Дата поступления рукописи в редакцию: 18.04.2026 г.
Дата принятия рукописи в печать: 27.05.2026 г.

DOI: 10.24412/2782-3849-2026-5-50-52

ЦАРЬКОВА Евгения Геннадьевна,

ведущий научный сотрудник ФКУ НИИ ФСИН России, кандидат физико-математических наук,

e-mail: university69@mail.ru

ПРАВОВЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЦЕССЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ФСИН РОССИИ

Аннотация. *В статье проводится анализ правовых барьеров практического внедрения технологий искусственного интеллекта (ИИ) в информационное обеспечение деятельности Федеральной службы исполнения наказаний (ФСИН России). Отмечаются ключевые проблемные моменты, включая неопределенность юридической силы алгоритмических отчетов, а также риски информационной безопасности в локальных ведомственных информационно-телекоммуникационных сетях. На основе адаптации доктринальных подходов, включая интерактивный режим верификации, сохранение статуса документов, разграничение служебных потоков, предлагаются меры по совершенствованию правовой основы ведомственного информационного обеспечения. В исследовании подчеркивается, что системное правовое укрепление служит преодолению барьеров цифровизации, обеспечению баланса между преимуществами инноваций и защитой прав осужденных в условиях режима изоляции. Предложенные меры направлены на укрепление государственной безопасности в контексте стратегических документов в сфере искусственного интеллекта.*

Ключевые слова: *искусственный интеллект, уголовно-исполнительная система Российской Федерации, алгоритмическая прозрачность, персональные данные, объяснимый ИИ, алгоритмическая дискриминация*.

TSARKOVA Evgeniya Gennadievna,

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

LEGAL ASPECTS OF IMPLEMENTING ARTIFICIAL INTELLIGENCE INTO THE INFORMATION SUPPORT PROCESSES OF THE FEDERAL PENITENTIARY SERVICE OF RUSSIA

Annotation. *The article analyzes the legal barriers to the practical implementation of artificial intelligence (AI) technologies in the information support of the Federal Penitentiary Service of Russia. It highlights key problematic issues, including the uncertainty of the legal force of algorithmic reports, as well as information security risks in local departmental information and telecommunication networks. Based on the adaptation of doctrinal approaches – including an interactive verification mode, the preservation of document status, and the segregation of official data flows – measures are proposed to improve the legal framework for departmental information support. The study emphasizes that systematic legal strengthening serves to overcome the barriers to digitalization, ensuring a balance between the benefits of innovation and the protection of the rights of convicted persons under conditions of isolation. The proposed measures are aimed at strengthening state security in the context of strategic documents in the field of artificial intelligence.*

Key words*: artificial intelligence, penal enforcement system of the Russian Federation, algorithmic transparency, personal data, explicable AI, algorithmic discrimination.*

Практическое внедрение технологий искусственного интеллекта в деятельность ФСИН России сегодня выходит за рамки теоретических дискуссий, становясь неотъемлемой частью цифровой трансформации уголовно-исполнительной системы Российской Федерации (УИС). Эти процессы осуществляются в соответствии с Национальной стратегией развития искусственного интеллекта в Российской Федерации на период до 2030 года, а также ведомственной программой цифровой трансформации ФСИН России. В настоящее время учреждениях и органах УИС искусственный интеллект (ИИ) широко применяется для автоматизированного анализа в системах видеонаблюдения, биометрической

идентификации и др. [1, С. 242]. При этом сферы внедрения ИИ имеют широкие перспективы применения, включая прогнозирование поведения осужденных на основе данных учета, оптимизацию расстановки персонала, обработку больших массивов статистической информации о нарушениях режима для оперативного реагирования на инциденты безопасности и снижения нагрузки на сотрудников [2, С. 330; 3, С. 8]. Однако реальная эксплуатация таких систем сталкивается с определенными правовыми барьерами, связанными, в том числе, с отсутствием четкого регулирования юридической силы решений, пголученных на основе ИИ-систем, неопределенностью статуса электронных документов, генерируемых большими языковыми моделями, а также пробелами в реализации процессов верификации результатов, полученных интеллектуальными алгоритмами, что делает затруднительным их полноценное использование на практике [4, С. 184].

В настоящее время внедрение систем искусственного интеллекта в практическую деятельность ФСИН России запущено в форме готовых решений, а также пилотных проектов по распознаванию лиц на камерах видеонаблюдения, где нейросетевые алгоритмы в режиме реального времени способны выявлять попытки несанкционированного перемещения или нарушения режима изоляции с выдачей сигналов тревоги на пост охраны [1, С. 243]. Такие системы требуют интеграции с локальными ведомственными компьютерными сетями, но не связаны с необходимостью подключения к сети Интернет. Параллельно развиваются направления внедрения ИИ-решений в пенитенциарную медицину, процессы трудовой адаптации, работу психологов, однако данные успешное протекание данных процессов во многом зависит от их качественного правового регулирования [5, С. 189].

Одним из проблемных аспектов практического применения ИИ в информационном обеспечении УИС становится понятийная неопределенность в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», где определение документированной информации не учитывает специфику алгоритмически сгенерированных отчетов о поведении осужденных, требующих реквизитов, подобных электронной подписи сотрудника, для закрепления их значимости. На практике это означает, что выводы ИИ-анализа видеозаписей с камер видеонаблюдения не могут быть приобщены к материалам дисциплинарных производств, поскольку отсутствует механизм удостоверения промежуточных результатов обработки данных. Аналогично, в Федеральном законе № 63-ФЗ «Об электронной подписи» отсутствуют положения, регулирующие закрепление внутренних решений ФСИН России, например, верификацию ИИ-прогнозов о рисках рецидива. В данном случае сотрудник оперативного отдела должен был бы ставить свою подпись под выводами нейросети, однако децентрализованные удостоверяющие центры не предоставляют сертификаты, адаптированные к режимным потребностям УИС.

Внедрение ИИ-решений в ведомственный документооборот, в свою очередь, сталкивается с рисками нарушения кибербезопасности, где информация об осужденных, обрабатываемая в экспертных системах, циркулирует в локальных сетях учреждений, но принцип открытости из статьи 3 Федерального закона № 149-ФЗ конфликтует с необходимостью полной изоляции данных, предотвращающей утечки в сеть Интернет. Без разграничения потоков – служебных в закрытых сетях и общедоступных на внешних веб-порталах – использование ИИ приводит к уязвимостям, усугубляемым отсутствием ведомственного центра электронной подписи. В результате эффективность пилотных проектов ограничены правовыми пробелами, требующими постоянной ручной верификации решений человеком-оператором в интерактивном режиме [6, С. 57].

Ведомственное делопроизводство и статистический учет не предусматривают порядок интеграции ИИ-решений, несмотря на планы цифровой трансформации, включающие широкое внедрение систем биометрической идентификации, анализ медицинских данных и др. В результате многие цифровые проекты рискуют остаться экспериментальными из-за неурегулированности правового статуса выводов, полученных на их основе. Возникает объективная необходимость в адаптации доктринальных конструкций, включая интерактивный режим работы ИИ-алгоритмов с обязательной проверкой сотрудником, сохранение статуса документированной информации и разграничение служебных потоков, применительно к реалиям функционирования органов и учреждений УИС, где алгоритмы искусственного интеллекта могут оказывать существенную помощь в обеспечении оперативного реагирования на нарушения, но требуют закрепления юридической силы полученных заключений для принятия, например, дисциплинарных мер.

В качестве практических рекомендаций для решения обозначенных проблемных моментов может быть рассмотрено внесение в Федеральный закон № 149-ФЗ

уточнений, касающихся состава реквизитов документированной информации, используемой пенитенциарным ведомством, а также закрепление принципа разграничения информационных потоков в режимных органах. Это позволило бы придавать отчетам искусственного интеллекта о нарушениях режима статус процессуальных доказательств. В Федеральный закон № 63-ФЗ целесообразно включить механизм создания удостоверяющих центров ФСИН России, обеспечивающих электронную подпись сотрудников при верификации алгоритмов, тем самым сделав возможным их применение в повседневных операциях, например, при контроле за передвижением осужденных. Целесообразно закрепление Приказом ФСИН России порядка применения ИИ, который определил бы практические особенности решения таких задач, как видеомониторинг и прогнозирование, установил бы процедуру интерактивной верификации, а также регламентировал защиту данных в локальных компьютерных сетях. Уместна также разработка государственной Доктрины информационного обеспечения с использованием ИИ для правоохранительных органов, где акцент делается, в том числе, на внедрении технологий искусственного интеллекта в деятельность УИС.

Практическое внедрение элементов искусственного интеллекта в деятельность ФСИН России, включая интеллектуальное видеонаблюдение, прогнозирование рисков деструктивного поведения в учреждениях УИС, демонстрирует свою эффективность в снижении инцидентов безопасности и оптимизации ресурсов, однако без преодоления выявленных нормативных пробелов остается уязвимым перед рисками утраты юридической силы полученных выводов и информационной безопасности. Предложенные авторские рекомендации служат укреплению правового фундамента, позволяющего масштабировать технологии ИИ на широкий спектр направлений деятельности УИС. Подобный системный подход не только направлен на устранение барьеров цифровизации, но и служит укреплению защиты прав осужденных, законности режимных решений и интересов государства, а также определяет направления ведомственных инноваций, соответствующих Национальной стратегии искусственного интеллекта на период до 2030 года. Гармоничное сочетание технологического потенциала и строгого правового регулирования способствуют устойчивому развитию уголовно-исполнительной системы Российской Федерации и служат инструментом обеспечения общественной безопасности.

Список литературы:

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

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

[3] Андреева Е.А., Беляев А.К., Еремин Ю.М., Царькова Е.Г. Методы биометрической идентификации на основе применения нейросетевых технологий / // Информационные технологии в УИС. 2019. № 3. С. 2-10.

[4] Забайкалов А.П. О регламенте Европейского Союза об искусственном интеллекте // Духовно-нравственные ценности как основа технологического суверенитета России: Материалы XVIII Всероссийской научно-практической конференции, Липецк, 24 апреля 2024 г. – Воронеж: Наука-Юнипресс, 2024. С. 181-185.

[5] Помогалова Ю.В. Зарубежный опыт использования технологии искусственного интеллекта в контексте пенитенциарной безопасности // Вестник Воронежского института ФСИН России. 2024, № 3. С. 188-194.

[6] 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.

References:

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

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

[3] Andreeva E.A., Belyaev A.K., Eremin Yu.M., Tsarkova E.G. Methods of biometric identification based on the use of neural network technologies///Information technologies in UIS. 2019. № 3. S. 2-10.

[4] Zabaykalov A.P. On the regulations of the European Union on artificial intelligence//Spiritual and moral values as the basis of the technological sovereignty of Russia: Materials of the XVIII All-Russian Scientific and Practical Conference, Lipetsk, April 24, 2024 - Voronezh: Nauka-Unipress, 2024. S. 181-185.

[5] Pomogalova Yu.V. Foreign experience in using artificial intelligence technology in the context of penitentiary security//Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2024, № 3. S. 188-194.

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