

Дата поступления рукописи в редакцию: 27.04.2026 г.

DOI: 10.24412/2782-3830-2026-5-415-420

Дата принятия рукописи в печать: 02.06.2026 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 ПРИНЦИПЫ ПРИМЕНЕНИЯ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЙ ФСИН РОССИИ

Аннотация. Статья посвящена формированию системы правовых принципов применения робототехники в учреждениях ФСИН России в условиях роста автономности технических средств и отсутствия специальных норм, комплексно регулирующих их использование в пенитенциарной сфере. Подчеркиваются преимущества внедрения роботов в деятельности учреждений уголовно-исполнительной системы Российской Федерации (УИС), включая возможность непрерывного наблюдения, снижение нагрузки на личный состав, повышение устойчивости контроля и расширение возможностей фото- и видеофиксации обстановки на охраняемом объекте, а также более точную локализацию потенциально опасных зон и оперативную маршрутизацию реагирования. Отмечается, что использование робототехники создает предпосылки для перераспределения функций между человеком и технической системой, что требует нормативно закреплённого разграничения задач автоматизированного мониторинга, аналитической поддержки и принятия юридически значимых решений. Обосновывается, что внедрение робототехнических систем в деятельность УИС не может строиться только на технической целесообразности и ведомственном усмотрении, поскольку автономность, программная изменяемость и повышенная причиняющая способность таких систем затрагивают конституционные права осуждённых, полномочия сотрудников и пределы уголовно-правовой ответственности, порождая также риск «размывания» субъекта ответственности при ошибках алгоритма или сбоях эксплуатации. Предлагается система правовых принципов применения робототехники в учреждениях ФСИН России, включающая принципы законности, функциональной определенности, соразмерности, алгоритмической прозрачности, сохранения существенного человеческого контроля, технологической верифицируемости, дифференциации правового режима по уровню автономности и персонализированного распределения ответственности, а также защиты прав человека и режимной безопасности данных. Приводится аргументация указанных принципов, подчеркивается, что именно системный подход, а не фрагментарные запреты, обеспечивает создание качественного методологического каркаса для будущего ведомственного, уголовно-исполнительного и уголовно-правового регулирования процессов внедрения робототехнических систем в деятельность учреждений УИС и минимизацию рисков произвольного или непропорционального использования таких технологий.

Ключевые слова: уголовно-исполнительная система Российской Федерации, робототехническая система, искусственный интеллект, автономная интеллектуальная система, правовые принципы, пенитенциарная безопасность, алгоритмическая прозрачность, человеческий контроль, цифровизация УИС, правовые риски, режим исполнения наказания, дифференциация ответственности, видеоаналитика, робот-патрульный.

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

LEGAL PRINCIPLES FOR THE USE OF ROBOTIC SYSTEMS IN THE ACTIVITIES OF INSTITUTIONS OF THE FEDERAL PENITENTIARY SERVICE OF RUSSIA

Annotation. *The article is devoted to the formation of a system of legal principles for the use of robotic systems in the activities of institutions of the Federal Penitentiary Service of Russia in the context of increasing autonomy of technical means and the absence of special norms comprehensively regulating their use in the penitentiary sphere. The advantages of introducing robots into the activities of institutions of the penal enforcement system of the Russian Federation are highlighted, including the possibility of continuous monitoring, reducing the burden on personnel, increasing the stability of control, expanding the possibilities of photo and video recording of the situation at a protected facility, as well as more precise localization of potentially dangerous zones and operational routing of response. It is noted that the use of robotics creates prerequisites for the redistribution of functions between humans and technical systems, which requires a normatively established differentiation of tasks of automated monitoring, analytical support, and making legally significant decisions. It is argued that the introduction of robotic systems into the activities of the penal enforcement system cannot be based solely on technical feasibility and departmental discretion, since the autonomy, software modifiability, and increased harmful potential of such systems affect the constitutional rights of convicts, the powers of employees, and the limits of criminal liability, also creating a risk of «blurring» the subject of responsibility in the event of algorithm errors or operational failures. A system of legal principles for the use of robotics in institutions of the Federal Penitentiary Service of Russia is proposed, including the principles of legality, functional certainty, proportionality, algorithmic transparency, preservation of meaningful human control, technological verifiability, differentiation of the legal regime according to the level of autonomy, personalized distribution of responsibility, as well as protection of human rights and regime data security. The rationale for these principles is provided, and it is emphasized that it is precisely a systemic approach, rather than fragmentary prohibitions, that ensures the creation of a high-quality methodological framework for future departmental, penal enforcement, and criminal law regulation of the processes of introducing robotic systems into the activities of penal institutions and minimizes the risks of arbitrary or disproportionate use of such technologies.*

Key words: *Federal Penitentiary Service of Russia, robotic system, artificial intelligence, autonomous intelligent system, legal principles, penitentiary security, algorithmic transparency, human control, correctional digitalization, legal risks, prison regime, differentiation of liability, video analytics, patrol robot.*

Введение

Преимущества использования робототехнических систем в учреждениях ФСИН России в настоящее время перестают быть чисто прогностической категорией и получают предметное подтверждение в пилотных проектах цифровизации УИС [1, с.62]. Так, в 2026 г. в Самарской области в двух исправительных колониях протестирован автономный робот-патрульный, оснащенный системами навигации, видеонаблюдения и аналитики, который способен самостоятельно патрулировать заданную территорию, фиксировать нарушения режима, передавать данные и реагировать на нештатные ситуации. Для пенитенциарной системы такой эксперимент обеспечивает ряд положительных эффектов, включая возможность непрерывного автоматизированного контроля, снижение нагрузки на сотрудников, повышение устойчивости надзорных процедур и расширение массива объективно фиксируемых данных о событиях на режимной территории. Вышеизложенное подчеркивает актуальность вопросов, связанных с правовыми принципами применения робототехники в УИС, которое должно начинаться не с запретов, а с точного понимания институциональной выгоды, которую государство получает от роботизации ФСИН России [2, с.114].

Применение робототехники в пенитенциарных учреждениях имеет высокий положительный эффект, во многом за счет возможности повышения безопасности пространства, в котором цена ошибки традиционно высока. Человек ограничен временем наблюдения, физической выносливостью, погодными условиями, обзором и скоростью одновременной обработки сигналов, тогда как робототехническая система может поддерживать дежурный режим контроля без утомления, непрерывно записывая происходящее и передавая данные оператору в режиме реального времени [3, с.330; 4, с.160]. Для учреждений ФСИН России данный фактор выражается в получении дополнительного канала объективной фиксации и, как следствие, снижении зависимости от субъективных объяснений участников инцидента и расширении доказательственной базы для служебных проверок или дисциплинарного производства [5, с.152].

Следующим положительным эффектом служит возможность перераспределения человеческого ресурса. На примере внедрения робота-патрульного отмечается снижение нагрузки на сотрудников и совершенствование охраны объектов УИС. Для правового анализа это обстоятельство существенно, поскольку любое высво-

бождение кадрового ресурса в местах лишения свободы должно оцениваться не только как экономический эффект, но и как фактор повышения качества исполнения основных обязанностей персонала, включая индивидуальную профилактику, документирование происшествий, оперативное реагирование на конфликты, работу с осужденными, относящимися к группам риска [6, с.242]. Робот в данном контексте выполняет функцию технологического усилителя надзорной и информационной инфраструктуры учреждения.

Еще одно преимущество связано с расширением спектра задач, выполняемых в среде повышенного риска. Роботы как сложные цифровые объекты сочетают программную и аппаратную компоненты, способны перемещаться в разных средах, действовать на удалении от оператора и выполнять алгоритмически сложные функции. Для учреждений УИС эти факторы открывают возможности не только патрулирования, но и доставки грузов, мониторинга периметра, досмотра опасных участков, сопровождения режимных мероприятий, использования мобильных камер в труднодоступных зонах.

Вместе с тем, каждое технологическое преимущество одновременно образует новую правовую проблему, поскольку алгоритм, повышающий точность контроля, способен также повысить масштаб вреда при ошибке настройки, сбое или намеренном неправомерном использовании. Такая двойственная природа роботизации делает вопрос о соответствующих правовых принципах центральным. В деятельности пенитенциарного ведомства робототехнические системы не являются обычным техническим оснащением, подобным бытовой электронике или пассивным средствам учета. С учетом встроенных возможностей искусственного интеллекта (ИИ) они могут участвовать в принятии решений, влияющих на режим, маршруты движения, фиксацию нарушений, идентификацию лиц и порядок реагирования на тревожные события, что приводит к возникновению источника неопределенности, в котором ответственность распределяется между оператором, разработчиком, поставщиком и должностным лицом, принявшим систему в эксплуатацию [7, с.56; 8, с.47].

Материалы и методы

Под робототехнической системой для целей деятельности учреждений ФСИН России предлагается понимать совокупность программных и аппаратных компонентов, предназначенных для выполнения задач охраны, надзора, досмотра, доставки, контроля доступа или иной служебной функции в пенитенциарной среде с возможностью автономного либо полуавтономного исполнения отдельных операций. Для ФСИН России

это определение принципиально, поскольку позволяет отделить робототехническую систему от обычной камеры наблюдения, от отдельного программного модуля и от стандартного механизма без элементов алгоритмической адаптации. Искусственный интеллект в рассматриваемой сфере не сводится к любой цифровой обработке информации. Поскольку отличие искусственного интеллекта от обычного программного обеспечения состоит в функционале, позволяющем имитировать когнитивные функции, самообучаться и выбирать алгоритм действий вне заранее установленной программы, для учреждений УИС эта разница приобретает прямое юридическое значение: если система лишь воспроизводит заранее заданный сценарий, зона правовой оценки концентрируется на корректности настройки и эксплуатации; если же система самостоятельно выбирает вариант реагирования в заранее не определенной ситуации, возникает качественно иной уровень риска для прав осужденных, безопасности личного состава и распределения ответственности [9, с.136].

Автономная интеллектуальная система, внедряемая в учреждениях ФСИН России, может быть описана как устройство-робот, способное в пределах заложенной цели принимать самостоятельные решения в ситуации неполной определенности без немедленной команды оператора. Такая система способна патрулировать маршрут, выделять аномалии поведения, приоритезировать сигналы тревоги, менять траекторию движения или инициировать предусмотренный протокол оповещения [10, с.262]. Вместе с тем, чем шире объем автономных решений, тем строже должна быть система правовых принципов, ограничивающих допустимое использование робототехники в УИС.

Результаты и обсуждение

Основу такой системы составляет принцип законности применения робототехнических систем в деятельности учреждений ФСИН России. Его содержание не исчерпывается общим требованием действовать в рамках закона. В отношении пенитенциарной робототехники принцип законности означает, что каждая функциональная задача робота должна иметь нормативно определенную цель, допустимый объем воздействия, круг уполномоченных операторов, порядок документирования и пределы использования полученных данных. Так, если робот-патрульный фиксирует нарушение режима, право учреждения использовать этот материал должно опираться на установленный правовой режим хранения, передачи и проверки данных, а не на одно лишь техническое наличие видеозаписи.

Следующий принцип определяется как функциональная определенность. Допустимость применения робототехнической системы в УИС должна определяться наличием заранее определенных задач и решений, которые ей предстоит принимать. Рассматриваемый в качестве модельного примера робот-патрульный предназначен для патрулирования, фиксации нарушений и передачи информации. Такой набор функций юридически обозрим, поскольку система наблюдает, сообщает и поддерживает надзорный процесс. Иная ситуация возникла бы, если той же платформе без отдельного правового регулирования делегировали бы автоматическое применение специальных средств, блокировку проходов или принятие решений, влияющих на порядок изоляции конкретного осужденного [11, с.110]. Функциональная определенность предотвращает постепенное расширение полномочий системы за пределы первоначальной задачи.

Принцип соразмерности означает, что уровень технологического вмешательства, глубина сбора данных и степень автономности системы должны соответствовать легитимной пенитенциарной цели и не выходить за ее пределы. Так, например, робот, способный непрерывно собирать изображение, траектории движения, поведенческие паттерны и биометрические данные, требует гораздо более строгого режима обоснования, чем устройство, ограниченное визуальным патрулированием периметра. Соразмерность имеет и уголовно-правовое измерение в силу повышенной причиняющей способности роботов, возможности действовать на удалении и автономно выполнять объективную сторону преступления при минимальном человеческом участии. При использовании робототехники в учреждении УИС из этого тезиса вытекает простой вывод: чем выше способность системы причинить физический, организационный или правовой вред, тем уже должен быть круг ее допустимых автономных действий. Робот, который наблюдает, и робот, который физически блокирует проход или активирует специальное оборудование, не могут регулироваться единым стандартом допустимости.

Следующий принцип сводится к алгоритмической прозрачности как нормативному требованию. Здесь прозрачность означает не публичное раскрытие исходного кода, а возможность верифицировать, по каким данным, при каких настройках и по каким логическим правилам система приняла конкретное решение. Например, если робот-патрульный зафиксировал нарушение режима, у правоприменителя должна быть возможность проверить, что именно система распознала как нарушение, на основании какого сигнала, в какое время, с какой точностью и не была

ли ситуация следствием ошибочной калибровки. Без такой верифицируемости любая ссылка на «объективность алгоритма» утрачивает юридическую ценность. Алгоритмическая прозрачность особенно значима при использовании систем с элементами искусственного интеллекта. Поскольку ИИ способен выбирать алгоритм действий вне заранее установленной программы, предсказуемость поведения системы снижается по мере роста автономности. В случае применения таких систем в деятельности УИС это означает необходимость ведения обязательных журналов событий, протоколов обучения, фиксации версий модели, архивирования исходных параметров и возможности последующего экспертного воспроизведения алгоритмического решения.

Принцип существенного человеческого контроля выступает центральным ограничителем допустимой автономии роботов в учреждениях УИС. Смысл принципа состоит в том, что решения, способные затронуть жизнь, здоровье, достоинство, режим содержания или объем ограничений прав осужденного, не могут полностью передаваться автономной системе без реальной возможности вмешательства уполномоченного лица. Так, робот-патрульный осуществляет мониторинг и передает данные, а не замещает человека в применении ограничительных мер. На этой стадии технологического развития должно быть закреплено правило, не позволяющее в дальнейшем трансформировать функцию наблюдения в функцию автономного принуждения без пересмотра всей нормативной модели. Существенный человеческий контроль предполагает наличие как минимум трех элементов, включая возможность оператора изменить или прекратить действие системы до наступления деструктивных последствий, обязанность человека подтверждать критически значимые решения и полную прослеживаемость того, кто именно принял итоговое решение при конфликте сигналов и данных. Для учреждений ФСИН России к таким решениям могут быть отнесены изменение режима доступа, маркировка события как угрозы, инициирование мер по изоляции, применение специальных средств, использование материалов автоматической идентификации как основания для дисциплинарного либо процессуального реагирования и др.

Следующий принцип определяется как технологическая верифицируемость и отличается от принципа прозрачности тем, что акцентируется не на понимании логики алгоритма, а на технической возможности доказать исправность, корректность и устойчивость системы в конкретный момент эксплуатации. Учреждение не вправе

опираться на выводы робота как на юридически значимую информацию, если не обеспечена доказуемая надежность самой системы.

Далее следует принцип дифференциации правового режима по уровню автономности и по характеру служебной функции. Роботы могут выступать и как предмет посягательства, и как средство совершения преступления, а также могут существенно повышать общественную опасность деяния за счет удаленности оператора, грузоподъемности, мобильности и координации нескольких устройств. Как следствие, не может быть установлен единый правовой режим для всех робототехнических систем. Робот-патрульный, робот-доставщик, робот досмотрового назначения, стационарная платформа биометрической идентификации и автономная система аналитики поведения должны регулироваться различными наборами ограничений, требований к оператору и правилами допустимости использования результатов их работы. Дифференциация необходима и по уровню автономности. Устройство, действующее только по прямой команде человека, допускает один стандарт ответственности. Система, выбирающая маршрут и выделяющая отклонения поведения в автоматическом режиме, требует более сложной регламентации. Платформа, самостоятельно определяющая вариант реагирования в неопределенной ситуации, должна подпадать под наиболее строгий режим допуска, документирования и контроля. Без такого разграничения ведомство рискует либо искусственно затормозить полезную роботизацию, либо, наоборот, легализовать опасную автономность под видом обычного технического оснащения.

Следующий принцип состоит в персонализированном распределении юридической ответственности. Робот не является субъектом преступления, хотя способен фактически полностью выполнить объективную сторону деяния, если человек ограничился постановкой цели или программированием. Для учреждений ФСИН России этот вывод означает, что внедрение робототехнической системы обязательно должно сопровождаться предварительным юридическим картированием ответственности за выбор системы, за ее поставку, за настройку, за обновление, за обучение модели, за допуск к эксплуатации, за ежедневный контроль и за принятие решений на основе полученных системой данных. Если эти зоны не разведены заранее, любое вредное последствие может сопровождаться институциональным «размыванием вины».

Ключевым является принцип защиты прав человека, который означает, что робототехническая система не может использоваться для соз-

дания режима тотального непрерывного анализа личности без ясной правовой цели и достаточных гарантий оспаривания решений. Ограничения допустимы лишь в том объеме, который прямо вытекает из закона и целей исполнения наказания. Поэтому автоматическая квалификация поведения как «опасного», «подозрительного» или «аномального» не должна порождать правовые последствия без проверки уполномоченным сотрудником и без процессуальной возможности поставить под сомнение надежность алгоритма.

Выводы

С учетом вышеизложенного может быть сформулирован ряд выводов. В частности, целесообразно закрепление в ведомственном акте классификации робототехнических систем по уровню автономности, по виду функции и по степени допустимого воздействия на права и безопасность лиц, находящихся в учреждениях УИС. Без подобных мер внедрение робототехники будет строиться на локальных экспериментах и закупочных решениях, а не на единых правовых стандартах. Далее, необходима разработка обязательного протокола алгоритмической отчетности для всех систем с элементами искусственного интеллекта, используемых в УИС, включая хранение логов, фиксацию версий, журналирование изменений модели и порядок предоставления данных для служебной проверки и уголовного процесса. Кроме того, важно встраивание в закупочную и приемочную процедуру робототехнических систем правовой экспертизы. Современные пилотные проекты по внедрению робототехники акцентируют внимание на технических возможностях, устойчивости к условиям эксплуатации и интеграции с системами безопасности. Однако этого недостаточно для правомерного развития цифровизации УИС. Важно, чтобы системы, внедряемые в УИС, оценивались по матрице юридических критериев, включая допустимость функции, уровень автономности, объем собираемых персональных и биометрических данных, наличие режима журналирования, возможность человеческого вмешательства, потенциальные уголовно-правовые риски и совместимость с режимом исполнения наказания [12, с.37]. Законность, функциональная определенность, соразмерность, алгоритмическая прозрачность, существенный человеческий контроль, технологическая верифицируемость, дифференциация правового режима, персонализированное распределение ответственности, защита прав человека и режимная безопасность данных образуют не перечень пожеланий, а необходимый минимум для правомерной роботизации учреждений ФСИН России.

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., Кадралева 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. Влияние семейного неблагополучия на формирование преступного поведения подростков // Закон и право. 2023, № 1. С. 159-161.
- [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. The influence of family trouble on the formation of criminal behavior of adolescents// Law and law. 2023, № 1. S. 159-161.
- [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.