Научная статья
УДК 349

Правовая охрана служебных секретов производства (ноу-хау) с помощью технологий искусственного интеллекта

Владислав Сергеевич Ващенко,
Российская государственная академия
интеллектуальной собственности, Москва, Россия
Аспирант
vladser2001@gmail.com
https://orcid.org/0009-0003-5175-3838

Аннотация. В статье исследуется трансформация парадигмы гражданско-правовой охраны служебных секретов производства (ноу-хау) под влиянием технологий искусственного интеллекта. Актуальность статьи обусловлена нарастающим несоответствием между традиционными правовыми механизмами защиты конфиденциальной информации и коммерческой тайны, основанными на договорных и деликтных конструкциях, и новыми технологическими рисками, которые искусственный интеллект не только создает, но и помогает нивелировать. В статье обосновывается научная проблема недостаточности теоретической проработки гражданско-правового статуса «интеллектуального агента» в охране секретов производства и формулируются варианты ее решения, включая концепцию «разумных мер охраны с использованием ИИ» и предложения по модификации договорных конструкций. В заключение предлагаются рекомендации по интеграции искусственного интеллекта в систему охраны ноу-хау, где требуется не только внедрение технических, но и доктринальных правовых инноваций, направленных на признание и регламентацию новых цифровых реалий в рамках гражданского оборота.

Ключевые слова: служебный секрет производства, ноу-хау, искусственный интеллект, гражданско-правовая охрана, коммерческая тайна, разумные меры охраны, правовой режим информации, деликтная ответственность, договор о неразглашении.

Для цитирования: Ващенко В.С. Правовая охрана служебных секретов производства (ноу-хау) с помощью технологий искусственного интеллекта / В.С. Ващенко // IP: теория и практика. – 2026. – № 1 (13).

Original article

Legal protection of service-related production secrets (know-how) using artificial intelligence technologies

Vladislav S. Vashchenko,
Russian State Academy
of Intellectual Property, Moscow, Russia
Postgraduate Student
vladser2001@gmail.com
https://orcid.org/0009-0003-5175-3838

Abstract. The article examines the transformation of the civil law protection paradigm for service-related production secrets (know-how) under the influence of artificial intelligence (hereinafter — AI) technologies. The relevance of the article stems from the growing gap between traditional legal mechanisms for protecting confidential information and trade secrets, which are based on contractual and tortious constructs, and the new technological risks that AI not only creates but also helps to mitigate. The article step-by-step substantiates the scientific problem of insufficient theoretical development of the civil law status of an "intelligent agent" in the protection of secrets and formulates options for its solution, including the concept of "reasonable protection measures using AI" and proposals for modifying contractual structures. In conclusion, recommendations are proposed for integrating AI into the know-how protection system, which requires not only the introduction of technical but also doctrinal legal innovations aimed at recognizing and regulating new digital realities within the framework of civil turnover.

Keywords: service-related production secret, know-how, artificial intelligence, civil law protection, trade secret, reasonable protection measures, legal regime of information, tort liability, non-disclosure agreement.

For citation: Vashchenko V.S. Legal protection of service-related production secrets (know-how) using artificial intelligence technologies // IP: Theory and Practice. 2026. No. 1 (13).

Введение

В современной цифровой экономике, где информация является ключевым стратегическим активом, служебные секреты производства (ноу-хау) занимают особое место. Их ценность напрямую зависит от сохранения конфиденциальности. Российское гражданское законодательство (ст. 1465 ГК РФ) предоставляет охрану ноу-хау при условии, что обладатель принял

разумные меры для сохранения его секретности[1]. Однако сама концепция «разумных мер» претерпевает трансформацию в эпоху цифровизации и широкого внедрения технологий искусственного интеллекта (далее – ИИ). В связи с чем целью статьи является выявление системных противоречий в действующем правовом регулировании и обоснование необходимости разработки специальных гражданско-правовых подходов к использованию ИИ как инструмента охраны ноу-хау.

Методы

Для достижения поставленной цели в исследовании применялся комплекс общенаучных и частнонаучных методов: общенаучные (анализ, синтез, абстрагирования, логический, восхождения от абстрактного к конкретному, аналогия, индукция, дедукция), специально-юридические (формально-юридический, толкования правовых норм, структурно-функциональный, межотраслевой).

Основное исследование

Существующие затруднения решения практической задачи, стоящей перед организацией-обладателем ноу-хау, обосновываются таким образом, что это приводит к возникновению вопроса: как эффективно и юридически безопасно интегрировать системы ИИ в комплекс мер по охране конфиденциальной информации? Согласно действующему законодательству, а именно п. 1 ст. 16 Федерального закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «защита информации представляет собой принятие правовых, организационных и технических мер…»[2]. Данный перечень мер направлен на три основных вектора:

---

[1] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 23.07.2025) // Собрание законодательства РФ, 25.12.2006, № 52 (1 ч.), ст. 5496; Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне» // Собрание законодательства РФ, 09.08.2004, № 32, ст. 3283.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.09.2025) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

1. Обеспечение защиты информации от:

– несанкционированного доступа, уничтожения, изменения, блокировки, копирования, передачи, распространения и иных противоправных действий;

– неправомерного доступа, уничтожения, модификации, блокирования, несанкционированного копирования, разглашения, распространения или иного незаконного использования;

– любых противоправных действий, включая неправомерный доступ, уничтожение, искажение, блокирование, несанкционированного копирование, предоставление третьим лицам, распространение.

2. Соблюдение конфиденциальности информации ограниченного доступа:

– поддержание режима конфиденциальности для информации ограниченного распространения;

– обеспечение сохранности конфиденциальных сведений, доступ к которым ограничен;

– неразглашение информации, отнесенной к ограниченному доступу.

3. Реализация права на доступ к информации:

– осуществление права на получение информации;

– обеспечение возможности доступа к сведениям;

– гарантирование реализации правомочия по доступу к информации.

Данные интегративные затруднения носят двуединый характер.

С одной стороны, это технические и организационные меры. В данном аспекте возникает неясность, какой уровень технологической сложности будет признан судом «разумной мерой» для конкретного бизнеса (малого, среднего, крупного). Будет ли достаточно системы логирования доступа (процесс записи информации о действиях пользователей и системных событиях для последующего анализа, аудита и устранения проблем), или же от организаций ожидают внедрения предиктивной аналитики, т.е. использования исторических данных, статистических алгоритмов и

машинного обучения для прогнозирования будущих событий? Отсутствие таких правовых критериев ведет к правовой неопределенности и риску признания мер недостаточными в случае возможного правового спора в переговорном формате, претензионном и последующем судебном порядке, для разграничения технических и организационных мер по защите ноу-хау.

С другой стороны, можно отметить второй затруднительный аспект – правовой. Использование ИИ порождает новые юридические факты, не укладывающиеся в традиционные конструкции. Например, если ИИ-система, программа для ЭВМ на основе ИИ, анализируя поведение сотрудника, автоматически (без команды должностного лица) ограничивает ему доступ к данным, классифицируя его действия как подозрительные или нарушающие процедурный порядок, можно ли говорить о законности такого одностороннего применения ограничительных мер для контроля действий сотрудников или контрагентов? Кто несет ответственность, если алгоритм ИИ выдал «ложноположительное» срабатывание и причинил убытки сотруднику или контрагенту? Как доказывать в суде, что утечка информации была предотвращена именно благодаря «решению», принятому ИИ, т.к. в настоящий момент искусственный интеллект не обладает правосубъектностью и не имеет воли для принятия такого решения. Анализируя имеющиеся научные знания, можно отметить три основных направления, каждое из которых в отдельности не дает ответа на поставленную проблему, но имеет доктринальное подкрепление.

В цивилистической доктрине охраны ноу-хау (труды В.А. Дозорцева, Э.П. Гаврилова, И.С. Мухамедшина, Н.В. Нестеровой) детально проработаны понятие, признаки, договорные конструкции, деликтная ответственность. Однако в этих работах природа ИИ рассматривается в лучшем случае как один из многих технических инструментов наряду с шифрованием [1–4]. Пока еще не исследованы качественные изменения, которые вносит предиктивная и автономная природа ИИ в понятия «доступ», «разглашение», «неосторожность».

Правовая доктрина в сфере ИИ фокусируется на макропроблемах: правосубъектности роботов, ответственности за вред, причиненный автономными системами, авторском праве на произведения, созданные ИИ. Вопросы охраны информации с помощью ИИ, т.е. ИИ как инструмента правоприменения, остаются на периферии научного интереса.

Исследования по информационному праву и правовой информатике касаются в основном вопросов защиты персональных данных и государственной тайны, где режимы регулирования жестко формализованы. Гибкий гражданско-правовой режим коммерческой тайны, где «разумность мер» определяется обстоятельствами конкретного случая, остается без внимания в контексте ИИ.

В монографии современного исследователя Д.В. Бахтеева «Искусственный интеллект: этико-правовые основы» затрагиваются аспекты общетеоретических основ исследования искусственного интеллекта, технологических основ ИИ, этико-правовых основ позиционирования систем искусственного интеллекта в обществе и рассмотрения его как объекта правового регулирования с точки зрения публичных отраслей права [5].

Таким образом, цивилисты не погружаются в технологические особенности ИИ, а специалисты по праву ИИ не фокусируются на специфике охраны ноу-хау. Нет комплексной работы, которая синтезировала бы эти направления для решения конкретной правовой задачи.

На основе выявленных затруднений и анализа состояния научного знания можно сформулировать противоречие между объективной социально-экономической потребностью в использовании автономных и предиктивных систем искусственного интеллекта для обеспечения эффективной охраны служебных секретов производства (как нового стандарта «разумных мер») и неадаптированностью традиционного гражданско-правового инструментария (норм о договорах, деликтах, доказывании), который не учитывает специфику ИИ как активного, обучаемого и потенциально непрозрачного «агента» в правоотношениях по охране конфиденциальной информации.

Это противоречие проявляется в нескольких аспектах.

Правовой режим. Возникают противоречия между динамичным, алгоритмически определяемым доступом к данным в системе с ИИ и статичными способами определения круга лиц (путем содержащегося в локальных актах организации перечня), имеющих доступ.

В аспекте ответственности возникает противоречие между коллективным, «сетевым» характером причинения вреда при сбое или злонамеренном использовании ИИ-системы (разработчик, интегратор, оператор, пользователь) и индивидуальными подходами к установлению вины в гражданском праве.

В *процедуре доказывания* возникает противоречие между «черным ящиком» сложных нейросетей и объяснением того, как алгоритм принимает решения, когда их трудно интерпретировать.

В обоснование разработки и постановки научной проблемы выявленное противоречие позволяет сформулировать научную проблему, которая заключается в отсутствии целостной гражданско-правовой концепции, определяющей статус, условия правомерного применения и границы ответственности при использовании технологий искусственного интеллекта в качестве средства охраны служебных секретов производства (ноу-хау) в рамках российской правовой системы.

Постановку данной проблемы можно представить следующим алгоритмом:

1. Констатация факта, где технологии ИИ активно внедряются бизнесом для защиты информации, включая ноу-хау.

2. Выявление аномалии, где действующее гражданское законодательство не содержит специальных норм, регулирующих использование. Правовые последствия его применения неочевидны и спорны.

3. Формулировка конкретного проблемного вопроса: каким образом институты гражданского права (вещные, обязательственные, исключительные права, деликты) должны быть интерпретированы или модифицированы, чтобы

адекватно регулировать отношения, возникающие в связи с охраной ноу-хау с помощью ИИ?

4. Декомпозиция проблемы на подпроблемы, а именно правовая квалификация принятия решения системой действий (бездействия) автономной ИИ-системы в контексте нарушения режима коммерческой тайны; определение содержания и минимальных стандартов «разумных мер охраны с использованием ИИ»; распределение рисков и ответственности между субъектами (владелец ноу-хау, разработчик ИИ, интегратор, сотрудник) при сбое или вредоносном использовании системы; доказывание факта принятия достаточных мер охраны в спорах, связанных с ИИ.

Можно иметь основания полагать, что решение сформулированной научной проблемы разрешается не путем изменений в федеральные законы, регулирующие ИИ и правовые отношения в области ноу-хау, а за счет целенаправленной адаптации существующего гражданско-правового инструментария через доктринальное толкование и точечные законодательные поправки или же договорные конструкции.

Можно обратить внимание на следующие варианты решения.

Вариант 1. Доктринальное развитие концепции «разумных мер охраны». Для этого необходимо выработать в науке и закрепить в руководящих разъяснениях Верховного Суда РФ принцип технологической нейтральности и соразмерности. «Разумность мер» должна оцениваться не по факту использования конкретной технологии ИИ, а по ее способности адекватно противостоять актуальным угрозам для конкретного вида информации с учетом размера и отрасли компании. Это позволит судам гибко подходить к оценке, избегая как избыточных требований к малому бизнесу, так и неоправданной снисходительности к высокотехнологичным корпорациям.

Вариант 2. Модификация договорного регулирования. Следует включить в трудовые договоры и соглашения о конфиденциальности (NDA) специальные «ИИ-оговорки». Необходимо явным образом информировать контрагента и сотрудника о применении систем мониторинга и анализа на базе

ИИ, целях их использования и основных принципах работы (принцип transparency-by-design/спроектированная приватность). Принцип означает, что защита данных должна быть заложена на самых ранних этапах разработки информационных систем и бизнес-процессов. Это не дополнительная опция или поздняя доработка, а неотъемлемая часть изначальной концепции программы для ЭВМ.

Следует подготовить с помощью локально-нормативных актов или соглашений процедуру, которая будет определять порядок обжалования автоматических решений системы, например, блокировки доступа сотруднику или контрагенту, и оценки оснований для привлечения их к дисциплинарной и гражданско-правовой ответственности; прописывать распределение ответственности между сторонами в случае, если утечка произошла вследствие сбоя алгоритма, за который отвечает одна из сторон, обладатель ноу-хау или третье лицо в лице разработчика программного обеспечения.

Вариант 3. Развитие деликтных конструкций. Полагаем, что может возникнуть правовой аспект, где требуется адаптация норм о причинении вреда (гл. 59 ГК РФ) к ситуации, когда вред причинен в результате функционирования ИИ-системы охраны. Целесообразно рассмотреть введение механизма воздействия на владельца системы. Если он докажет, что вред (например, ложное обвинение сотрудника или контрагента) наступил вследствие вины разработчика или иного лица, ответственного за функционирование данной системы, он сможет предъявить регрессное требование. Это стимулирует владельцев ноу-хау к выбору надежных и сертифицированных решений.

Вариант 4. Создание стандартов «доверенного ИИ» для охраны секретов производства. На уровне регулирующих органов (Минцифры и Роскомнадзор) совместно с бизнес- и научным сообществом могут быть разработаны рекомендательные стандарты по архитектуре мягкого права, алгоритмической прозрачности explainable ИИ. Данный подход к созданию систем искусственного интеллекта предполагает создание организационных и

технических мер, позволяющих должностным лицам понимать и проверять, как именно ИИ приходит к своим выводам. Следование таким стандартам будет служить весомым доказательством принятия «разумных мер» в суде.

Наиболее эффективным представляется комплексный подход, сочетающий все четыре варианта. Доктрина задаст общие принципы, договоры обеспечат конкретику в отношениях, деликтное право распределит риски, а стандарты сформируют технологический базис для исполнения правовых норм.

Результаты исследования позволяют утверждать, что интеграция технологий искусственного интеллекта в процессы охраны служебных секретов производства не является лишь техническим усовершенствованием. Это вызов, требующий глубокого переосмысления ряда устоявшихся гражданско-правовых категорий. Выявленное противоречие между технологической необходимостью и правовой неопределенностью носит системный характер и не может быть разрешено только в рамках существующей правоприменительной практики.

Необходимость дальнейшего научного исследования данной темы обусловлена следующими факторами.

Опережающий характер развития технологий приводит к тому, что право рискует постоянно отставать от практики, вырабатывая решения постфактум, после масштабных инцидентов. Потенциальное исследование позволяет смоделировать риски и предложить новые правовые механизмы.

Также компании, инвестирующие в дорогостоящие ИИ-системы защиты, нуждаются в понятных правовых рамках, т.к. отсутствие таковых сдерживает инновации и создает правовые риски, обесценивающие сами инвестиции.

Актуальный глобальный контекст приводит к конкуренции в сфере высоких технологий и делает защиту ноу-хау вопросом технологической безопасности, т.к. развитие адекватного правового сопровождения для самых современных средств защиты становится стратегической задачей.

Заключение

Таким образом, дальнейшая научная разработка предложенных вариантов решения (разработка модельных положений для договоров, проектов поправок в федеральное законодательство, детализация стандартов «разумных мер с использованием ИИ») является не только академически значимой, но и практически востребованной. Это исследование будет способствовать формированию гармоничного правового поля, где инновационные технологии будут реализовывать свой потенциал для охраны ключевых активов цифровой экономики, не создавая при этом непреодолимых правовых рисков для участников отношений.

Список источников

1. Гаврилов Э.П. Гражданско-правовая защита и охрана секретов производства и коммерческой тайны / Э.П. Гаврилов // Хозяйство и право. – 2014. – №. 7. – С. 41–56.
2. Дозорцев В.А. Понятие секрета производства (ноу-хау) / В.А. Дозорцев // Вестник Высшего Арбитражного Суда Российской Федерации. – 2001. – №. 8. – С. 105–119.
3. Мухамедшин И.С. Основы правовой охраны интеллектуальной собственности по законодательству Российской Федерации // Вестник Северо-Восточного федерального университета имени МК Аммосова. Vestnik of North-Eastern Federal University. Серия «Общественные науки. Social science». – 2021. – № 3. – С. 5–10.
4. Нестерова Н.В. Служебное ноу-хау: проблемы взаимоотношений работника и работодателя // Копирайт (Вестник Академии интеллектуальной собственности). – 2016. – №. 4. – С. 64–77.
5. Бахтеев Д.В. Искусственный интеллект: этико-правовые основы: Монография. – Москва: Проспект, 2021.

References

1. Gavrilov E.P. Civil law protection and protection of production secrets and trade secrets. *Economy and law*. 2014. No. 7. Pp. 41–56 (in Russ.).

2. Dozortsev V.A. The concept of the secret of production (know-how). *Bulletin of the Supreme Arbitration Court of the Russian Federation.* 2001. No. 8. Pp. 105–119 (in Russ.).

3. Mukhamedshin I.S. Fundamentals of legal protection of intellectual property under the legislation of the Russian Federation. *Vestnik of North-Eastern Federal University=Bulletin of the Northeastern Federal University named after MK Ammosov*. The series Social Sciences. Social science. 2021. No. 3. Pp. 5–10 (in Russ.).

4. Nesterova N.V. Service know-how: problems of employee-employer relations. *Copyright. Bulletin of the Russian Academy of Intellectual Property.* 2016. No. 4. Pp. 64–77 (in Russ.).

5. Bakhteev D.V. Artificial intelligence: ethical and legal foundations. The monograph. *Prospekt Publishing House*, 2021 (in Russ.).

Статья поступила 27.12.2025, принята к публикации: 25.02.2026.