

Дата поступления рукописи в редакцию: 25.06.2026 г.

DOI: 10.24412/2076-1503-2026-8-694-697

Дата принятия рукописи в печать: 15.07.2026 г.

КОЧКИНА Оксана Владимировна,
сотрудник отдела по исследованию проблем трудовой
занятости осужденных и экономических проблем
функционирования уголовно-исполнительной системы НИЦ-1
ФКУ НИИ ФСИН России, кандидат юридических наук,
e-mail: oks2790@list.ru

ТЯБИНА Юлия Александровна,
кандидат юридических наук,
e-mail: juliatyabina@yandex.ru

К ВОПРОСУ СТАНОВЛЕНИЯ И РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье исследуется процесс становления и развития искусственного интеллекта в уголовно-исполнительной системе Российской Федерации. Произведен анализ нормативных правовых актов, которые затрагивают рассматриваемую сферу деятельности, на протяжении всего исторического периода внедрения искусственного интеллекта в учреждениях и органах уголовно-исполнительной системы Российской Федерации. Детальный анализ исторического развития искусственного интеллекта в уголовно-исполнительной системе Российской Федерации позволил произвести периодизацию и выделить основные этапы развития исследуемой деятельности. Подробно проанализированы проблемы и ограничения, которые непосредственно отражаются на эффективности использования искусственного интеллекта в уголовно-исполнительной системе Российской Федерации. С 1 марта 2026 года вступил в силу приказ ФСТЭК от 11.04.2025 года № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», который установил новые требования к защите информации при использовании искусственного интеллекта в государственных органах. Данные требования в основном касаются безопасности внедряемого продукта, уровня квалификации работников в этой сфере, степени ответственности при работе с подрядчиками. Детально рассматриваются проблемы и ограничения, которые непосредственно отражаются на эффективности применения и использования искусственного интеллекта в уголовно-исполнительной системе Российской Федерации. Произведенное исследование позволило обозначить ряд рекомендаций организационного, правового и технического характера, которые направлены на усиление защиты информации в учреждениях и органах уголовно-исполнительной системы Российской Федерации.

Ключевые слова: технологии, цифровизация, искусственный интеллект, уголовно-исполнительная система, информационные технологии, цифровая трансформация.

KOCHKINA Oksana Vladimirovna,
employee of the Department of Problem Research the employment
of convicts and the economic problems of the functioning of the
penal system SIC-1 of the Federal Research Institute of the Federal
Penitentiary Service of Russia, Candidate of Law

TYABINA Yuliya Alexandrovna,
candidate of Law

ON THE ISSUE OF THE FORMATION AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN THE PENAL SYSTEM OF THE RUSSIAN FEDERATION

Annotation. *The article examines the process of formation and development of artificial intelligence in the penal system of the Russian Federation. The analysis of regulatory legal acts that affect the field of activity under consideration has been carried out throughout the historical period of the introduction of artificial intelligence into institutions and bodies of the penal system of the Russian Federation. A detailed analysis of the historical development of artificial intelligence in the penal system of the Russian Federation allowed us to make a periodization and identify the main stages of the development of the activity under study. The problems and limitations that directly affect the effectiveness of the use of artificial intelligence in the penal system of the Russian Federation were analyzed in detail. On March 1, 2026, FSTEC Order No. 117 dated 04/11/2025 "On Approval of Requirements for the Protection of Information Contained in State Information Systems, other Information Systems of Government Agencies, State Unitary Enterprises, and Government Agencies" entered into force, which established new requirements for information protection when using artificial intelligence in government agencies. These requirements mainly relate to the safety of the product being implemented, the level of education of employees in this area, and the degree of responsibility when working with contractors. The problems and limitations that directly affect the effectiveness of the application and use of artificial intelligence in the penal system of the Russian Federation are considered in detail. The study made it possible to identify a number of recommendations of an organizational, legal and technical nature, which are aimed at strengthening information protection in institutions and bodies of the penal system of the Russian Federation.*

Key words: *technology, digitalization, artificial intelligence, penal enforcement system, information technology, digital transformation.*

Повышение эффективности работы любой организации все чаще достигается за счет развития и внедрения искусственного интеллекта (далее – ИИ), благодаря которому оптимизируются многие внутренние процессы и сокращаются операционные издержки. В уголовно-исполнительной системе Российской Федерации (далее – УИС РФ) использование технического потенциала началось с 2010 года, что отразилось в распоряжении Правительства Российской Федерации от 14.10.2010 № 1772-р «Концепция развития уголовно-исполнительной системы Российской Федерации до 2020 года». Внедряемые технологии были направлены на мониторинг поведения осужденных и обеспечение безопасности. В этот период (с 2011 года по 2015 год) формировалась базовая автоматизация деятельности учреждений и органов УИС РФ без учета решений на базе ИИ. Данный период характеризуется развитием видеонаблюдения, но без видеоаналитики, активным использованием электронных браслетов, внедрением электронного документооборота, автоматизацией основной отчетности УИС РФ и др. С 2016 года по 2018 год появляются первые шаги по объединению отдельных ранее полученных разработок в данной области, путем создания автоматизированных информационных систем и пр.

Дальнейший стратегический вектор на внедрение ИИ в Российской Федерации (далее – РФ)

определили указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» и «Национальная стратегия развития искусственного интеллекта на период до 2030 года». С этого момента УИС РФ участвует в постепенной цифровизации процессов, направленных на безопасность и эффективное управление за счет аналитических и прогнозных данных, обрабатываемых посредством ИИ. Нормативную правовую основу для внедрения цифровых технологий в деятельность учреждений и органов УИС РФ заложила Концепция развития уголовно-исполнительной системы РФ на период до 2030 года, утвержденная распоряжением Правительства РФ от 29 апреля 2021 года № 1138-р (далее – Концепция). Документ включает в себя раздел цифровой трансформации УИС РФ, что говорит о стратегическом курсе технологической модернизации учреждений и органов до 2030 года.

В период с 2022 по 2023 год происходило тестирование различных алгоритмов для автоматического обнаружения противоправной активности среди осужденных через систему видеонаблюдения, формирование единой информационной системы и электронного взаимодействия с различными правоохранительными органами. В 2024 году наращиваются обороты по применению ИИ-решений в деятельности учреждений и органов УИС РФ. Проводятся научные исследования и

эксперименты с различными программами. И уже 2025 год можно охарактеризовать как год активного внедрения робототехники и цифровых программ. Стоит отметить, что за эти 15 лет УИС РФ прошла огромный путь от начальных этапов автоматизации процессов до внедрения системных решений на базе алгоритмов ИИ. Сейчас ИИ является важным инструментом, который способен трансформировать пенитенциарную систему [1].

Таким образом, анализ исторического развития ИИ в УИС РФ позволил выделить основные этапы в данной деятельности, а именно:

этап базовой информатизации и подготовки необходимой инфраструктуры (2010 – 2018 гг.);

этап создания нормативных правовых основ и стратегических ориентиров (2019-2021 гг.);

этап практического внедрения (2021 – 2024 гг.);

этап масштабирования и внедрения комплексных решений (2025 – по наст.вр.).

Вместе с тем, следует отметить, что применение ИИ в УИС РФ по сей день сопряжено с рядом ограничений и проблем, которые непосредственно отражаются на объемах внедрения и эффективности его использования.

К таким сдерживающим факторам можно отнести следующее:

Правовые ограничения. Основная проблема в данном направлении связана с отсутствием специальных нормативных правовых актов, которые бы регулировали вопросы внедрения и использования ИИ в учреждениях и органах УИС РФ. Так же стоит отметить, что единый реестр российского программного обеспечения (далее – ЕРРПО) и Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) ввели ряд ограничений и требований к внедрению и использованию ИИ-технологий в России, что обусловлено необходимостью обеспечения информационной безопасность нашей страны. Данные меры могут повлиять на доступность таких решений для учреждений и органов, так как при выборе программного обеспечения УИС РФ должна отдавать предпочтение продуктам, входящим в этот реестр. В настоящее время разработан законопроект «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации», планируемый к введению в действие с 01.09.2027. Данный законопроект направлен на защиту России в рассматриваемой сфере и закрепляет исключительность использования ИИ только на базе отечественного программного обеспечения, соответствующее требованиям ЕРРПО и ФСТЭК. Это накладывает в определенной степени ограничения в выборе платформ, что может замедлить развитие ИИ в УИС.

Конфиденциальность и безопасность. Работа с программным обеспечением всегда связана с риском утечки важных сведений. Стоит отметить, что Приказ ФСТЭК от 11.04.2025 года № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – приказ ФСТЭК № 117) закрепил требования к безопасности внедряемого ИИ и наложил запрет на использование облачных ИИ-сервисов для обработки данных, относящихся к информации ограниченного доступа. Согласно данному нормативному правовому акту, информационные системы УИС РФ теперь должны соответствовать новым требованиям, так же вводятся непрерывный цикл оценки состояния защиты информации и конкретные сроки по устранению уязвимостей.

Степень ответственности. Согласно приказу ФСТЭК № 117 подрядчики, которые взаимодействуют с учреждениями и органами при получении доступа к информационным системам УИС РФ обязаны соблюдать политику по защите информации в государственных учреждениях. Данные условия должны быть отражены в договорах с подрядчиками. Но стоит учитывать тот факт, что ответственность за защиту информации лежит на УИС РФ, даже если работы были проведены подрядчиком. На наш взгляд, рассматриваемая проблема требует детальной проработки, необходимо четкое закрепление и распределение обязанностей между разработчиком программного обеспечения, учреждениями и органами УИС РФ, и конкретными должностными лицами, которые принимают решения с учетом прогнозов [2].

Требования к квалификации персонала. Востребованность в специалистах с навыками работы ИИ и анализом данных растет с каждым годом [3]. Приказ ФСТЭК № 117 закрепляет требования к работникам по защите информации, а именно не менее 30 % работников подразделения по защите информации должны иметь соответствующее профессиональное образование, специальности или направление подготовки по информационной безопасности, либо пройти обучение по соответствующей программе профессиональной переподготовки. Обязательная оценка знаний данных специалистов должна производиться раз в три года. Любое компьютерное происшествие в учреждении (органе) должно сопровождаться внеплановым обучением. ИИ-сфера достаточно стремительно развивается, что диктует необходимость непрерывного обучения и быстрой адаптации специалистов к постоянно меняющимся условиям.

Обязанности по защите информации должны быть отражены в должностных инструкциях указанных сотрудников. Вместе с тем, специалисты такого уровня требуют соответствующей оплаты труда, что, в свою очередь, отражается на финансовой нагрузке УИС РФ.

Таким образом, проведенный анализ позволил сформулировать комплекс рекомендаций по оптимальному использованию технологий ИИ в УИС РФ, учитывающий в первую очередь необходимость усиления защиты информации. Представляется необходимым закрепление лиц, ответственных за защиту информации в учреждениях и органах УИС РФ с четким разграничением функционала, обязанностей и ответственности. Вместе с тем, необходимо пересмотреть и актуализировать документацию в соответствии с обновленными нормативными требованиями. Следует акцентировать внимание на квалификации работников в рассматриваемой области и практических отработках действий по факту различных инцидентов. Договоры, заключенные с подрядчиками, необходимо дополнить требованиями по защите информации. Одним из ключевых приоритетов остается миграция ИТ-ландшафта на отечественные решения с полным отказом от иностранного ПО и зарубежных облачных сервисов. Данные меры позволят оптимизировать административные процессы и обеспечить надлежащий контроль за использованием ИИ в УИС РФ.

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] Царькова Е.Г. Правовые принципы применения предиктивного искусственного интеллекта в учреждениях уголовно-исполнительной системы Российской Федерации // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». 2026. № 41. С. 152-160.

[3] Лещенко С.А., Тищенко Ю.Ю. Искусственный интеллект в системе высшего юридического образования уголовно-исполнительной системы // Вопросы современной науки и практики. 2024. № 2 (11). С. 87-90.

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] Tsarkova E.G. Legal principles for the use of predictive artificial intelligence in institutions of the penitentiary system of the Russian Federation // Bulletin of the public research laboratory "Interaction of the penitentiary system with civil society institutions: historical, legal and theoretical-methodological aspects." 2026. № 41. S. 152-160.

[3] Leshchenko S.A., Tishchenko Yu.Yu. Artificial intelligence in the system of higher legal education of the penitentiary system // Issues of modern science and practice. 2024. № 2 (11). S. 87-90.

