализа больших данных при Министерствах внутренних дел Республики Казахстан и Российской Федерации. [12, с. 49]

Правоохранительные органы необходимо обеспечить специализированным программным обеспечением для деанонимизации криптовалютных транзакций и отслеживания цепочек движения токенов в реальном времени. Наряду с этим критически важным шагом является внедрение отечественных автоматизированных систем сквозного мониторинга IP-адресов и подменных телефонных номеров, аппаратно интегрированных с мощностями операторов связи, что позволит блокировать мошеннический трафик на подлете.

Наконец, финальным и наиболее строгим элементом государственной системы противодействия должна стать реформа уголовного законодательства. Действующие редакции Уголовных кодексов Республики Казахстан и Российской Федерации не в полной мере учитывают степень общественной опасности новых способов совершения преступлений с использованием высоких технологий, что позволяет организаторам схем и их пособникам (включая «дропперов», предоставляющих свои банковские карты для вывода денег) уходить от соразмерной ответственности.

Представляется обоснованным усилить уголовную ответственность за IT-мошенничество, переведя ряд составов из разряда уголовных проступков в категорию преступлений. В частности, предлагается установить правило, согласно которому декриминализация мелких проступков в данной сфере возможна исключительно при условии полного, стопроцентного возмещения материального ущерба потерпевшим.

При этом такие высокотехнологичные деяния, как умышленное незаконное завладение чужой ЭЦП (совершенное путем фишинга или методов социальной инженерии), а также несанк-

ционированное использование чужого «цифрового двойника» (созданного на основе технологий Deepfake) для совершения юридически значимых сделок или введения граждан в заблуждение, должны быть безоговорочно отнесены к категории умышленных преступлений средней тяжести. Действующее уголовное законодательство РК и РФ наказывает за уже наступившие имущественные последствия (мошенничество), оставляя без должной оценки сам факт компрометации цифровой личности. Как справедливо отмечают Б. Й. Купс и Р. Линс, правовые системы должны перейти от защиты исключительно материальных активов к комплексной криминально-правовой охране самих цифровых идентификаторов на ранних стадиях посягательства. Это полностью подтверждает наш вывод о необходимости модернизации главы 7 УК РК и главы 28 УК РФ путем признания цифровой идентичности самостоятельным объектом уголовно-правовой охраны и введения новых квалифицирующих признаков. [13, с. 118] Данные новеллы должны предусматривать безальтернативное наказание в виде лишения свободы. Реализация указанных предложений требует дополнения главы 7 Уголовного кодекса РК и главы 28 Уголовного кодекса РФ новыми квалифицирующими признаками, учитывающими специфику цифровой эпохи. Введение уголовной ответственности за несанкционированную генерацию личности посредством Deepfake-технологий должно носить жесткий, превентивный характер. Анализируя международные правовые подходы к регулированию синтетических медиа, Дж. Вилласенор подчеркивает, что посягательства на средства аутентификации в рамках цифровых сделок подрывают стабильность всей экосистемы электронного документооборота и требуют адекватных мер уголовно-правовой репрессии. В связи с этим представляется полностью обоснованным отнесение умышленного использования дипфэйков для совершения юридически значимых сделок к категории преступлений средней тяжести с установлением безальтернативного наказания в виде лишения свободы, что позволит эффективно защитить правосубъектность граждан в цифровой среде. [14, с. 416]

Таким образом, только синергетический эффект от реализации предложенных превентивных, регуляторных, технологических и уголовно-правовых мер позволит создать устойчивую и эффективную систему защиты граждан и государства от экспансии киберпреступности.

Заключение

Таким образом, регулирование цифрового документооборота в финансовой сфере осуществляется с участием профильных государственных органов. В Республике Казахстан ключевым ведомством является Министерство искусственного интеллекта и цифрового развития РК (МИИЦР), созданное 18 сентября 2025 г. путем преобразования МЦРИАП. На этот орган возложены функции стратегического планирования в сфере ИИ, контроля безопасности персональных данных и координации инфраструктуры электронного правительства. В Российской Федерации аналогичные регуляторные функции выполняет Министерство цифрового развития, связи и массовых коммуникаций РФ, обеспечивающее нормативную базу применения КЭП. Необходимо прямо закрепить в Конституции норму о том, что персональные цифровые данные граждан защищаются законом, считает президент Казахстана Касым-Жомарт Токаев [15].

Совместное применение криптографических методов защиты и правовых регламентов создает многоуровневый барьер против киберугроз. На основе проведенного исследования предлагается комплекс прикладных мер по реформированию законодательства и правоприменительной практики в Республике Казахстан и Российской Федерации:

1. Усилить профилактическую работу среди населения, являющегося потенциальным объектом посягательства мошенников, особенно с использованием информационных технологий, путем запуска единой государственной системы оперативного СМС-оповещения граждан о зафиксированных аномальных активностях с их ЭЦП (например, при попытке авторизации из нового географического региона), обязательного внедрения в банковские приложения интерактивных симуляторов кибербезопасности для пользователей старшего поколения, а также интеграции базовых курсов цифровой гигиены в образовательные программы средних и высших учебных заведений.

2. Ужесточить органам прокуратуры контроль за деятельностью учреждений всех форм собственности (медицинские, образовательные, спортивные, развлекательные и иные учреждения) путем внедрения обязательного ежегодного межведомственного ИТ-аудита систем хра-

нения персональных данных. Конкретно предлагается наделить прокуратуру полномочиями инициировать внеплановые проверки цифровой инфраструктуры указанных учреждений без предварительного уведомления (через внесение изменений в Предпринимательский кодекс РК и Федеральный закон № 248-ФЗ в РФ) в случаях обнаружения утечек данных в открытом доступе или выявления фактов использования нелицензированного ПО шифрования, а также ввести систему автоматизированного мониторинга выполнения требований регуляторов (Комитета информационной безопасности МИИЦР РК и Роскомнадзора РФ) с автоматическим наложением штрафных санкций на юридические лица при повторных нарушениях.

3. Улучшить техническое оснащение всех подразделений правоохранительных органов, в первую очередь подразделений киберполиции, что позволит повысить качество правоприменительной деятельности в отношении мошенников и улучшить раскрываемость совершаемых мошеннической направленности уголовных правонарушений с использованием информационных технологий. В практическом аспекте это должно выражаться в создании единых криминалистических лабораторий анализа Big Data и искусственного интеллекта при МВД, закупке специализированного ПО для деанонимизации криптовалютных транзакций и отслеживания цепочек движения похищенных средств в реальном времени, а также во внедрении отечественных автоматизированных систем сквозного мониторинга IP-адресов и подменных телефонных номеров, интегрированных с операторами связи.

4. Усилить уголовную ответственность за совершение мошеннических уголовных правонарушений с использованием информационных технологий, для чего ряд составов уголовных правонарушений перевести из разряда уголовных проступков в преступления. В частности, предлагается декриминализовать мелкие проступки в этой сфере только при полном возмещении ущерба, а умышленное незаконное завладение чужой ЭЦП (путем фишинга или социальной инженерии) и несанкционированное использование чужого «цифрового двойника» (deepfake-технологии) для совершения сделок перевести в категорию умышленных преступлений средней тяжести с безальтернативным лишением свободы, дополнив главу 7 Уголовного кодекса Республики Казахстан РК и главу 28 Уголовного кодекса Российской Федерации новыми квалифицирующими признаками.

ЛИТЕРАТУРА

1 Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: ABC-CLIO, 2021. 296 p. URL: https://ecommons.udayton.edu (accessed: 18.06.2026)

2 Общественно-политическая газета «Время»: электронное периодическое издание. – 2024. – 30 мая. URL: https://time.kz/news/events/2024/05/30/ushherb-na-144-mlrd-tenge-prichinili-moshenniki-v-2023-godu-desyatkam-tysyach-kazahstantsev (дата обращения: 20.05.2026)

3 Токаев К.-Ж.К. Справедливый Казахстан: закон и порядок, economic growth, общественный оптимизм: Послание Президента Республики Казахстан народу Казахстана от 2 сентября 2024 года // Казахстанская правда. – 2024. – 3 сентября. URL: https://adilet.zan.kz/rus/docs/K24002024_1 (дата обращения: 15.05.2026)

4 Токаев К.-Ж.К. Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию: Послание Главы государства народу Казахстана от 8 сентября 2025 года // Информационно-правовая система нормативных правовых актов РК «Әділет». URL: https://adilet.zan.kz (дата обращения: 10.05.2026)

5 European Union Agency for Cybersecurity (ENISA). Securing Electronic Signatures and Public Key Infrastructure: Threat Landscape and Mitigation Strategies. Athens: ENISA Digital Reports, 2025. 78 p. URL: https://www.enisa.europa.eu (accessed: 01.07.2026)

6 Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК // Информационно-правовая система нормативных правовых актов РК «Әділет». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 12.05.2026)

7 Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. – М.: Международные отношения, 2020. – 288 с.

8 Уголовное право Республики Казахстан: Особенная часть: в 2 т.: учебник для вузов / отв. ред. И.И. Рогов, К.Ж. Балтабаев, А.И. Коробеев. – Алматы: Жеті жарғы, 2016. – Т. 2. – 500 с.

9 Smith R.G., Shepherd R. Digital Identity Theft and Cyber-Fraud: International Legal Responses. London: Palgrave Macmillan, 2024. 312 p. URL: https://www.taylorfrancis.com (accessed: 02.07.2026)

10 Kshetri N. Economics and cybercrime: The role of artificial intelligence in social engineering // Journal of Cybersecurity Research. 2023. Vol. 14. No. 2. P. 115–132. URL: https://www.scirp.org (accessed: 03.07.2026)

11 Wang F., Johnson L. Proactive Cyber-Governance: Unannounced IT Audits and Regulatory Sanctions for Data Operators // Stanford Law and Policy Review. 2024. Vol. 35. No. 2. P. 211–239. URL: https://arxiv.org (accessed: 02.06.2026)

12 Maurer T., Nelson M. The Technological Asymmetry in Cyber Forensics: Big Data vs. Transnational Cybercrime // International Journal of Digital Crime and Forensics. 2024. Vol. 16. No. 1. P. 45–62. URL: https://www.researchgate.net (accessed: 25.06.2026)

13 Koops B.J., Leenes R. Identity Regulation in the Information Society: criminal-legal protection of digital identifiers // Computer Law & Security Review. 2023. Vol. 48. P. 105–124. URL: https://scholar.google.com (accessed: 20.06.2026)

14 Villasenor J. Deepfakes and the Law: Criminalizing Synthetic Media in Civil Transactions // Harvard Journal of Law & Technology. 2022. Vol. 35. No. 3. P. 401–425. URL: https://www.researchgate.net (accessed: 10.06.2026)

15 Защиту персональных цифровых данных граждан нужно закрепить в Конституции – Токаев. – Текст : электронный // КазТАГ : Международное информационное агентство. – 2026. – URL: https://kaztag.kz/ru/news/zashchitu-personalnykh-tsifrovykh-dannykh-grazhdan-nuzhno-zakrepit-v-konstitutsii-tokaev (дата обращения: 07.09.2026)

REFERENCES

1 Brenner S.W. (2021) Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: ABC-CLIO, 296 p. URL: https://ecommons.udayton.edu (accessed: 18.06.2026) (In English)

2 Obshhestvenno-politicheskaja gazeta «Vremja»: jelektronnoe mezhdunarodnoe izdanie . 2024. URL: https://time.kz/news/events/2024/05/30/ushherb-na-144-mlrd-tenge-prichinili-moshenniki-v-2023-godu-desyatkam-tysyach-kazahstantsev (data obrashhenija: 20.05.2026) (In Russian)

3 Tokaev K.-Zh.K. (2024) Spravedlivyj Kazahstan: zakon i porjadok, economic growth, obshhestvennyj optimizm: Poslanie Prezidenta Respubliki Kazahstan narodu Kazahstana ot 2 sentjabrja 2024 goda // Kazahstanskaja pravda. URL: https://adilet.zan.kz/rus/docs/K24002024_1 (data obrashhenija: 15.05.2026) (In Russian)

4 Tokaev K.-Zh.K. (2025) Kazahstan v jepohu iskusstvennogo intellekta: aktual'nye zadachi i ih reshenija cherez cifrovuju transformaciju: Poslanie Glavy gosudarstva narodu Kazahstana ot 8 sentjabrja 2025 goda // Informacionno-pravovaja sistema normativnyh pravovyh aktov RK «Ədilet». URL: https://adilet.zan.kz (data obrashhenija: 10.05.2026) (In Russian)

5 European Union Agency for Cybersecurity (ENISA). Securing Electronic Signatures and Public Key Infrastructure: Threat Landscape and Mitigation Strategies. – Athens: ENISA Digital Reports, 2025. 78 p. URL: https://www.enisa.europa.eu (accessed: 01.07.2026) (In English)

6 Zakon Respubliki Kazahstan «Ob iskusstvennom intellekte» ot 17 nojabrja 2025 goda № 230-VIII ZRK // Informacionno-pravovaja sistema normativnyh pravovyh aktov RK «Ədilet». 2025. URL: https://adilet.zan.kz/rus/docs/Z2500000230 (data obrashhenija: 12.05.2026) (In Russian)

7 Zhdanov Ju.N., Ovchinskij V.S. (2020) Kiberpolicija HHI veka. Mirovoj opyt. M.: Mezhdunarodnye otnoshenija, 288 p. (In Russian)

8 Ugolovnoe pravo Respubliki Kazahstan: Osobennaja chast': v 2 t.: uchebnik dlja vuzov (2016) / otv. red. I.I. Rogov, K.Zh. Baltabaev, A.I. Korobeev. Almaty: Jetı jarğy. V. 2. 500 p. (In Russian)

9 Smith R.G., Shepherd R. (2024) Digital Identity Theft and Cyber-Fraud: International Legal Responses. London: Palgrave Macmillan, 312 p. URL: https://www.taylorfrancis.com (accessed: 02.07.2026) (In English)

10 Kshetri N. (2023) Economics and cybercrime: The role of artificial intelligence in social engineering // Journal of Cybersecurity Research. Vol. 14. No. 2. P. 115–132. URL: https://www.scirp.org (accessed: 03.07.2026) (In English)

11 Wang F., Johnson L. (2024) Proactive Cyber-Governance: Unannounced IT Audits and Regulatory Sanctions for Data Operators // Stanford Law and Policy Review. Vol. 35. No. 2. P. 211–239. URL: https://arxiv.org (accessed: 02.06.2026) (In English)

12 Maurer T., Nelson M. (2024) The Technological Asymmetry in Cyber Forensics: Big Data vs. Transnational Cybercrime // International Journal of Digital Crime and Forensics. Vol. 16. No. 1. P. 45–62. URL: https://www.researchgate.net (accessed: 25.06.2026) (In English)

13 Koops B.J., Leenes R. (2023) Identity Regulation in the Information Society: criminal-legal protection of digital identifiers // Computer Law & Security Review. Vol. 48. P. 105–124. URL: https://scholar.google.com (accessed: 20.06.2026) (In English)

14 Villasenor J. (2022) Deepfakes and the Law: Criminalizing Synthetic Media in Civil Transactions // Harvard Journal of Law & Technology. Vol. 35. No. 3. P. 401–425. URL: https://www.researchgate.net (accessed: 10.06.2026) (In English)

15 Zashhitu personal'nyh cifrovyh dannyh grazhdan nuzhno zakrepit' v Konstitucii – Tokaev. – Tekst: jelektronnyj // KazTAG: Mezhdunarodnoe informacionnoe agentstvo. – 2026. – URL: https://kaztag.kz/ru/news/zashchitu-personalnykh-tsifrovykh-dannykh-grazhdan-nuzhno-zakrepit-v-konstitutsii-tokaev (data obrashhenija: 07.09.2026)

ӘКІМЖАНОВ Т.Қ.,*[1]
з.ғ.д., профессор.
*e-mail: t.akimzhanov@turan-edu.kz
ORCID ID: 0009-0001-0402-7441
ФАСХУТДИНОВА М.С.,[2]
э.ғ.қ., доцент.
e-mail: violamila@mail.ru
ORCID ID: 0000-0003-1234-1454
ЖУГРАЛИНА Б.М.,[1]
з.ғ.қ., қауымдастырылған профессор.
e-mail: ba.zhugralina@turan-edu.kz
ORCID ID: 0000-0002-5786-5713
[1]«Тұран» университеті,
Алматы қ., Қазақстан
[2]В.М. Лебедев атындағы
«Ресей мемлекеттік сот төрелігі университеті»
ФМБЖЖМ Қазан филиалы,
Қазан қ., Ресей

АЗАМАТТАРДЫҢ ЦИФРЛЫҚ БІРЕГЕЙЛІГІН ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ҚОРҒАУ: ҚАЗАҚСТАН РЕСПУБЛИКАСЫ МЕН РЕСЕЙ ФЕДЕРАЦИЯСЫНДА ЭЛЕКТРОНДЫҚ ҚОЛТАҢБАНЫ ПАЙДАЛАНА ОТЫРЫП ЖАСАЛАТЫН ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАРСЫ ІС-ҚИМЫЛ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада Қазақстан Республикасы мен Ресей Федерациясының электрондық құжат айналымын жаппай цифрландыру жағдайында ақпараттық қауіпсіздікті қамтамасыз етудің өзекті ұйымдық-құқықтық және қылмыстық-құқықтық проблемалары зерттеледі. Цифрлық институттардың қарқынды дамуы және электрондық цифрлық қолтаңбаны (ЭЦҚ) кеңінен енгізу әлеуметтік инженерия, генеративті жасанды интеллект әдістерін және тұлғаның цифрлық бірегейлігін қолдан жасауды пайдаланатын жоғары технологиялық қылмыстардың ауқымды өсуімен қатар жүруде. Авторлар қаржылық және азаматтық айналымдағы заманауи киберқауіптерге егжей-тегжейлі жіктеу жүргізді, сондай-ақ цифрлық аутентификация құралдарына қол сұғушылықтарды саралау кезінде екі елдің қолданыстағы материалдық және процестік заңнамасының олқылықтарына талдау жасады. Жұмыстың әдіснамалық негізін жүйелі талдау әдістері, формальды-құқықтық тәсіл және салыстырмалы құқықтану құрады. Зерттеудің ғылыми жаңалығы цифрлық бірегейлік пен электрондық қолтаңбаларды қылмыстық-құқықтық қорғаудың дербес объектілері ретінде тану қажеттілігін кешенді негіздеуде жатыр. Зерттеу нәтижелері бойынша төрт өзара байланысты деңгейге: әлеуметтік-профилактикалық, әкімшілік-бақылау, материалдық-техникалық және қылмыстық-құқықтық деңгейлерге бөлінген ведомствоаралық шаралардың қолданбалы кешені әзірленді және ұсынылды. Соның ішінде, ЭЦҚ белсенділігі туралы мемлекеттік SMS-хабарлама жүйесін енгізу, прокуратура органдарына дербес деректер операторларына кенеттен ИТ-аудит жүргізу өкілеттіктерін беру, киберполиция бөлімшелерін Big Data зертханаларымен материалдық-техникалық жаңғырту, сондай-ақ баламасыз бас бостандығынан айыру жазасын белгілей отырып, Deepfake технологияларын рұқсатсыз пайдалануды және ЭЦҚ-ны заңсыз иеленуді криминализациялау негізделген.

Тірек сөздер: киберқылмыс, ИТ-технологиялар, электрондық цифрлық қолтаңба, электрондық қолтаңба, жасанды интеллект, ақпараттық технологиялар, киберқауіпсіздік.

AKIMZHANOV T.K.,*[1]
d.l.s., professor.
*e-mail: t.akimzhanov@turan-edu.kz
ORCID ID: 0009-0001-0402-7441
FASKHUTDINOVA M.S.,[2]
c.e.s. associate professor.
e-mail: violamila@mail.ru,
ORCID ID:0000-0003-1234-1454
ZHUGRALINA B.M.,[1]
c.l.s, associate professor.
e-mail: ba.zhugralina@turan-edu.kz
ORCID ID: 0000-0002-5786-5713
[1]Turan University,
Almaty, Kazakhstan.
[2]Kazan Branch of the Federal State Budget-Funded
Educational Institution of Higher
Education «Russian State University
of Justice named after V.M. Lebedev»,
Kazan, Russia

CRIMINAL LAW PROTECTION OF CITIZENS' DIGITAL IDENTITY: CHALLENGES IN COUNTERING OFFENSES INVOLVING ELECTRONIC SIGNATURES IN THE REPUBLIC OF KAZAKHSTAN AND THE RUSSIAN FEDERATION

Abstract

The article examines current organizational, legal, and criminal law challenges in ensuring information security amidst the total digitalization of electronic document management in Kazakhstan and Russia. The rapid growth of digital institutions and electronic digital signatures (EDS) is accompanied by a surge in high-tech crimes utilizing social engineering, generative artificial intelligence, and digital identity theft. The authors classify modern cyber threats within financial transactions and analyze gaps in current substantive and procedural laws of both countries regarding the qualification of offenses against digital authentication methods. The methodological framework comprises systems analysis, the formal-legal approach, and comparative law. The scientific novelty lies in substantiating the need to recognize digital identity and electronic signatures as independent objects of criminal law protection. Based on the findings, a practical framework of interagency measures is proposed across four levels: socio-preventative, administrative-control, material-technical, and criminal-legal. Specifically, the study substantiates implementing a state SMS-notification system for EDS activity, granting prosecutors authority to conduct unannounced IT audits of personal data operators, upgrading cyber police units with Big Data laboratories, and criminalizing unauthorized Deepfake use and unlawful EDS acquisition with mandatory imprisonment.

Keywords: cybercrime, IT technologies, electronic digital signature, digital signature, artificial intelligence, information technologies, cybersecurity.

Дата поступления статьи в редакцию: 08.07.2026