



Ж.К. Какимов

*Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан,
г. Косшы, Республика Казахстан*

ТРАНСФОРМАЦИЯ ИНСТИТУТА ДИСЦИПЛИНАРНОЙ ОТВЕТСТВЕННОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье исследуются актуальные вопросы трансформации института дисциплинарной ответственности сотрудников органов внутренних дел в условиях цифровизации управленческих процессов. Предметом исследования являются правовые и организационные отношения, возникающие при фиксации должностных проступков в виртуальной среде. Методологическую основу работы составили формально-юридический метод, системно-структурный подход и метод правового моделирования. Эмпирической базой послужили результаты обобщения практики проверок в департаментах полиции за 2024-2025 гг.

Автор обосновывает вывод о том, что переход к модели управления на основе данных (data-driven governance) требует не только технологического обновления, но и формирования новой правовой базы ответственности за качество, достоверность и своевременность внесения информации в государственные информационные системы (далее – ИС). Главным научным результатом исследования является разработка концепции «цифровой дисциплинарной ответственности» и алгоритмической модели «Дисциплинарный ЕРАП» на базе искусственного интеллекта.

В работе обоснована необходимость автоматизации служебных расследований через внедрение стандартизированных цифровых шаблонов, что позволит минимизировать субъективизм и сократить бюрократические издержки. Практическая значимость работы заключается в том, что сформулированы предложения по внесению изменений в ведомственные нормативные акты МВД РК, регулирующие порядок проведения служебных расследований, и внедрению механизмов «цифрового следа» как доказательной базы дисциплинарного правонарушения.

Ключевые слова: цифровая ответственность; аналитические подразделения ОВД; служебное расследование; служебная дисциплина; Цифровой кодекс; правоохранительный орган; искусственный интеллект; цифровые доказательства.

Ж.К. Кәкімов

*Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының,
Қосшы қ., Қазақстан Республикасы*

ЦИФРАНДЫРУ ЖАҒДАЙЫНДА ІШКІ ІСТЕР ОРГАНДАРЫ ҚЫЗМЕТКЕРЛЕРІНІҢ ТӘРТІПТІК ЖАУАПТЫЛЫҚ ИНСТИТУТЫН ТРАНСФОРМАЦИЯЛАУ

Аннотация. Мақалада басқару процестерін цифрландыру жағдайында ішкі істер органдары қызметкерлерінің тәртіптік жауаптылық институтын трансформациялаудың өзекті мәселелері зерттеледі. Зерттеу пәні виртуалды ортада лауазымдық теріс қылықтарды тіркеу кезінде туындайтын құқықтық және ұйымдастырушылық қатынастар болып табылады. Зерттеудің әдіснамалық негізін формальды-құқықтық әдіс, жүйелік-құрылымдық тәсіл және құқықтық модельдеу әдісі құрады. Эмпирикалық негіз ретінде 2024-2025 жылдардағы полиция департаменттерінде жүргізілген тексерулер практикасын қорытындылау нәтижелері пайдаланылды.

Автор деректерге негізделген басқару моделіне (data-driven governance) көшу тек технологиялық жаңаруды ғана емес, сонымен қатар мемлекеттік ақпараттық жүйелерге ақпаратты енгізудің сапасы, анықтығы мен уақтылылығы үшін жауаптылықтың жаңа құқықтық базасын қалыптастыруды талап ететінін негіздейді. Негізгі ғылыми нәтиже «цифрлық тәртіптік жауаптылық» тұжырымдамасын және жасанды интеллект негізіндегі «Тәртіптік ӨЖБТ» алгоритмдік моделін әзірлеу болып табылады.

Жұмыста стандартталған цифрлық үлгілерді енгізу арқылы қызметтік тергеулерді автоматтандыру қажеттілігі негізделген, бұл субъективизмді барынша азайтуға және бюрократиялық шығындарды қысқартуға мүмкіндік береді. Жұмыстың практикалық маңыздылығы ҚР ІІМ қызметтік тергеулерді жүргізу тәртібін реттейтін



ведомстволық нормативтік актілеріне өзгерістер енгізу және тәртіптік құқық бұзушылықтың дәлелдемелік базасы ретінде «цифрлық із» тетіктерін енгізу бойынша ұсыныстар тұжырымдалған.

Түйінді сөздер: цифрлық жауаптылық; ІІО талдау бөлімшелері; қызметтік тергеу; қызметтік тәртіп; Цифрлық кодекс; құқық қорғау органы; жасанды интеллект; цифрлық дәлелдемелер.

Zh.K. Kakimov

*The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan,
Kosshy, the Republic of Kazakhstan*

TRANSFORMATION OF THE INSTITUTE OF DISCIPLINARY RESPONSIBILITY OF EMPLOYEES OF INTERNAL AFFAIRS BODIES IN THE CONTEXT OF DIGITALIZATION

Abstract. The article explores current issues regarding the transformation of the system of disciplinary liability for law enforcement officers in the context of the digitalization of management processes. The subject of the study comprises the legal and organizational relations arising from the registration of misconduct in the virtual environment. The methodological framework includes the formal-legal method, system-structural approach, and legal modeling, while the empirical base is drawn from data analyzed during internal investigations within Police Departments for the 2024-2025 period.

The author substantiates that transitioning to a data-driven governance model requires not only technological updates but also the formation of a new legal framework governing liability for the quality, accuracy, and timeliness of data entry into state information systems. The main scientific result is the development of the concept of “digital disciplinary liability” and the AI-based algorithmic model “Disciplinary ERAP”.

The paper substantiates the need to automate internal investigations through the implementation of standardized digital templates, which will minimize subjectivity and reduce bureaucratic costs. The practical significance of the study lies in the formulated proposals for amending the departmental regulatory acts of the Ministry of Internal Affairs of the Republic of Kazakhstan that govern internal investigation procedures, and for implementing “digital footprint” mechanisms as an evidentiary base for disciplinary offenses.

Keywords: digital disciplinary liability; analytical units of internal affairs bodies; internal investigation; service discipline; Digital Code; law enforcement agencies; artificial intelligence; digital evidence.

Введение. Актуальность темы исследования обусловлена масштабной цифровой трансформацией государственного управления в Республике Казахстан (далее – РК). Принятие Цифрового кодекса РК закрепило переход к модели управления на основе данных (*data-driven governance*), где информация признается стратегическим ресурсом.

В системе органов внутренних дел (далее – ОВД) ключевая роль в этой трансформации отведена подразделениям стратегического планирования, анализа и контроля центрального аппарата и департаментов полиции (на территориальном уровне – подразделениям анализа и контроля), которые обеспечивают общую координацию и мониторинг.

Однако на практике внедрение аналитических платформ и систем мониторинга сталкивается с проблемой низкой достоверности данных и исполнительской инерции. Существующий институт дисциплинарной ответственности, закреплённый в Законе «О правоохранительной службе»¹ и Правилах проведения внутреннего расследования², ориентирован на традиционную «бумажную» модель. Он не учитывает специфику правонарушений в цифровой среде, таких как намеренное искажение статистических показателей в информационных системах (далее – ИС), несвоевременное обновление баз данных или игнорирование автоматизированных уведомлений системы контроля.

Научная проблема заключается в наличии нормативного разрыва: при обязательности

¹ О правоохранительной службе: закон Республики Казахстан от 6 янв. 2011 г. № 380-IV (с изм. и доп. по сост. на 03.09.2026 г.) [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1100000380>.

² Об утверждении Правил проведения служебного расследования в органах внутренних дел Республики Казахстан: приказ Министра внутренних дел Республики Казахстан от 16 нояб. 2020 г. № 776 [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/V2000021648>.



использования цифровых инструментов в аналитических подразделениях ОВД отсутствует легальный механизм привлечения к ответственности за ненадлежащее исполнение «цифровых» обязанностей. Это порождает формализм в отчетности и снижает эффективность управленческих решений. Целью настоящей статьи является обоснование и разработка концепции «цифровой дисциплинарной ответственности» как необходимого элемента обеспечения достоверности управленческих данных и укрепления служебной дисциплины в условиях цифровой трансформации ОВД [1].

Научная новизна исследования заключается в том, что автором впервые сформулирована и теоретически обоснована концепция «цифровой дисциплинарной ответственности» применительно к ОВД в условиях действия Цифрового кодекса. В отличие от существующих общих подходов к цифровизации ведомственного контроля, в статье предложена авторская классификация «цифровых» проступков и разработана уникальная модель «Дисциплинарный ЕРАП» [2]. Данная модель переводит процесс фиксации нарушений и формирования материалов служебных расследований в автоматический режим на основе алгоритмов искусственного интеллекта и верификации «цифрового следа», что позволяет исключить субъективный фактор и минимизировать коррупционные риски.

Принципиальное отличие авторского подхода от известных механизмов контроля заключается в переводе технической фиксации действий в плоскость правовой квалификации. В рамках концепции техническая запись (системный лог) рассматривается не просто как элемент служебной информации, а как самостоятельное цифровое доказательство, напрямую интегрированное в процессуальный алгоритм дисциплинарного производства для оптимизации временных затрат.

В настоящей работе под «цифровым следом» понимаются технические записи (логи) о действиях сотрудника в корпоративных информационных системах, зафиксированные с применением средств криптографической защиты.

Материалы и методы. Методологическую основу исследования составил комплексный анализ нормативных правовых актов, регулирующих правоохранительную деятельность и процессы цифровизации в РК. Ключевыми источниками послужили Цифровой кодекс РК³, Закон «О правоохранительной службе»⁴, а также Правила проведения внутреннего расследования в ОВД РК⁵.

В работе применен междисциплинарный комплекс методов:

- формально-юридический метод: использован для анализа действующих норм и разработки авторских формулировок для дополнения ведомственных приказов [3];
- системно-структурный подход: позволил рассмотреть цифровую ответственность как элемент единой экосистемы управления аналитическими подразделениями ОВД [4];
- метод правового моделирования: применен при разработке алгоритма автоматизированного служебного расследования и создания шаблонов управленческих решений;
- сравнительный анализ: использован для сопоставления традиционных форм контроля и перспективных моделей цифрового аудита исполнительской дисциплины.

Эмпирическую базу составили результаты аудита текущих циклов планирования и анализ распорядительных документов подразделений стратегического планирования, анализа и контроля, выявивший системные риски «бумажной инерции» в цифровых системах.

³ Цифровой кодекс Республики Казахстан: от 9 янв. 2026 г. № 255-VIII [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/K2600000255>.

⁴ О правоохранительной службе: закон Республики Казахстан от 6 янв. 2011 г. № 380-IV (с изм. и доп. по сост. на 03.09.2026 г.) [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1100000380>.

⁵ Об утверждении Правил проведения служебного расследования в органах внутренних дел Республики Казахстан: приказ Министра внутренних дел Республики Казахстан от 16 нояб. 2020 г. № 776 [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/V2000021648>.



В частности, согласно обобщенным данным анализа правоприменительной практики в департаментах полиции за период 2024-2025 гг., установлено, что отсутствие единых ведомственных критериев оценки нарушений при работе в ИС приводит к региональным диспропорциям. Ввиду отсутствия четко регламентированных составов «цифровых» проступков тяжесть нарушения и мера взыскания оцениваются руководством сугубо субъективно. Это приводит к юридическому дисбалансу: за аналогичные дисциплинарные проступки в одном регионе на сотрудника налагается строгое дисциплинарное взыскание, тогда как в другом субъекте – выносится устное предупреждение, что прямо нарушает принцип единообразия правоприменения.

Результаты, обсуждение. В ходе исследования установлено, что ключевым барьером цифровой трансформации аналитических подразделений ОВД выступает институциональная неготовность традиционных дисциплинарных процедур к фиксации нарушений в виртуальной среде.

Зарубежные исследователи, в частности Дж. Чан (J. Chan), подчеркивают, что цифровая трансформация полиции – это не просто смена инструментов, а фундаментальное изменение «профессиональной игры» (field of policing), которое неизбежно меняет механизмы подотчетности и контроля внутри ведомств [5].

Практика деятельности аналитических подразделений ОВД наглядно иллюстрирует эту проблему двумя типичными кейсами.

Кейс 1 (искажение отчетности). При формировании сводного аналитического отчета за квартал автоматизированная система выявила расхождение данных. В ходе проверки выяснилось, что сотрудник территориального звена умышленно не вносил корректировки в ИС в течение 10 дней, чтобы искусственно удержать высокий рейтинг раскрываемости подразделения. Из-за отсутствия прямой нормы ответственности за «цифровое бездействие» сотрудник избежал дисциплинарного взыскания.

Кейс 2 (несвоевременное распределение документа руководством). В ведомственную систему электронного документооборота поступил контрольный документ со строгим сроком исполнения. Из-за несвоевременного рассмотрения и затягивания процесса наложения резолюции руководством исполнитель получил документ в свой «личный кабинет» уже с истекшим (или критически поджимающим) сроком исполнения. При автоматическом аудите система фиксирует просрочку со стороны исполнителя. Возникает правовая коллизия: традиционная служебная проверка по факту нарушения дедлайна возлагает вину на конечного исполнителя. Однако верификация «цифрового следа» движения документа по системе позволяет четко разграничить ответственность и доказать невиновность сотрудника, чьи права нарушены несвоевременными действиями руководства на этапе распределения задач.

Для решения этой проблемы автором предлагается внедрение системы цифровой дисциплинарной ответственности, базирующейся на трех ключевых компонентах:

1. Классификация «цифровых» проступков. Предлагается дополнить перечень дисциплинарных проступков, предусмотренных ведомственными нормативными актами и этическими нормами службы, следующими составами:

- умышленное сокрытие служебной информации: невыполнение обязательств по внесению сведений в ИС с целью искажения отчетности о результатах деятельности;
- внесение недостоверных данных: искажение сведений в ИС для искусственного формирования положительных показателей работы подразделения;
- несанкционированное использование средств аутентификации: выполнение операций в ИС с использованием чужих учетных данных или электронных подписей (далее – ЭЦП) [6].

2. Алгоритмизация и автоматизация внутренних расследований на основе анализа



действующих Правил проведения внутреннего расследования, предлагается внедрить в ведомственные системы штабов (ИС «Мониторинг» или аналоги) модуль автоматической фиксации нарушений.

Механизм: система в автоматическом режиме выявляет просрочку исполнения задачи или факт изменения данных после их утверждения.

Результат: программа автоматически формирует пакет документов – рапорт о выявлении нарушения, электронный шаблон объяснительной (направляемый в «личный кабинет» сотрудника) и проект приказа о назначении служебного расследования. Это сводит к минимуму субъективизм проверяющего и риск необоснованного освобождения от ответственности [1].

3. Правовое закрепление: проект дополнений в законодательство для легитимации данных процессов – предлагается внести изменения в ведомственные приказы МВД РК⁶, регламентирующие порядок проведения служебных расследований, закрепив:

- статус «автоматизированного отчета системы» как достаточного основания для начала служебного расследования;
- признание логов (журналов событий) ИС в качестве объективных доказательств вины или невиновности сотрудника.

Для минимизации правовых рисков при работе сотрудников ОВД в виртуальной среде критически важно создать детализированную нормативную базу. Исследователи А.А. Мукашева и Э.Ф. Нигматуллина справедливо подчеркивают, что именно отсутствие четкого правового регламента в цифровой среде может стать препятствием для реализации государственных функций в современных условиях [7].

4. Экономический эффект («Low-cost» модернизация) обоснован тем, что внедрение данных механизмов не требует приобретения дорогостоящего программного обеспечения. Речь идет о доработке существующего функционала действующих систем ОВД. Это позволит сократить расходы на выездные инспекционные проверки, так как «цифровой аудит» исполнительской дисциплины будет осуществляться дистанционно из центрального аппарата, департамента до районного звена [8].

Механизм работы ИИ в модели «Дисциплинарный ЕРАП»:

1. Автоматическая фиксация состава (Цифровой протокол): ИИ, интегрированный в рабочие системы (ЕРДР, ИС штаба, базы данных), в режиме реального времени мониторит выполнение регламентов. При выявлении очевидного нарушения (например, нарушение срока регистрации заявления или несанкционированное удаление данных) ИИ автоматически генерирует «Цифровой протокол дисциплинарного проступка».

Алгоритм разграничения умысла и технического сбоя строится по принципу сетевой кросс-верификации. ИИ анализирует три параметра: во-первых, общую телеметрию ИС (наличие массовых задержек пакетов или падения серверов в момент фиксации проступка); во-вторых, паттерны поведения пользователя (если сотрудник совершал другие операции в системе, значит, доступ к сети был стабилен); в-третьих, корреляцию действий (если данные не внесены в ИС, но параллельно была заполнена бумажная карточка, ИИ квалифицирует это как техническую адаптацию, а не саботаж). При обнаружении системной аномалии ИИ автоматически присваивает инциденту статус «Технический сбой» и блокирует формирование протокола до верификации администратором.

Аналогия с ЕРАП: как камера фиксирует превышение скорости, так и ИИ фиксирует отклонение от регламентных параметров (просрочку, изменение данных, несанкционированное

⁶ Об утверждении Правил проведения служебного расследования в органах внутренних дел Республики Казахстан: приказ Министра внутренних дел Республики Казахстан от 16 нояб. 2020 г. № 776 [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/V2000021648>.



действие), зафиксированное в журналах событий автоматизированной системы.

2. Безбумажное служебное расследование: на основе зафиксированного нарушения ИИ автоматически подтягивает из системы кадрового подразделения данные о личности сотрудника, его стаже и наличии действующих взысканий. Система сама формирует проект заключения служебного расследования. Сотруднику в личный кабинет (или на служебный планшет) приходит уведомление о зафиксированном проступке с предложением дать электронное объяснение в течение установленного срока.

3. Цифровое содействие в оценке материалов (рекомендательная модель ИИ): алгоритмы искусственного интеллекта полностью лишены права самостоятельного вынесения окончательного правового акта или автоматического назначения дисциплинарного взыскания. На основе верифицированного цифрового следа и предоставленного сотрудником электронного объяснения ИИ выполняет исключительно вспомогательную аналитическую функцию. Программа сопоставляет зафиксированный факт просрочки или искажения данных с санкциями ст. 56 Закона «О правоохранительной службе» и генерирует рекомендательный проект заключения. Окончательное решение, оценка вины сотрудника, изучение возможных технических сбоев и подписание мотивированного приказа о наложении взыскания остаются исключительным персональным полномочием уполномоченного должностного лица (руководителя ОВД).

Аналогия с ЕРАП: процесс становится «прозрачным», а удаление или изменение записи о проступке в системе становится технически невозможным, что минимизирует коррупционные риски.

4. Снижение административной нагрузки: Применение ИИ по данной модели позволяет перевести до 70% типовых дисциплинарных расследований в автоматический режим. Данный показатель обосновывается структурой ведомственных правонарушений, где до двух третей от общего массива составляют очевидные и технически фиксируемые проступки (нарушение установленных сроков регистрации, несвоевременное закрытие контрольных карточек, просрочка направления аналитических форм). Поскольку установление факта совершения данных проступков не требует проведения сложных оперативно-проверочных мероприятий, формирование материалов по ним может быть полностью делегировано алгоритмам ИИ. Это освобождает аналитические подразделения от рутины, позволяя им сосредоточиться на организационно-аналитической работе.

Использование систем ИИ в деятельности силовых структур сегодня становится не просто техническим новшеством, а стратегическим приоритетом. Как отмечает Г.А. Арғынғазин, ИИ выступает новым фактором конкурентоспособности современных государств. Использование интеллектуальных алгоритмов позволяет минимизировать коррупционные риски и субъективизм при оценке действий сотрудников [9].

Внедрение цифровой дисциплинарной ответственности вызывает необходимость дискуссии о балансе между автоматизированным контролем и соблюдением прав сотрудников правоохранительных органов [10]; [11].

Риск «технократического детерминизма» и технических сбоев. Одной из главных проблем автоматизации взысканий является риск наказания сотрудника за сбой, вызванные нестабильностью сетевой инфраструктуры или программными ошибками. В этой связи автор настаивает на принципе «human-in-the-loop» (человек в контуре): автоматизированная система лишь фиксирует аномалию и формирует первичные материалы, но окончательное решение о виновности должно приниматься должностным лицом после изучения всех обстоятельств. Необходимо юридически закрепить положение о том, что технический сбой ИС является безусловным основанием для освобождения от ответственности [12].

Гарантией защиты прав сотрудника при этом выступает трехуровневый правовой фильтр:



во-первых, презумпция технического сбоя при мотивированном заявлении исполнителя; во-вторых, обязательный 3-дневный срок для предоставления встречных электронных объяснений через личный кабинет [13]; в-третьих, исключительный правовой суверенитет руководителя ОВД при окончательном подписании акта наложения взыскания, согласно статье 57 Закона «О правоохранительной службе».

Преодоление «цифрового формализма». Существует риск, что сотрудники начнут работать «на показатели системы», игнорируя реальное качество оперативной работы. Цифровая ответственность должна наступать не за отсутствие «галочки» в системе, а за нарушение конкретных, измеримых и достижимых целей (SMART) [14].

Правовой статус цифровых доказательств. Традиционно в рамках служебных расследований ключевыми являются бумажные объяснительные. Переход к использованию логов системы и данных блокчейн-платформ (для фиксации истории изменений документов) требует пересмотра Правил проведения служебного расследования. Обсуждение данного вопроса подводит к выводу о необходимости легализации данных журналов регистрации (логов) автоматизированных систем в качестве полноценного доказательства по делам о дисциплинарных проступках [15].

Антикоррупционный потенциал. Важным аспектом дискуссии является снижение коррупционных рисков. Автоматизация процесса – от фиксации нарушения до формирования шаблона приказа – исключает возможность «выборочного» привлечения к ответственности со стороны руководства. Это создает прозрачную среду, где правила игры едины для центрального аппарата и районного отдела [16].

Заключение. Проведенное исследование позволяет сделать следующие выводы:

1. Необходимость правовой адаптации. Действующая нормативная база, включая Закон «О правоохранительной службе» и Правила проведения служебного расследования в ОВД, требует дополнения в части определения цифровых дисциплинарных проступков. Установлено, что без введения персональной ответственности за работу с данными цифровая трансформация аналитических подразделений будет носить формальный характер.

2. Внедрение института цифровой ответственности. Автором обоснована концепция «цифровой дисциплинарной ответственности», которая должна охватывать нарушения, связанные с искажением управленческой информации, несвоевременным наполнением ИС и несоблюдением регламентов работы в аналитических платформах. Это обеспечит достоверность данных, на основе которых Министерство внутренних дел РК принимает стратегические решения⁷.

3. Автоматизация процедур контроля. Предложенный алгоритм автоматизированного служебного расследования (на основе «цифрового следа» и готовых шаблонов) позволяет значительно дебюрократизировать процесс. Это исключает субъективизм при привлечении сотрудников к ответственности и обеспечивает прозрачность управленческой вертикали «центр – область – район» [17].

4. Практическая значимость. Реализация предложенных поправок в ведомственные приказы МВД РК позволит реализовать модель «электронного служебного расследования». Это приведет к существенной экономии рабочего времени и минимизации человеческого фактора в контрольно-надзорной деятельности аналитических подразделений⁸.

Таким образом, создание правового механизма цифровой ответственности является обязательным условием для полноценной реализации норм Цифрового кодекса РК в деятельности

⁷ От профилактики к цифровой трансформации: в МВД подведены итоги работы за 2025 год и определены приоритеты на предстоящий период [Электронный ресурс]. – Режим доступа: <https://www.gov.kz/memleket/entities/qriim/press/news/details/1139163?lang=ru>.

⁸ О мерах по реализации Послания Главы государства народу Казахстана от 8 сентября 2025 года «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию»: указ Президента Республики Казахстан от 13 окт. 2025 г. № 1042 [Электронный ресурс]. – Режим доступа: <https://adilet.zan.kz/rus/docs/U2500001042/history>.



органов внутренних дел. Совершенствование данного направления деятельности соответствует инициативе «Цифровой полицейский» для повышения прозрачности, эффективности и доверия в обществе⁹.

Исследование выполнено в рамках научно-исследовательской работы (НИР) на базе Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

Список использованной литературы:

1. Идришева, С.К. О Цифровом кодексе Казахстана: проблемы кодификации и систематизации / С.К. Идришева // Юридический вестник МНУ. – 2022. – № 3. – С. 72-87.
2. Ysmanova, A. Public perception of algorithmic policing in a non-democratic context: Kazakhstan's case / A. Ysmanova // Policing and Society. – 2025. – Vol. 35. – No. 4. – Pp. 382-398.
3. Babuta, A. Proactive Policing and Artificial Intelligence: The Role of Ethics and Law in Technological Change / A. Babuta, M. Oswald // British Journal of Criminology. – 2023. – Vol. 63, No. 2. – Pp. 450-467.
4. Ахметов, А.С. Цифровое право в правовой системе Казахстана: теоретико-правовые аспекты / А.С. Ахметов, Д. Мун // Вестник Института законодательства и правовой информации РК. – 2025. – № 4 (80). – С. 88-101.
5. Chan, J.B.L. The technological game: How information technology is transforming police practice / J.B.L. Chan // Criminal Justice: International Journal of Policy and Practice. – 2001. – Vol. 1, No. 2. – Pp. 139-159.
6. Беляева, Е.Г. Принципы дисциплинарной ответственности в органах внутренних дел в условиях цифровизации служебной среды / Е.Г. Беляева // Юридическая наука и практика. – 2024. – № 2. – С. 114-121.
7. Мукашева, А.А. Государственный механизм регулирования цифрового пространства / А.А. Мукашева, Э.Ф. Нигматуллина // Вестник Академии правоохранительных органов. – 2025. – № 38. – С. 45-56.
8. Бегалиев, Е.Н. Цифровизация судебной и правоохранительной деятельности в Республике Казахстан: состояние и перспективы развития / Е.Н. Бегалиев // Вестник Карагандинского университета. Серия: Право. – 2023. – № 4 (112). – С. 54-62.
9. Арғынғазин, Ғ.А. Искусственный интеллект как новый фактор конкурентоспособности современных государств / Ғ.А. Арғынғазин // Вестник Академии правоохранительных органов. – 2025. – № 37. – С. 14-25.
10. Duvanova, D. Algorithmic governance, data protection, and accountability mechanisms in modern law enforcement systems / D. Duvanova // Policing: An International Journal. – 2024. – Vol. 47, № 5. – Pp. 612-628.
11. Marciniak, M. Law Enforcement Professionals' Trust in Algorithms and Due Process Guarantees / M. Marciniak // SAGE Criminal Justice Review. – 2025. – Vol. 30, № 2. – Pp. 144-159.
12. Ferguson, A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement / A.G. Ferguson // NYU Press. – 2024. – 2nd Edition. – 296 p.
13. Кулик, А.А. Проблемы защиты персональных данных сотрудников силовых структур при автоматизированном камеральном контроле / А.А. Кулик // Право и кибербезопасность. – 2025. – № 3. – С. 88-96.
14. Oswald, M. Algorithmic risk assessment in law enforcement: Accountability, rights and the SMART framework / M. Oswald // Computer Law & Security Review. – 2024. – Vol. 52. – Pp. 105-121.
15. Расторопов, С.В. Цифровые доказательства в расследовании правонарушений: организационно-правовые аспекты / С.В. Расторопов // Вестник уголовного права. – 2025. – № 1. – С. 45-53.
16. Kaufmann, M. Algorithmic Governance in Policing: Between Efficiency and Democratic Accountability / M. Kaufmann, S. Egbert // Science, Technology, & Human Values. – 2025. – Vol. 50, No. 1. – Pp. 26-53.
17. Канатов, А.К. Мониторинг реализации цифровых технологий в правоохранительной и нормотворческой деятельности / А.К. Канатов // Вестник Института законодательства и правовой информации РК. – 2026. – № 1 (81). – С. 302-312.

References:

1. Idrisheva, S.K. O Cifrovom kodekse Kazahstana: problemy kodifikacii i sistematizacii / S.K. Idrisheva // Juridicheskij vestnik MNU. – 2022. – № 3. – S. 72-87
2. Ysmanova, A. Public perception of algorithmic policing in a non-democratic context: Kazakhstan's case / A. Ysmanova // Policing and Society. – 2025. – Vol. 35. – No. 4. – Pp. 382-398.

⁹ Kazakhstan's Digital Policeman: Pioneering the future of law enforcement // Computerworld / Network World. – December 2024 [Электронный ресурс]. – Режим доступа: <https://www.computerworld.com/article/3628334/kazakhstans-digital-policeman-pioneering-the-future-of-law-enforcement.html>.



3. Babuta, A. Proactive Policing and Artificial Intelligence: The Role of Ethics and Law in Technological Change / A. Babuta, M. Oswald // *British Journal of Criminology*. – 2023. – Vol. 63, No. 2. – Pp. 450-467.
4. Ahmetov, A.S. Cifrovoe pravo v pravovoj sisteme Kazahstana: teoretiko-pravovye aspekty / A.S. Ahmetov, D. Mun // *Vestnik Instituta zakonodatel'stva i pravovoj informacii RK*. – 2025. – № 4 (80). – S. 88-101.
5. Chan, J.B.L. The technological game: How information technology is transforming police practice / J.B.L. Chan // *Criminal Justice: International Journal of Policy and Practice*. – 2001. – Vol. 1, No. 2. – Pp. 139-159.
6. Beljaeva, E.G. Principy disciplinarnoj otvetstvennosti v organah vnutrennih del v uslovijah cifrovizacii sluzhebnoj sredy / E.G. Beljaeva // *Juridicheskaja nauka i praktika*. – 2024. – № 2. – S. 114-121.
7. Mukasheva, A.A. Gosudarstvennyj mehanizm regulirovaniya cifrovogo prostranstva / A.A. Mukasheva, Je.F. Nigmatullina // *Vestnik Akademii pravoohranitel'nyh organov*. – 2025. – № 38. – S. 45-56.
8. Begaliev, E.N. Cifrovizacija sudebnoj i pravoohranitel'noj dejatel'nosti v Respublike Kazahstan: sostojanie i perspektivy razvitija / E.N. Begaliev // *Vestnik Karagandinskogo universiteta. Serija: Pravo*. – 2023. – № 4 (112). – S. 54-62.
9. Arrynfazin, F.A. Iskustvennyj intellekt kak novyj faktor konkurentosposobnosti sovremennyh gosudarstv / F.A. Arrynfazin // *Vestnik Akademii pravoohranitel'nyh organov*. – 2025. – № 37. – S. 14-25.
10. Duvanova, D. Algorithmic governance, data protection, and accountability mechanisms in modern law enforcement systems / D. Duvanova // *Policing: An International Journal*. – 2024. – Vol. 47, № 5. – Pp. 612-628.
11. Marciniak, M. Law Enforcement Professionals' Trust in Algorithms and Due Process Guarantees / M. Marciniak // *SAGE Criminal Justice Review*. – 2025. – Vol. 30, № 2. – Pp. 144-159.
12. Ferguson, A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement / A.G. Ferguson // *NYU Press*. – 2024. – 2nd Edition. – 296 p.
13. Kulik, A.A. Problemy zashhity personal'nyh dannyh sotrudnikov silovyh struktur pri avtomatizirovannom kameral'nom kontrole / A.A. Kulik // *Pravo i kiberbezopasnost'*. – 2025. – № 3. – S. 88-96.
14. Oswald, M. Algorithmic risk assessment in law enforcement: Accountability, rights and the SMART framework / M. Oswald // *Computer Law & Security Review*. – 2024. – Vol. 52. – Pp. 105-121.
15. Rastoropov, S.V. Cifrovye dokazatel'stva v rassledovanii pravonarushenij: organizacionno-pravovye aspekty / S.V. Rastoropov // *Vestnik ugolovnogogo prava*. – 2025. – № 1. – S. 45-53.
16. Kaufmann, M. Algorithmic Governance in Policing: Between Efficiency and Democratic Accountability / M. Kaufmann, S. Egbert // *Science, Technology, & Human Values*. – 2025. – Vol. 50, No. 1. – Pp. 26-53.
17. Kanatov, A.K. Monitoring realizacii cifrovyyh tehnologij v pravoohranitel'noj i normotvorcheskoj dejatel'nosti / A.K. Kanatov // *Vestnik Instituta zakonodatel'stva i pravovoj informacii RK*. – 2026. – № 1 (81). – S. 302-312.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Жасұлан Кәкімұлы Кәкімов – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының магистранты, e-mail: jasulan_kjk_sjk@mail.ru, orcid.org/0009-0007-2178-6574.

Какимов Жасулан Какимович – магистрант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: jasulan_kjk_sjk@mail.ru, orcid.org/0009-0007-2178-6574.

Kakimov Zhasulan Kakimovich – Master's Student at the Law Enforcement Academy under the Procurator General's Office of the Republic of Kazakhstan, e-mail: jasulan_kjk_sjk@mail.ru, orcid.org/0009-0007-2178-6574.