

БЕРЕЗЕНКО Елена Валерьевна,
преподаватель СПО Новочеркасского политехнического колледжа
Южно-Российского государственного политехнического
университета (НПИ) имени М.И. Платова,
e-mail: yelena.archakova.84195@mail.ru.

КУЗНЕЦОВ Александр Владимирович,
преподаватель кафедры специальных дисциплин
Крымского филиала Краснодарского университета МВД России,
майор полиции,
e-mail: v.shanko@mail.ru.

ЧИЖОВ Илья Александрович,
к.ю.н., доцент кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел (ИКТД ОВД)
Белгородский юридический институт МВД России имени И.Д. Путилина,
e-mail: v.shanko@mail.ru.

ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ

Аннотация. В статье рассматриваются основные правовые риски, возникающие в процессе использования цифровых технологий в деятельности полиции. Обосновывается, что цифровизация правоохранительной деятельности, способствуя повышению оперативности, управляемости и доказательственной обеспеченности полицейской работы, одновременно создает комплекс новых юридических проблем, связанных с защитой прав и свобод человека, обработкой персональных данных, пределами полицейского усмотрения, использованием алгоритмических решений и обеспечением информационной безопасности. Анализируются действующие нормативные правовые акты, регулирующие деятельность полиции, обращение с информацией и персональными данными, а также современные научные подходы к оценке цифровой трансформации органов внутренних дел. Делается вывод о том, что минимизация правовых рисков цифровизации полиции требует не только технического обновления, но и последовательного совершенствования законодательства, ведомственных регламентов, механизмов контроля и профессиональной подготовки сотрудников.

Ключевые слова: полиция, цифровые технологии, цифровизация правоохранительной деятельности, правовые риски, персональные данные, информационная безопасность, полицейское усмотрение, административно-правовое регулирование, цифровая трансформация, органы внутренних дел.

BEREZENKO Elena Valeryevna,
Lecturer in the Secondary Vocational Education Department
at the Novocherkassk Polytechnic College of the South-Russian State
Polytechnical University (NPI) named after M.I. Platov

KUZNETSOV Aleksandr Vladimirovich,
Lecturer in the Department of Specialized Disciplines

at the Crimean Branch of the Krasnodar University
of the Ministry of Internal Affairs of Russia, Police Major

CHIZHOV Ilya Aleksandrovich,
PhD in Law, Associate Professor in the Department of Information and
Computer Technologies in the Activities of Internal Affairs Bodies (ICTD OVD),
Belgorod Law Institute of the Ministry of Internal Affairs
of Russia named after I.D. Putilin

LEGAL RISKS OF USING DIGITAL TECHNOLOGIES IN POLICE ACTIVITIES

Annotation. *This article examines the main legal risks arising from the use of digital technologies in police work. It is argued that the digitalization of law enforcement, while promoting greater efficiency, manageability, and evidentiary support for police work, simultaneously creates a complex set of new legal challenges related to the protection of human rights and freedoms, the processing of personal data, the limits of police discretion, the use of algorithmic solutions, and information security. It analyzes current regulations governing police activities, the handling of information and personal data, as well as modern scientific approaches to assessing the digital transformation of internal affairs agencies. It concludes that minimizing the legal risks of police digitalization requires not only technical updating but also consistent improvements to legislation, departmental regulations, control mechanisms, and the professional training of officers.*

Key words: *police, digital technologies, digitalization of law enforcement, legal risks, personal data, information security, police discretion, administrative and legal regulation, digital transformation, internal affairs agencies.*

Современное развитие правоохранительной деятельности все в большей степени связано с внедрением цифровых технологий в практику органов внутренних дел, поскольку электронный документооборот, цифровые базы данных, системы видеонаблюдения, аналитические платформы, средства автоматизированной обработки информации, элементы искусственного интеллекта и иные технологические решения позволяют полиции быстрее получать, сопоставлять и использовать сведения, имеющие значение для охраны общественного порядка, предупреждения правонарушений и раскрытия преступлений.

Термин «цифровая трансформация» в последнее десятилетие стал символом прогресса в экономике, государственном управлении, социальной сфере и знаменует собой новый, возможно, завершающий этап построения «информационного общества» в масштабах современной цивилизации. Указом Президента Российской Федерации от 21 июля 2020 г. № 4741 ЦТ определена в качестве одной из пяти национальных целей развития нашей страны на период до 2030 г. При этом процесс цифровой трансформации в сфере государственного управления определен как «совокупность действий, осуществляемых государственным органом, направленных на изменение (трансформацию) государственного управления и деятельности государственного органа по предоставлению им государственных услуг и исполнению государственных функций за счет использования данных в электронном виде и внедрения информационных технологий в свою деятельность», в целях, указанных в п. 16 Положения о ведомственных программах цифровой трансформации: повышение удовлетворенности граждан государственными услугами, снижение издержек бизнеса при взаимодействии с государством; снижение издержек государственного

управления, экономики, социальной сферы; надежность и безопасность ИКТ; устранение избыточной контрольной (надзорной) деятельности в отношении предпринимательства [7].

Отметим, что система МВД России является наиболее многочисленным и многофункциональным правоохранительным органом государства и цифровизация полицейской деятельности не может рассматриваться исключительно как техническое усовершенствование, поскольку она затрагивает сферу конституционных прав личности, пределы государственного вмешательства, режим обращения с информацией и распределение юридической ответственности за принимаемые решения. В этой связи проблема правовых рисков использования цифровых технологий в деятельности полиции приобретает не только прикладное, но и принципиальное административно-правовое значение и, как справедливо отмечается в литературе, современные проблемы правоприменения требуют обращения не только к нормативному материалу, но и к понятийным и методологическим основаниям правопонимания, поскольку именно от них зависит определение пределов допустимого государственного вмешательства, юридической оценки цифровых решений и соотношения законности с технологической эффективностью [13]. В то же время Федеральный закон «О полиции», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О персональных данных» и стратегические акты о развитии информационного общества образуют базовую нормативную рамку такой цифровизации.

Правовые риски цифровизации полиции обусловлены прежде всего тем, что расширение технологических возможностей государства объективно усиливает интенсивность воздействия на сферу частной жизни граждан. Цифровые

средства обеспечивают более широкий сбор, хранение, передачу и анализ сведений о поведении людей, их перемещениях, коммуникациях и взаимодействиях с органами публичной власти. При этом сама по себе технологическая эффективность еще не означает правомерности соответствующих действий. Напротив, чем выше возможности полиции по обработке информации, тем более определенными должны быть правовые основания ее получения, использования, хранения и удаления. Законодательство об информации и о персональных данных ориентировано на защиту прав и свобод человека при обращении с информацией и обработке персональных данных, что требует от полиции постоянного соблюдения принципов законности, целевого характера обработки сведений, соразмерности вмешательства и недопустимости избыточного цифрового контроля [3; 4]. Официальные тексты 149-ФЗ и 152-ФЗ прямо закрепляют регулирование отношений в сфере информации и защиту прав человека при обработке персональных данных.

Одним из наиболее существенных правовых рисков выступает недостаточная определенность нормативной регламентации отдельных цифровых процедур в деятельности полиции. Общие законодательные основы цифрового обращения с информацией закреплены на федеральном уровне, однако значительная часть конкретных вопросов — порядок использования цифровых материалов, пределы доступа к ним, сроки хранения, условия межведомственного обмена, правила применения аналитических систем и степень допустимости алгоритмических рекомендаций — нередко остается на уровне ведомственных регламентов либо складывающейся практики. Такая ситуация создает риск неодинакового правоприменения, поскольку один и тот же цифровой инструмент может использоваться различными подразделениями при неодинаковом понимании его юридической природы и процессуального значения. В научной литературе справедливо отмечается, что цифровая трансформация органов внутренних дел должна сопровождаться не только внедрением новых технологий, но и развитием нормативной среды, способной обеспечить единообразие и правовую определенность служебной деятельности [7, с.9; 10].

Не менее значимым риском является нарушение прав граждан в сфере персональных данных и частной жизни. Для полиции цифровые технологии открывают возможность оперативного доступа к большим массивам сведений, однако такое расширение информационных ресурсов неизбежно порождает угрозу чрезмерного накопления данных, выхода за пределы заявленных

целей их обработки и недостаточной защищенности цифровой инфраструктуры. Особенно чувствительными являются ситуации, связанные с видеофиксацией, использованием биометрических характеристик, аналитикой массивов данных, а также последующим хранением и воспроизведением собранной информации. В этих условиях особое значение имеет соблюдение баланса между публичным интересом в обеспечении безопасности и конституционными гарантиями личности. Любое технологическое решение, применяемое полицией, должно оцениваться через призму его необходимости, законности, соразмерности и возможности последующего контроля [10]. Именно поэтому правовые риски цифровизации нельзя сводить к техническим сбоям или организационным просчетам: по существу речь идет о рисках чрезмерного ограничения прав человека в цифровой среде.

Самостоятельное значение имеет риск подмены правовой оценки автоматизированным или алгоритмическим решением. Развитие цифровой аналитики, автоматического ранжирования событий, интеллектуального поиска и прогнозных моделей объективно повышает управленческие возможности полиции, однако одновременно ставит вопрос о пределах допустимого использования таких технологий. Алгоритм способен выявлять корреляции, предлагать зоны повышенного риска или фиксировать аномальное поведение, но он не должен подменять полицейское усмотрение и юридическую квалификацию конкретной ситуации. Ответственность за применение мер административного принуждения, принятие процессуальных решений и оценку доказательственной значимости цифровых материалов должна сохраняться за должностным лицом. В противном случае возникает риск размывания персональной ответственности, формализации правоприменения и переноса фактической власти на техническую систему, не обладающую ни юридическим статусом, ни способностью учитывать весь контекст конкретного события [8; 12]. Современная научная литература о цифровой трансформации и полицейском усмотрении также исходит из необходимости сохранять за человеком окончательное юридически значимое решение.

Серьезную угрозу представляет и риск снижения доказательственной надежности цифровых материалов при недостаточно урегулированном порядке их использования. Цифровые записи, электронные следы, данные аналитических систем и результаты автоматизированной обработки информации все чаще используются в административной и правоохранительной практике. Однако для их полноценного и законного

применения необходимо четко понимать условия происхождения таких сведений, порядок их фиксации, возможность проверки достоверности, а также наличие гарантий от последующего изменения, утраты или несанкционированного доступа. Если цифровой материал используется без понятной процедуры верификации и без надлежащего документального сопровождения, возрастает риск процессуальных ошибок, последующего оспаривания законности действий полиции и утраты доверия к самой цифровой системе [6; 8]. В данном аспекте правовой риск проявляется в том, что технологическая новизна способна опередить правовую готовность системы к ее корректному использованию.

Отдельную группу составляют риски информационной безопасности и служебной устойчивости цифровой инфраструктуры полиции. Чем больше процессов переводится в электронную форму, тем выше значение надежности каналов связи, защищенности ведомственных информационных систем, контроля доступа и предотвращения утечек служебно значимой информации. Для полиции подобные риски имеют двойную природу. С одной стороны, уязвимость цифровой инфраструктуры создает угрозу нарушения прав граждан вследствие компрометации их данных; с другой — она способна негативно влиять на эффективность охраны общественного порядка, оперативность реагирования и устойчивость повседневной служебной деятельности. Следовательно, информационная безопасность в сфере полицейской цифровизации должна рассматриваться не как сугубо техническая категория, а как важнейший элемент правового режима использования цифровых технологий [3; 5]. Стратегия развития информационного общества и действующее информационное законодательство также связывают цифровое развитие с требованиями безопасности и правовой защищенности информационной среды.

Преодоление указанных рисков возможно только при комплексном подходе. Во-первых, требуется дальнейшая детализация нормативной базы, регулирующей использование цифровых средств в деятельности полиции, включая правила обращения с цифровыми материалами, пределы алгоритмической аналитики, условия межведомственного информационного обмена и стандарты юридически значимой фиксации действий сотрудников. Во-вторых, необходимо закрепить принцип обязательного человеческого контроля при использовании любых аналитических и прогнозных систем: цифровой инструмент может содействовать принятию решения, но не подменять собой правовую оценку и ответственность должностного лица. В-третьих, следует

усиливать внутренний и внешний контроль за обращением с персональными данными, а также развивать профессиональную подготовку сотрудников полиции, формируя у них не только технические навыки, но и устойчивое понимание правовых границ цифрового вмешательства [2; 4]. Такой подход позволяет рассматривать цифровизацию не как самодостаточную цель, а как правовой и организационный процесс, допустимый лишь при условии сохранения баланса между эффективностью полицейской деятельности и гарантиями прав личности.

Таким образом, использование цифровых технологий в деятельности полиции представляет собой объективное и во многом неизбежное направление развития современной правоохранительной системы. Однако вместе с ростом технологических возможностей возрастает и объем правовых рисков, связанных с обработкой персональных данных, алгоритмизацией полицейского усмотрения, недостаточной определенностью нормативных процедур, доказательственным статусом цифровых материалов и уязвимостью информационной инфраструктуры. Следовательно, цифровая трансформация полиции должна сопровождаться последовательным совершенствованием законодательства, развитием ведомственных регламентов, усилением режимов контроля и подготовкой сотрудников к правомерной работе в цифровой среде. Только при таком подходе возможно обеспечить, чтобы цифровые технологии усиливали законность и результативность полицейской деятельности, а не становились источником новых нарушений прав и свобод граждан.

Список литературы:

- [1] Кодекс Российской Федерации об административных правонарушениях: федер. закон от 30.12.2001 № 195-ФЗ (ред. от 23.03.2026) // Официальный интернет-портал правовой информации. Дата обращения: 03.04.2026.
- [2] О полиции: федер. закон от 07.02.2011 № 3-ФЗ // Собрание законодательства Российской Федерации. 2011. № 7, ст. 900.
- [3] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // Официальный интернет-портал правовой информации. Дата обращения: 03.04.2026.
- [4] О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ // Официальный интернет-портал правовой информации. Дата обращения: 03.04.2026.
- [5] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Российской Федерации от

09.05.2017 № 203 // Официальный интернет-портал правовой информации. Дата обращения: 03.04.2026.

[6] Об утверждении Наставления об организации служебной деятельности строевых подразделений патрульно-постовой службы полиции территориальных органов МВД России : приказ МВД России от 28.06.2021 № 495 // Официальный интернет-портал правовой информации. Дата обращения: 03.04.2026.

[7] Лукашов, Н. В. Теоретические и организационные основы цифровой трансформации территориальных органов внутренних дел системы МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 128–130.

[8] Власов, К. А. Проблемы применения мер непосредственного принуждения сотрудниками полиции и пути их решения // Право и государство: теория и практика. 2023. № 10 (226).

[9] Агакишиев, С. А. О., Комахин, Б. Н. Вопросы обеспечения общественной безопасности: от устава к новому наставлению // Юристъ-Правоведъ. 2022. № 1 (100).

[10] Кодзоков, Б. В. Организационно-правовые особенности деятельности патрульно-постовой службы полиции // Пробелы в российском законодательстве. 2023. № 4.

[11] Дежурный, А. А., Бондаренко, Д. М. Роль патрульно-постовой службы полиции в обеспечении общественной безопасности и правопорядка в Российской Федерации // Право и государство: теория и практика. 2025. № 4.

[12] Костин, С. Г. Полицейское усмотрение в условиях цифровой трансформации государственного управления // ВБ: Административное право и практика администрирования. 2025. № 1.

[13] Шанько, В. В. Понятийные и методологические подходы к проблемам современного правопонимания / В. В. Шанько, Е. Г. Светличный // Философия права. – 2021. – № 3(98). – С. 64–67.

References:

[1] Code of Administrative Offences of the Russian Federation: feder. Law No. 30.12.2001 of 195-FZ (as amended by 23.03.2026) //Official Internet Portal of Legal Information. Accessed 03.04.2026.

[2] On the police: feder. Law No. 07.02.2011 dated 3-FZ//Collection of Legislation of the Russian Federation. 2011. No. 7, Art. 900.

[3] About Information, Information Technology, and Information Security: Feder. Law No. 27.07.2006 of 149-FZ//Official Internet Portal of Legal Information. Accessed 03.04.2026.

[4] About personal data: feder. Law No. 27.07.2006 of 152-FZ//Official Internet Portal of Legal Information. Accessed 03.04.2026.

[5] On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030: Decree of the President of the Russian Federation of 09.05.2017 No. 203//Official Internet portal of legal information. Accessed 03.04.2026.

[6] On approval of the Instruction on the organization of service activities of combat units of the patrol and guard service of the police of the territorial bodies of the Ministry of Internal Affairs of Russia: order of the Ministry of Internal Affairs of Russia dated 28.06.2021 No. 495//Official Internet portal of legal information. Accessed 03.04.2026.

[7] Lukashov, N.V. Theoretical and organizational foundations of the digital transformation of the territorial bodies of internal affairs of the system of the Ministry of Internal Affairs of Russia//Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2023. № 3 (67). S. 128–130.

[8] Vlasov, K. A. Problems of the use of direct coercion by police officers and ways to solve them// Law and state: theory and practice. 2023. № 10 (226).

[9] Agakishiev, S. A. O., Komakhin, B. N. Issues of ensuring public safety: from the charter to a new instruction//Lawyer-Pravoveda. 2022. № 1 (100).

[10] Kodzokov, B.V. Organizational and legal features of the activities of the police patrol service// Gaps in Russian legislation. 2023. № 4.

[11] Duty officer, A. A., Bondarenko, D. M. The role of the police patrol service in ensuring public safety and law and order in the Russian Federation// Law and state: theory and practice. 2025. № 4.

[12] Kostin, S. G. Police discretion in the context of digital transformation of public administration//NB: Administrative law and administration practice. 2025. № 1.

[13] Shanko, V.V. Conceptual and methodological approaches to the problems of modern legal understanding/V.V. Shanko, E.G. Svetlichny//Philosophy of Law. – 2021. – № 3(98). – S. 64–67.

