Дата поступления рукописи в редакцию: 11.06.2026 г. DOI: 10.24412/2782-3830-2026-7-363-368
Дата принятия рукописи в печать: 13.07.2026 г.

ЦАРЬКОВА Евгения Геннадьевна,
кандидат физико-математических наук,
ведущий научный сотрудник
ФКУ НИИ ФСИН России,
0000-0002-5610-9895,
e-mail: university69@mail.ru

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ФСИН РОССИИ

Аннотация. *Статья посвящена актуальным правовым вопросам применения искусственного интеллекта в служебной деятельности сотрудников ФСИН России. Обращение к данной теме обусловлено развитием цифровых технологий в государственном управлении, расширением практик алгоритмизации служебных процессов и возрастанием требований к правовому обеспечению таких решений. Использование искусственного интеллекта в деятельности уголовно-исполнительной системы Российской Федерации (УИС) рассматривается как перспективное направление совершенствования служебной деятельности, повышения эффективности управления и развития современных механизмов информационного обеспечения. Вместе с тем, цифровая трансформация данной сферы актуализирует вопросы о пределах допустимости применения интеллектуальных систем, о необходимости соблюдения прав человека, а также о выработке специальных правовых ориентиров для их внедрения и использования. В работе предложен подход, основанный на рассмотрении искусственного интеллекта не только как технологического инструмента, но и как объекта правового регулирования, способного оказывать влияние на содержание служебных решений и практику их принятия. Особое внимание уделяется необходимости формирования системы правовых принципов, которая позволила бы согласовать задачи цифрового развития ФСИН России с требованиями законности, обоснованности, контролируемости и защиты прав лиц, вовлеченных в уголовно-исполнительные отношения. Обосновывается, что дальнейшее развитие технологий искусственного интеллекта в данной сфере требует не фрагментарных решений, а целостной правовой модели, учитывающей отраслевую специфику, характер служебной деятельности и риски алгоритмического вмешательства. Перспективность рассматриваемых вопросов связана с тем, что применение интеллектуальных систем в уголовно-исполнительной сфере выходит за рамки исключительно технической модернизации и затрагивает фундаментальные вопросы соотношения цифровых средств управления, публичной власти и правового статуса личности. Использование алгоритмических решений в служебной деятельности сотрудников ФСИН России требует учета не только функциональной полезности методов искусственного интеллекта, но и правовых последствий, возникающих при обработке информации, формировании рекомендаций и использовании результатов автоматизированного анализа в практической деятельности. Поскольку правовое осмысление искусственного интеллекта в пенитенциарной сфере, во-многом, развивается опережающими темпами по отношению к практике его внедрения, требуется дальнейшая разработка категориального аппарата, уточнение отраслевых принципов, определение правовых ограничений и выработка единых подходов к оценке допустимости использования интеллектуальных технологий в служебной деятельности сотрудников ФСИН России. Предлагаемый в работе подход ориентирован на формирование теоретической основы, которая может быть использована в дальнейших научных исследованиях в сфере развития специального нормативного регулирования.*

Ключевые слова*: искусственный интеллект, уголовно-исполнительная система Российской Федерации, служебная деятельность, правовые принципы, алгоритмическая прозрачность, видеоаналитика, персональные данные, нейросетевые алгоритмы, экспертные системы, правовая информатика, цифровая трансформация.*

TSARKOVA Evgeniya Gennadievna,
Candidate of Physico-mathematical Sciences,
Senior Researcher of the Research Institute
of the Federal Penitentiary Service of Russia

LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE OFFICIAL DUTIES OF EMPLOYEES OF THE FEDERAL PENITENTIARY SERVICE OF RUSSIA

Annotation. *The article is devoted to current legal issues concerning the use of artificial intelligence in the official duties of employees of the Federal Penitentiary Service of Russia. The consideration of this topic is driven by the development of digital technologies in public administration, the expansion of practices in the algorithmization of official processes, and the increasing demands for legal support of such solutions. The use of artificial intelligence in the activities of the Russian penal enforcement system is viewed as a promising direction for improving official duties, enhancing management efficiency, and developing modern mechanisms for information support. At the same time, the digital transformation of this area raises the question of the permissible limits for the use of intelligent systems, the need to respect human rights, and the development of specific legal guidelines for their implementation and use. The paper proposes an approach based on considering artificial intelligence not only as a technological tool but also as an object of legal regulation capable of influencing the content of official decisions and the practices by which they are made. Particular attention is paid to the need to form a system of legal principles that would align the digital development objectives of the Federal Penitentiary Service of Russia with the requirements of legality, reasonableness, controllability, and the protection of the rights of persons involved in penal legal relations. It is argued that further development of artificial intelligence technologies in this area requires not fragmentary solutions, but a comprehensive legal model that accounts for sectoral specificities, the nature of official duties, and the risks of algorithmic intervention. The promise of the issues under consideration is related to the fact that the use of intelligent systems in the penal sphere goes beyond purely technical modernization and touches on fundamental questions regarding the relationship between digital management tools, public authority, and the legal status of the individual. The use of algorithmic solutions in the official duties of employees of the Federal Penitentiary Service of Russia requires consideration not only of the functional utility of artificial intelligence methods but also of the legal consequences arising from the processing of information, the formation of recommendations, and the use of automated analysis results in practical activities. Since the legal understanding of artificial intelligence in the penitentiary sphere is, in many respects, developing at a faster pace relative to the practice of its implementation, further development of the conceptual apparatus, clarification of sectoral principles, definition of legal restrictions, and the formulation of unified approaches to assessing the permissibility of using intelligent technologies in the official duties of employees of the Federal Penitentiary Service of Russia are required. The proposed approach is aimed at forming a theoretical foundation that can be used in further scientific research on the development of special regulatory frameworks.*

Key words: *artificial intelligence, Penal System of the Russian Federation, official duties, legal principles, algorithmic transparency, video analytics, personal data, neural network algorithms, expert systems, legal informatics, digital transformation.*

Введение

Цифровая трансформация уголовно-исполнительной системы Российской Федерации (УИС) в настоящее время постепенно переходит с уровня ведомственных дискуссий на уровень официального государственного планирования [1, С.63]. Концепцией развития уголовно-исполнительной системы Российской Федерации на период до 2030 года в качестве основных направлений развития УИС отмечаются проведение цифровой трансформации и научно-техническое развитие, создание и внедрение единой информационной системы ФСИН России, развитие систем сбора и обработки данных, принятие решений на основе результатов применения искусственного интеллекта, создание единого защищенного управляемого информационного пространства, а также использование видеоаналитики и прогнозирования поведения осужденных и сотрудников. Такая нормативная постановка вопроса меняет предмет научного анализа. Речь идет уже не о возможности гипотетического применения технологий искусственного интеллекта (ИИ) в пенитенциарной сфере, а о правовых

условиях допустимости их использования в текущей и перспективной служебной деятельности сотрудников ФСИН России. ИИ в данном случае выступает не как внешнее технологическое дополнение, а как потенциальный элемент управленческой инфраструктуры, влияющий на сбор, обработку, интерпретацию и использование информации в сфере охраны, надзора, обеспечения режима, медицинского сопровождения, организационного взаимодействия и кадровой подготовки [2, С.113]. Государственный курс на развитие таких технологий закреплен и в более широком нормативном контексте. Так, Указом Президента Российской Федерации от 10 октября 2019 г. № 490 утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года, направленная на ускоренное развитие искусственного интеллекта, проведение научных исследований, повышение доступности информации и вычислительных ресурсов, а также совершенствование системы подготовки кадров. Для УИС этот курс приобретает особое значение, поскольку пенитенциарное ведомство сочетает в своей деятельности властные полномочия, работу с ограничением свободы человека и обращение с информацией ограниченного доступа [3, С.330].

Материалы и методы

Юридическая специфика пенитенциарной сферы во-многом состоит в том, что любое цифровое средство здесь соприкасается с правовым статусом личности. В учреждениях УИС объектами обработки становятся сведения о подозреваемых, обвиняемых, осужденных, сотрудниках, режимной обстановке, медицинском обеспечении, перемещениях, коммуникациях и соблюдении установленных ограничений [4, С.198]. Поэтому алгоритмическая система в служебной деятельности сотрудников ФСИН России не может оцениваться исключительно по техническим критериям производительности, скорости или удобства использования. Для нее принципиальны правовые параметры: допустимость исходных данных, цель обработки, пределы использования результата, возможность проверки ошибки, соразмерность вмешательств [5, С.154]. Важно рассматривать правовые аспекты применения ИИ в служебной деятельности сотрудников ФСИН не в абстрактной форме, а через конкретные управленческие и режимные функции [6, С.241].

В наиболее общем виде такие функции можно разделить на четыре блока [7, С.53]. Первый блок образуют системы наблюдения и видеоаналитики, используемые для обеспечения безопасности, фиксации событий и реагирования на отклонения от режима. Второй блок составляют системы учета, маршрутизации и аналитической обработки данных о лицах и событиях внутри УИС. Третий блок связан с интеллектуальными справочными, экспертными и образовательными системами, которые могут использоваться для подготовки сотрудников, правовой навигации и поддержки принятия управленческих решений. Четвертый блок образуют прогнозные и классификационные алгоритмы, которые потенциально способны влиять на оценку рисков, распределение внимания персонала и выбор дальнейших мер реагирования.

Данный блок порождает наибольшее количество правовых вопросов [8, С.47]. Если технология ограничивается передачей сигнала о событии, например, о появлении постороннего объекта или нарушении заданной границы охраняемой территории, она остается в пределах технического сопровождения режима. Когда система начинает строить прогноз поведения, классифицировать уровень риска, формировать цифровой профиль или предлагать управленческое решение, возникает качественно иной режим правовой оценки. В этом случае алгоритм уже влияет не только на информационную обстановку, но и на структуру служебного усмотрения сотрудника [9, С.135]. Указанная проблема усугубляется тем, что в действующем нормативном массиве стратегические ориентиры цифрового развития сформулированы значительно полнее, чем специальные правовые принципы применения ИИ в служебной деятельности органов правопорядка [10, С.261]. В открытых нормативных актах не представлена завершенная специальная модель, которая бы детально разграничивала допустимые и недопустимые сценарии использования интеллектуальных систем именно в служебной деятельности сотрудников УИС.

Отсюда вытекает первая методологическая позиция настоящего исследования. По мнению автора, правовое регулирование ИИ в деятельности сотрудников ФСИН России должно строиться не вокруг абстрактного понятия «внедрение технологии», а вокруг юридически значимого служебного действия. Для правовой оценки важна не сама архитектура системы, а вопрос о том, какое служебное последствие она способна породить. Одна и та же технологическая платформа может использоваться либо как вспомогательный инструмент обработки информации, либо как механизм, фактически влияющий на решения о безопасности, режиме, контроле поведения, дисциплинарной реакции или организационной оценке деятельности персонала.

Из этого следует, что правовая модель применения искусственного интеллекта в служебной деятельности сотрудников ФСИН России должна быть многоуровневой. Первый уровень — уровень данных. Здесь определяется, какие катего-

рии сведений допускаются к алгоритмической обработке, какова цель их использования, соответствует ли объем данных заявленной задаче и допускает ли правовой режим их обработку в конкретной цифровой системе. Следующий уровень — уровень алгоритма. На этой стадии оцениваются интерпретируемость модели, устойчивость результата, наличие ограничений на использование прогноза и способность системы работать в контролируемом правовом режиме, а не только в технически эффективном. Третий уровень — уровень служебного решения. Здесь решается вопрос о том, какое значение может иметь результат алгоритма для конкретного сотрудника: информационное, рекомендательное или фактически определяющее. Четвертый уровень — уровень последующего юридического контроля, где подлежат проверке обоснованность применения системы, корректность исходных данных, допустимость служебной реакции и возможность пересмотра спорного решения.

Результаты и обсуждение

Учет отмеченных выше факторов позволяет сформулировать систему специальных правовых принципов применения искусственного интеллекта в деятельности сотрудников ФСИН России.

Первый принцип состоит в нормативной определенности функции. Каждая применяемая ведомственная ИИ-система должна иметь ясно установленное служебное назначение, а не использоваться «по аналогии» для новых задач без отдельной правовой оценки. Следующий принцип — алгоритмическая интерпретируемость. Важно, чтобы сотрудник, использующий результат системы, понимал не внутреннюю программную математику в полном объеме, а юридически значимые основания применения результата: источник данных, тип события, смысл сигнала, пределы надежности и допустимые варианты реакции. Третий принцип заключается в запрете скрытого нормообразования [11, С.108]. Алгоритм не может превращать накопленные массивы прошлых решений или наблюдений в квазинормативный стандарт, который затем начинает действовать как самостоятельное правило поведения внутри учреждения. Далее, принцип, предусматривающий обязательный человеческий контроль. Формула о сохранении «человека в контуре управления» в пенитенциарной сфере не должна пониматься формально. Необходимо, чтобы сотрудник проверял основания применения алгоритмического результата, соотносил его с фактической ситуацией и принимал самостоятельное решение в пределах компетенции. Пятым принципом вводится разделение статуса данных и статуса вывода. Первичная информация и алгоритмический прогноз не тождественны. Документированный факт, видеозапись, медицинское заключение и машинно построенный рейтинг риска имеют различную правовую природу и не могут пользоваться одинаковым уровнем доверия. Шестой принцип — минимизация вмешательства. Если служебная задача может быть решена менее инвазивным цифровым средством, без формирования устойчивого профиля личности или без расширенного сбора персонализированных сведений, именно такой вариант должен считаться приоритетным. Далее, принцип усиленной защиты уязвимого адресата. Лицо, находящееся в местах лишения свободы или под стражей, изначально ограничено в свободе действий, доступе к коммуникациям и возможностях защиты своих интересов. Это повышает требования к правовой осторожности при использовании алгоритмов, способных влиять на условия содержания, режим контроля, интенсивность наблюдения или организацию обращения с человеком. И, наконец, восьмой принцип вводит двухконтурный аудит. Любая система, применяемая в деятельности ФСИН России, должна быть подотчетна не только в момент внедрения, но и на стадии последующей эксплуатации. Ошибки, ложные срабатывания, спорные сигналы и последствия использования системы должны становиться предметом постоянной ведомственной и правовой проверки.

Отдельного внимания заслуживает связь цифровизации и кадровой политики. В Концепции развития УИС на период до 2030 года отмечается необходимость повышения эффективности служебной деятельности и формирования профессионального кадрового потенциала. Национальная стратегия развития искусственного интеллекта также включает совершенствование системы подготовки кадров. Поэтому правовое регулирование ИИ в уголовно-исполнительной системе Российской Федерации не может ограничиваться вопросами эксплуатации оборудования и программного обеспечения. Оно должно включать обязательную подготовку сотрудников к работе с интеллектуальными системами, обучение правовым ограничениям алгоритмического анализа, формирование навыков интерпретации цифровых сигналов и понимания различия между технической рекомендацией и юридически значимым решением.

Практическая потребность в такой подготовке подтверждается самим характером информационного обеспечения ФСИН России, поскольку современная ведомственная цифровая среда многослойна. В ней сосуществуют инфраструктурные, аналитические, режимные, организационные и образовательные решения.

Чем сложнее становится эта среда, тем опаснее полагаться лишь на общее ведомственное усмотрение без специальной правовой модели.

В научном отношении проблема выходит за пределы ведомственного администрирования, затрагивая соотношение информационного права, уголовно-исполнительного права, административного права и формирующегося направления, которое все чаще связывают с правовым регулированием искусственного интеллекта. Для ФСИН России это соотношение имеет прикладное значение. Уголовно-исполнительное право задает пределы обращения с осужденным и цели исполнения наказания. Информационное право определяет режимы доступа, защиты и обработки сведений. Административное право отвечает за законность деятельности публичной администрации и организацию контроля. Право искусственного интеллекта, если использовать этот термин как рабочую конструкцию, призвано соединить эти блоки применительно к новым алгоритмическим средствам управления [12, С.37]. Перспективной представляется разработка специального ведомственного механизма правовой сертификации ИИ-систем, применяемых в ФСИН России, включая конструктивный контур регулирования. Такой контур может включать реестр ИИ-систем по уровням риска; паспорт системы с описанием ее функций, используемых данных и правовых ограничений; запрет на применение непрозрачных алгоритмов в ситуациях, где результат способен затронуть правовой статус личности; процедуру ведомственного и внешнего аудита; механизм фиксации и оспаривания ошибок; а также специальные программы подготовки сотрудников. Наличие подобного набора инструментов служит гармонизации цифровой трансформации ФСИН России с принципами законности, гуманизации и защиты прав человека.

Выводы

Искусственный интеллект, используемый в служебной деятельности сотрудников ФСИН России, представляет собой не только технологический ресурс, но и самостоятельный юридический вызов. Перспективы его применения очевидны: повышение точности наблюдения, ускорение обработки информации, развитие аналитических возможностей, поддержка управленческих решений, создание единой цифровой среды. Но эти перспективы становятся правомерными лишь при условии, что интеллектуальные системы будут встроены в четкий нормативный контур, исключающий подмену права автоматизированным усмотрением. Дальнейшее развитие рассматриваемой проблематики связано с выработкой специальной отраслевой модели, в которой служебная целесообразность, техническая эффективность и правовая допустимость рассматриваются как взаимосвязанные, но не совпадающие основания применения искусственного интеллекта в учреждениях и органах УИС.

Список литературы:

[1] Шиняев К.А., Морозов А.С. Современные цифровые технологии в системе надзора следственных изоляторов уголовно-исполнительной системы Российской Федерации // Вестник Самарского юридического института. 2025, №4 (65). С. 62-66.

[2] Денисенко О. И., Жаров И. С., Кадралеева Ж. А. Использование систем идентификации личности для обеспечения безопасности на режимных объектах уголовно-исполнительной системы // Вестник Самарского юридического института ФСИН России. 2024, № 4. С. 113-119.

[3] Пекарева В.В., Фроловская Ю.И. Искусственный интеллект в уголовно-исполнительной системе // Право и государство: теория и практика. 2024, № 10. С. 329-331.

[4] Зорина Н.С. О факторах и профилактике компьютерной зависимости у подростков // Евразийский юридический журнал. 2021. № 8(159). С. 198-199.

[5] Зорина Н.С. Информационная безопасность подростков в Интернете как средство предупреждения преступности среди несовершеннолетних // Закон и право. 2022, № 2. С. 152-155.

[6] Ковалев С.Д. Перспективы использования искусственного интеллекта в исправительных учреждениях ФСИН России // Аграрное и земельное право. 2025, № 1. С. 241-243.

[7] Царькова Е.Г., Кочкина О.В. Применение искусственного интеллекта при обработке данных в научной и образовательной деятельности Федеральной службы исполнения наказаний // Ведомости уголовно-исполнительной системы. 2022, № 9(244). С. 51-59.

[8] Минаев В.А., Бондарь К.М., Федорович В.Ю. Биометрия защиты объектов: возможности и перспективы // Информация и безопасность. 2025. Т. 28, № 1. С. 47-56.

[9] Царькова Е.Г. К вопросу формирования обучающих датасетов для выявления источников распространения экстремистского контента в сети Интернет // Научно-технический вестник Поволжья. 2024, № 3. С. 134-136.

[10] Пальянова Н.В. Использование искусственного интеллекта в сфере Legal Tech: современные возможности и перспективы // Социально-экономическое развитие и качество правовой среды: Труды VIII Моск. юрид. форума, XIX Междунар. науч.-прак. конф. Ч. 2. М.: МГЮА, 2021 С. 260-267.

[11] Понкин И.В. Государственное управление и регуляторное пространство в сфере искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022, № 11 (99). С. 108-116.

[12] Минбалеев А.В. Регулирование использования искусственного интеллекта в России // Информационное право. 2020, № 1. С. 36-39.

References:

[1] Shinyaev K.A., Morozov A.S. Modern digital technologies in the system of supervision of pre-trial detention centers of the penitentiary system of the Russian Federation//Bulletin of the Samara Law Institute. 2025, №4 (65). S. 62-66.

[2] Denisenko O. I., Zharov I. S., Kadraleeva Zh. A. The use of identity systems to ensure security at sensitive facilities of the ugo-catch-executive system//Bulletin of the Samara Law Institute of the Federal Penitentiary Service of Russia. 2024, № 4. S. 113-119.

[3] Pekareva V.V., Frolovskaya Yu.I. Artificial intelligence in the penal system//Law and the state: theory and practice. 2024, № 10. S. 329-331.

[4] Zorina N.S. On factors and prevention of computer addiction in sprouts//Eurasian Law Journal. 2021. № 8(159). S. 198-199.

[5] Zorina N.S. Information security of adolescents on the Internet as a means of preventing juvenile crime//Law and law. 2022, № 2. S. 152-155.

[6] Kovalev S.D. Prospects for the use of artificial intelligence in government institutions of the Federal Penitentiary Service of Russia//Agrarian and land law. 2025, № 1. S. 241-243.

[7] Tsarkova E.G., Kochkina O.V. The use of artificial intelligence in the processing of data in the scientific and educational activities of the Federal Penitentiary Service//Vedomosti of the penal system. 2022, № 9(244). S. 51-59.

[8] Minaev V.A., Bondar K.M., Fedorovich V.Yu. Biometrics of object protection: opportunities and prospects//Information and security. 2025. T. 28, NO. 1. S. 47-56.

[9] Tsarkova E.G. On the formation of training datasets to identify sources of distribution of extremist content on the Internet//Scientific and Technical Bulletin of the Volga Region. 2024, № 3. S. 134-136.

[10] N.V. Palyanova. The use of artificial intelligence in the field of Legal Tech: modern opportunities and prospects//Socio-economic development and quality of the legal environment: Proceedings VIII Mosk. jurid. forum, XIX International. scientific-practical. conf. PART 2. M.: MOSCOW STATE LAW ACADEMY, 2021 S. 260-267.

[11] Ponkin I.V. Public administration and regulatory space in the field of artificial intelligence//Bulletin of the University named after O.E. Kutafina (MSLA). 2022, № 11 (99). S. 108-116.

[12] Minbaleev A.V. Regulation of the use of artificial intelligence in Russia//Information law. 2020, № 1. S. 36-39.

