Политика и регламент использования ИИ при разработке программного обеспечения

Образец локального нормативного акта для компании-разработчика

Опубликовано: август 2026
Источник: внутренний документ Вебформата, обезличенный для публикации.

> **Как пользоваться этим образцом.** Это рабочий документ из практики одной студии, а не юридическая консультация. Структура и логика проверены на реальном производстве, но формулировки об ответственности, перечень инструментов и ссылки на внутренние документы вы заполняете под свою компанию. Перед введением приказом покажите готовый текст своему юристу: у вас другой трудовой договор, другие клиенты и другие поручения на обработку данных.

Места, которые заполняются под себя, помечены как `<...>`.

Документ состоит из двух частей с разным статусом.

- **Часть I - Политика.** Обращение с данными, перечни инструментов, ответственность за код, права на результат. Нарушение считается нарушением трудовых обязанностей, последствия - в разделе 12.
- **Часть II - Регламент.** Порядок работы разработчика с ИИ на конкретной задаче: описание, план, шаги, проверка, разборы. Соблюдение проверяется на ревью и на ежемесячном разборе. Дисциплинарные меры применяются только за систематическое неисполнение после письменных замечаний (пункт 12.4).

Зачем этот документ. Не запретить ИИ, а сделать так, чтобы разработчик управлял ИИ, понимал результат и отвечал за качество продукта. Использование ИИ-инструментов в рамках разрешённого перечня допускается и поощряется.

ЧАСТЬ I. ПОЛИТИКА

1. Общие положения

1.1. Сфера применения

Настоящая Политика устанавливает правила использования инструментов искусственного интеллекта (далее - ИИ-инструменты) при выполнении работниками `<наименование организации>` (далее - Работодатель) трудовых обязанностей, связанных с созданием, изменением, отладкой, проверкой, документированием программного кода, а также с обработкой данных клиентов в проектах автоматизации.

Политика распространяется на всех работников, имеющих в трудовых обязанностях разработку, проектирование, тестирование или сопровождение программного обеспечения, а также на работников, работающих с данными клиентов через ИИ-инструменты вне разработки.

1.2. Цели Политики

1. Обеспечить качество и безопасность исходного кода, передаваемого клиентам Работодателя.
2. Защитить персональные данные клиентов и данные, составляющие коммерческую тайну, при использовании ИИ-инструментов.
3. Зафиксировать персональную ответственность работника за результат своей работы независимо от способа создания.
4. Соблюсти требования законодательства Российской Федерации о персональных данных, коммерческой тайне, авторском праве на служебные произведения.
5. Задать единый порядок работы с ИИ на задаче, при котором решения принимает человек, а результат проверяем и объясним.

1.3. Нормативная основа

Политика разработана с учётом требований:

- Трудового кодекса Российской Федерации (статьи 21, 22, 70, 71, 81, 192, 243);
- Гражданского кодекса Российской Федерации (статья 1295 - служебные произведения);
- Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных";
- Федерального закона от 29.07.2004 № 98-ФЗ "О коммерческой тайне";
- Уголовного кодекса Российской Федерации (статьи 183, 272, 272.1);
- внутренних документов Работодателя: Положения о коммерческой тайне, Политики обработки персональных данных, Правил внутреннего трудового распорядка.

2. Термины и определения

ИИ-инструмент - программный продукт или сервис, использующий генеративные модели искусственного интеллекта для создания, изменения, анализа или проверки исходного кода, документации, текстов, изображений или иных результатов интеллектуальной деятельности. Включает интегрированные среды разработки с ИИ-помощником (Cursor, GitHub Copilot, Claude Code), чат-интерфейсы (Claude.ai, ChatGPT, GigaChat), API крупных языковых моделей, локально развёрнутые модели.

ИИ-агент - программная сущность, способная автономно выполнять последовательность действий в рабочей среде Работодателя (запуск кода, изменение файлов, обращение к внешним системам) на основании инструкций пользователя или предварительно заданных правил.

Корпоративная учётная запись - учётная запись ИИ-сервиса, оформленная на юридическое лицо Работодателя или приобретённая Работодателем для конкретного работника, с режимом приватности, исключающим использование передаваемых данных для дообучения моделей провайдером сервиса.

Личная учётная запись - учётная запись ИИ-сервиса, не оформленная на Работодателя, в том числе бесплатная или оплачиваемая работником самостоятельно.

Разрешённый перечень - перечень ИИ-инструментов, использование которых при выполнении трудовых обязанностей разрешено настоящей Политикой.

Запрещённый перечень - перечень действий с ИИ-инструментами, прямо запрещённых настоящей Политикой.

Клиентский код - исходный код, конфигурации, скрипты миграций, файлы окружения, дампы баз данных и иные технические артефакты, созданные Работодателем для клиента или полученные от клиента в рамках исполнения договора.

Персональные данные - определены статьёй 3 Федерального закона № 152-ФЗ.

Технический руководитель - работник, назначенный приказом директора ответственным за техническое качество разработки: ведёт разрешённый перечень, согласовывает подходы по сложным и критичным задачам, проводит ежемесячные разборы.

Карточка использования ИИ - короткая запись работника о том, как ИИ применялся на задаче. Форма - Приложение № 3.

3. Принципы использования ИИ-инструментов

3.1. Персональная ответственность за результат

Работник несёт полную профессиональную ответственность за качество, безопасность, корректность работы и соответствие требованиям заказчика всего исходного кода, который он коммитит в репозитории Работодателя или передаёт заказчику в любой иной форме, независимо от того, был ли указанный код полностью или частично создан с использованием ИИ-инструментов.

Признание факта использования ИИ-инструмента при создании кода (включая объяснения вида "так предложил Claude / Cursor / Copilot") **не является основанием** для освобождения работника от ответственности за дефекты кода, инциденты в проекте клиента, нарушения требований безопасности и иные последствия выполнения такого кода.

3.2. Верификация

Любой результат работы ИИ-инструмента (код, текст, рекомендация по архитектуре, ответ на вопрос о работе системы) подлежит проверке работником до его применения в работе. Работник обязан:

- понимать, что делает каждая строка кода, которую он коммитит;
- проверять корректность вызовов внешних API (включая предотвращение использования несуществующих методов и параметров);
- проверять выполнение требований безопасности (валидация ввода, защита от SSRF, корректное закрытие соединений и сессий);

- проверять, что код не содержит конфиденциальных данных, оставленных ИИ-инструментом из общедоступных учебных корпусов.

Работник должен быть готов объяснить логику любого фрагмента переданного им кода без обращения к ИИ-инструменту.

3.3. Ключевые решения принимает человек

ИИ-инструмент предлагает, решение принимает работник или технический руководитель. К ключевым решениям относятся: архитектура и способ встраивания в существующую систему, выбор библиотек и внешних сервисов, структура базы данных и миграции, способ обработки и хранения данных, фоновые и отложенные механизмы, схема прав доступа.

Принятое решение работник должен уметь обосновать: какая задача решается, какие рассматривались альтернативы, почему выбран этот вариант. Для сложных и критичных задач обоснование фиксируется письменно (пункт 10.4).

3.4. Прозрачность использования

При создании запроса на слияние (Pull Request, Merge Request) работник указывает в описании факт существенного использования ИИ-инструмента при подготовке изменений, если изменения сгенерированы целиком или содержат существенные блоки, написанные ИИ-инструментом.

Цель указания - облегчить проверку коллегой, а не ограничить использование. Использование ИИ-инструмента по умолчанию допускается и поощряется в рамках разрешённого перечня.

Порядок и объём фиксации - в пункте 10.5 и Приложении № 3.

3.5. Защита данных

Работник не загружает в ИИ-инструменты данные, на загрузку которых отсутствует юридическое основание: персональные данные граждан Российской Федерации без выполнения требований раздела 5 настоящей Политики, информацию, составляющую коммерческую тайну Работодателя или его клиентов, без выполнения требований раздела 6 настоящей Политики.

4. Разрешённый и запрещённый перечни

4.1. Разрешённый перечень ИИ-инструментов

Перечень ниже - пример из практики студии, работающей с российскими клиентами. Заполняется под свой стек и свои подписки. Смысл не в конкретных названиях, а в трёх колонках: инструмент, что им разрешено делать, на каком тарифе.

При условии использования через корпоративные учётные записи Работодателя:

Инструмент	Допустимая роль	Тариф или режим
Cursor (Teams или Enterprise)	Среда разработки с ИИ-помощником, повседневное использование	Корпоративная подписка с режимом приватности
Claude (Anthropic) через корпоративную подписку Pro/Max или API	Чат-интерфейс для разработки, проверка кода, объяснения кода	Корпоративная учётная запись или API-ключ Работодателя
Claude Code	Командная строка с ИИ-агентом для разработки	Через корпоративную учётную запись
GitHub Copilot Business	Автодополнение и ИИ-чат в среде разработки	Корпоративная подписка
GigaChat for Business (Сбер)	Чат-интерфейс и API, в том числе для проектов с персональными данными граждан РФ	Корпоративная учётная запись
YandexGPT (Yandex Cloud)	API и чат-интерфейс, в том числе для проектов с персональными данными граждан РФ	Корпоративная учётная запись
Локально развёрнутые открытые модели (Llama, Mistral, Qwen, прочие)	Любые задачи, при условии корректного развёртывания на инфраструктуре Работодателя или клиента	Внутренняя инфраструктура

Перечень изменяется приказом директора. Работник, желающий использовать инструмент вне перечня, направляет письменное уведомление техническому руководителю (раздел 8).

4.2. Запрещённый перечень действий

Работнику запрещено:

1. Загружать клиентский код, конфигурации, секреты, токены доступа, ключи API, файлы окружения, дампы баз данных или их фрагменты в **личные учётные записи** ChatGPT, Claude.ai, Gemini, DeepSeek, Mistral Le Chat, Perplexity и иных ИИ-сервисов, в том числе бесплатных.
2. Загружать персональные данные клиентов и третьих лиц в зарубежные ИИ-сервисы без выполнения требований раздела 5 настоящей Политики.
3. Публиковать фрагменты клиентского кода в публичных чатах, форумах, на платформах вопросов и ответов с целью получения помощи от ИИ-сервисов или от иных пользователей.
4. Использовать ИИ-инструменты для обхода контроля доступа, аудита, ревью кода, иных мер обеспечения качества и безопасности, установленных Работодателем или клиентом.
5. Передавать корпоративные учётные записи ИИ-сервисов третьим лицам, использовать их вне трудовых обязанностей, публиковать API-ключи Работодателя.
6. Подавать как результат собственного авторского труда (в портфолио, на собеседованиях, в публикациях) код, существенная часть которого создана ИИ-инструментом, без явного указания на это.

7. Заявлять заказчику о применении в проекте ИИ-инструментов, использование которых не было предварительно согласовано с директором или техническим руководителем.

4.3. Особый режим: ИИ-агенты в автономном режиме

Использование ИИ-агентов в автономном режиме (Claude Code agent mode, Copilot cloud agent, аналогичные функции с автоматическим запуском кода и изменением файлов без подтверждения каждого действия) допускается **только** при выполнении совокупности условий:

- запуск производится в изолированной среде (отдельная ветка репозитория, отдельный контейнер, песочница), не допускающей прямого изменения основной ветки и продуктивных сред;
- перед слиянием результатов работы агента в основную ветку проводится обязательное ревью человеком;
- в описании запроса на слияние указано использование ИИ-агента и приведены параметры запуска;
- подключение MCP-серверов к рабочей среде, содержащей доступы к продуктивным системам клиентов, требует предварительного согласования с техническим руководителем.

Отдельно запрещено давать ИИ-агенту доступ к продуктивной среде клиента с правами на изменение данных без присутствия работника, контролирующего каждое действие.

4.4. Ограничения со стороны клиента

Если договор с клиентом, его политика безопасности или поручение на обработку данных ограничивают либо запрещают использование ИИ-инструментов, приоритет имеет требование клиента.

Перечень проектов с такими ограничениями ведёт технический руководитель и доводит до работников, занятых на этих проектах, до начала работ. Работник, увидевший подобное условие в договоре или переписке с клиентом, сообщает о нём техническому руководителю.

---

5. Особый режим: персональные данные граждан Российской Федерации

5.1. Базовое правило

Работник, занятый на проектах, в рамках которых обрабатываются персональные данные граждан Российской Федерации (включая клиентов клиентов Работодателя - субъектов персональных данных в проектах автоматизации и в собственных продуктах Работодателя), обязан соблюдать ограничения, установленные:

- Федеральным законом № 152-ФЗ;
- поручением на обработку персональных данных, заключённым между Работодателем и клиентом по конкретному проекту;
- настоящей Политикой;
- Политикой обработки персональных данных Работодателя.

5.2. Ограничения на передачу персональных данных в ИИ-инструменты

Передача персональных данных граждан Российской Федерации в ИИ-инструменты допускается при соблюдении совокупности условий:

1. Передача предусмотрена поручением на обработку персональных данных от клиента или согласием субъекта.
2. ИИ-инструмент использует серверы на территории Российской Федерации (GigaChat for Business, YandexGPT) **или** трансграничная передача данных в страну размещения сервиса осуществляется с соблюдением статьи 12 ФЗ-152 (уведомление Роскомнадзора, согласие субъекта на трансграничную передачу с указанием страны).
3. Передача регистрируется в журнале обработки персональных данных.

5.3. Архитектурное правило для проектов с ИИ-чат-ботами

В проектах, где ИИ-чат-бот или ИИ-агент работает с обращениями граждан Российской Федерации, проектное решение по умолчанию предусматривает:

1. Первичный сбор и хранение данных на серверах в Российской Федерации (пункт 1 части 5 статьи 18 ФЗ-152).
2. Обезличивание персональных данных перед отправкой в API крупных языковых моделей при использовании моделей вне Российской Федерации.
3. Журналирование всех запросов к ИИ-инструменту с привязкой к субъекту персональных данных и оператору, поручившему обработку.
4. Использование российских моделей (GigaChat, YandexGPT) в качестве основной модели, иные модели - как дополнительные при наличии оснований для трансграничной передачи.

Отклонения от указанного правила допускаются только по согласованию с директором и при наличии подтверждённого юридического основания.

5.4. Запрет загрузки персональных данных в личные учётные записи

Работнику категорически запрещено направлять персональные данные субъектов в личные учётные записи ИИ-сервисов вне зависимости от формы (текст, скриншот таблицы, фрагмент дампа базы данных, лог системы, переписка с клиентом). Нарушение настоящего пункта квалифицируется как нарушение требований обработки персональных данных, влечёт дисциплинарную ответственность по разделу 12 настоящей Политики и может повлечь ответственность по части 1 статьи 13.11 КоАП РФ либо уголовную ответственность по статье 272.1 УК РФ.

6. Особый режим: коммерческая тайна

6.1. Информация, составляющая коммерческую тайну

Перечень информации, составляющей коммерческую тайну Работодателя и (или) клиентов Работодателя, утверждается отдельным документом - Перечнем сведений, составляющих коммерческую тайну. К таким сведениям относятся, в частности:

- исходные коды программного обеспечения клиентов;
- архитектурные решения и проектная документация;
- конфигурационные файлы продуктивных сред;
- учётные данные, токены доступа, ключи API;
- финансовые показатели Работодателя;
- сведения о клиентах, в том числе условия договоров, перечень используемых клиентом систем.

6.2. Запрет передачи в ИИ-инструменты вне разрешённого перечня

Передача информации, составляющей коммерческую тайну, в ИИ-инструменты, не входящие в разрешённый перечень (пункт 4.1), запрещена. Передача в инструменты разрешённого перечня допускается только в объёме, необходимом для выполнения трудовых обязанностей.

6.3. Учёт лиц, имеющих доступ

Работник, получающий доступ к информации, составляющей коммерческую тайну, до начала работы знакомится под роспись с Положением о коммерческой тайне, Перечнем сведений, подписывает соглашение о неразглашении. Журнал учёта допущенных лиц ведёт ответственный за обработку коммерческой тайны.

7. Права на результат и лицензионная чистота

7.1. Код, созданный работником при выполнении трудовых обязанностей, является служебным произведением (статья 1295 ГК РФ). Использование ИИ-инструмента при создании кода не меняет порядок перехода прав к Работодателю и не создаёт прав у провайдера ИИ-сервиса.

7.2. Работник обязан не допускать попадания в передаваемый клиенту код фрагментов, воспроизводящих чужие произведения с несовместимыми условиями лицензии. ИИ-инструмент может воспроизвести узнаваемый фрагмент открытого кода: при появлении в ответе крупного самостоятельного блока (алгоритм, класс, модуль) работник проверяет его происхождение до включения в проект.

7.3. Подключение в проект внешней библиотеки, предложенной ИИ-инструментом, допускается после проверки её лицензии на совместимость с условиями договора с клиентом. Проверка лицензии - часть решения о выборе библиотеки (пункт 3.3).

7.4. Если договор с клиентом содержит требования к происхождению кода или к раскрытию использования ИИ, работник выполняет их и сообщает о таких требованиях техническому руководителю.

8. Порядок добавления нового ИИ-инструмента в разрешённый перечень

8.1. Работник, считающий целесообразным использовать ИИ-инструмент, не входящий в разрешённый перечень, направляет техническому руководителю письменное уведомление по форме, приведённой в Приложении № 2 к настоящей Политике.

8.2. Уведомление содержит:

- наименование инструмента, наименование провайдера, страна размещения серверов;
- предполагаемая цель использования и категории задач;
- категории данных, которые предполагается обрабатывать;
- наличие или отсутствие корпоративного тарифа с режимом приватности;
- сведения о соответствии требованиям ФЗ-152 при предполагаемом использовании.

8.3. Технический руководитель рассматривает уведомление в течение 7 рабочих дней, при необходимости консультируется с директором, ответственным за обработку персональных данных, юристом. Решение направляется работнику в письменной форме (включая электронную).

8.4. Использование инструмента до получения положительного решения не допускается.

ЧАСТЬ II. РЕГЛАМЕНТ РАБОТЫ РАЗРАБОТЧИКА С ИИ

9. Категории задач

9.1. Категории

Категория задачи определяется до начала работы и записывается в задаче.

Простая. Изолированное изменение с наглядным результатом, откат в одно действие. Правка текста, стилей, метатегов, параметра, починка в одном месте. Не затрагивает структуру данных, права доступа, деньги, интеграции.

Обычная. Новая функция или доработка в пределах одного модуля. Может менять поведение системы для пользователя, но не меняет структуру данных и не затрагивает внешние системы.

Сложная. Затрагивает несколько модулей, меняет структуру базы данных, добавляет или меняет интеграцию с внешней системой, вводит фоновые и отложенные механизмы, требует миграции данных.

Критичная. Задача, ошибка в которой видна клиенту клиента или стоит денег. К критичным относятся: приём и учёт платежей, персональные данные, права доступа и авторизация, работа в продуктивной

среде клиента, обмен с учётными системами (1С и аналогичные), массовые операции над данными, рассылки и любые исходящие сообщения от имени клиента.

При сомнении между двумя категориями берётся более высокая.

9.2. Требования по категориям

Требование	Простая	Обычная	Сложная	Критичная
Описание задачи работником до работы с ИИ (10.1)	не требуется	да	да	да
Запрос у ИИ плана и рисков до кода (10.2)	по усмотрению	да	да	да
Согласование подхода с техническим руководителем до кода (10.4)	нет	нет	да	да, с альтернативами
Карточка использования ИИ (10.5)	нет	да, кратко	да	да
Письменный план проверки (10.6)	нет	да	да	да, включая проверку на копии данных клиента
Ревью кода (10.7)	обычное	обычное	ревью с проверкой понимания	ревью технического руководителя

9.3. Кто присваивает категорию

Категорию присваивает работник при взятии задачи в работу. Технический руководитель вправе её изменить. Если категория меняется по ходу работы (выяснилось, что задача затрагивает платежи или структуру базы), работник останавливается, меняет категорию и выполняет требования новой категории.

10. Порядок работы над задачей

10.1. Описание задачи до обращения к ИИ

До обращения к ИИ работник сам описывает задачу. В описании:

- что делаем;
- зачем, какой результат у клиента или пользователя;
- что в задачу не входит;
- какие части системы затрагиваются;
- какие есть риски;
- как планируется проверять результат.

Описание пишется в задаче. Если работник не может описать задачу сам, это признак того, что задача не понята: следует уточнить постановку у технического руководителя или у автора задачи, а не поручать её понимание ИИ.

10.2. Постановка задачи ИИ-инструменту

Задача в формате "сделай фичу" ИИ-инструменту не ставится. Работник даёт:

- контекст проекта: что за система, где живёт код, какие соглашения приняты;
- ограничения: чего делать нельзя, какие библиотеки и подходы уже используются, что нельзя ломать;
- границы задачи: что не входит.

Первым запросом запрашивается **план, риски и варианты решения**, а не готовый код. Работник разбирает предложенный план, отклоняет неподходящее и только затем переходит к коду.

10.3. Маленькие шаги

Большая задача целиком ИИ-инструменту не поручается. Задача разбивается на понятные части; после каждой существенной части работник сам проверяет результат: читает изменения, запускает, сверяет с описанием задачи.

Признак нарушения этого пункта - объёмный запрос на слияние, содержимое которого работник не разбирал построчно.

10.4. Предварительное согласование (сложные и критичные задачи)

До написания кода работник коротко объясняет техническому руководителю:

- задачу и её границы;
- риски;
- выбранный подход;
- какие альтернативы рассматривались и почему отклонены;
- как будет проверять результат.

Формат - разговор на 10-15 минут или письменное сообщение. Итог фиксируется в задаче: подход согласован, дата, что решили. Для критичных задач альтернативы приводятся обязательно: вариант без альтернатив к согласованию не принимается.

Технический руководитель отвечает в течение одного рабочего дня. Если ответа нет, работник поднимает вопрос директору, а не начинает работу без согласования.

10.5. Фиксация использования ИИ

Работник фиксирует, как использовал ИИ на задаче. Кратко:

- для чего использовался ИИ;
- какие ограничения были даны;

- что ИИ предложил;
- что принято;
- что отвергнуто и почему;
- что проверено вручную.

Место записи: описание запроса на слияние. Если задача выполнялась без кода (конфигурация, настройка, разбор данных) - комментарий в задаче. Форма - Приложение № 3.

Запись нужна проверяющему, а не для отчёта: она показывает, где искать слабые места, и экономит время на ревью.

10.6. План проверки перед сдачей

Задача не сдаётся без плана проверки. Проверяются не только идеальные сценарии, но и:

- ошибки и некорректный ввод;
- нестандартные и граничные случаи (пустые данные, максимальные объёмы, одновременная работа нескольких пользователей);
- повторный запуск: что будет, если операция выполнится дважды;
- права доступа: что видит и что может пользователь с меньшими правами;
- работа с данными: что происходит с уже накопленными данными, нужна ли миграция и обратима ли она;
- влияние на старое поведение: что могло сломаться в соседних местах.

Для критичных задач проверка выполняется на копии данных клиента, а не только на пустой тестовой базе.

Результат проверки записывается в задачу: что проверял, как, что получилось. Чек-лист - Приложение № 4.

10.7. Ревью

Ревью кода остаётся обязательным и не является единственным контролем. При ревью смотрят не только код, но и:

- как работник понял задачу;
- какие ограничения дал ИИ;
- какие решения принял сам и чем их обосновывает;
- чем подтверждено качество результата.

Проверяющий вправе задать вопрос по любому фрагменту кода и ожидать объяснения без обращения к ИИ. Ответ вида "так предложил ИИ" ответом не считается и является основанием вернуть задачу на доработку.

11. Разборы и обратная связь

11.1. Ежемесячный разбор

Раз в месяц технический руководитель разбирает с каждым разработчиком одну реальную задачу целиком: от постановки до результата. Смотрят описание задачи, работу с ИИ, принятые решения, отвергнутые предложения, проверки и итоговый код.

Задачу для разбора выбирает технический руководитель. Длительность - до одного часа.

11.2. Зоны роста

По итогам разбора для каждого разработчика письменно фиксируются 1-2 конкретные зоны роста. Например: подробнее описывать риски, глубже проверять нестандартные случаи, не принимать архитектуру от ИИ без анализа альтернатив.

Зоны роста проверяются на следующем разборе.

11.3. Сводка директору

Технический руководитель ежемесячно направляет директору короткую сводку по команде: основные риски, повторяющиеся ошибки, кому нужна помощь, где нужен более сильный контроль, какие правила процесса нужно доработать.

Сводка касается процесса и рисков, а не оценки личных качеств работников.

11.4. Тревожные признаки

Отдельно фиксируются признаки неправильной работы с ИИ:

- ответы вида "так предложил ИИ" при разборе кода;
- непонимание работником собственного кода;
- отсутствие альтернатив при выборе решения;
- отсутствие проверок нестандартных случаев;
- регулярные ошибки, обнаруженные после выпуска.

Обнаружение таких признаков не является дисциплинарным нарушением само по себе. Технический руководитель применяет рабочие меры: все задачи работника временно проходят предварительное согласование независимо от категории, назначается парная работа над ближайшей сложной задачей, назначается повторный разбор через месяц.

Если признаки сохраняются после двух разборов, вопрос выносится директору.

ЧАСТЬ III. ОТВЕТСТВЕННОСТЬ И ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12. Ответственность за нарушение

12.1. Дисциплинарная ответственность

Нарушение Части I настоящей Политики является нарушением трудовых обязанностей и влечёт дисциплинарную ответственность в соответствии со статьями 192, 193 Трудового кодекса Российской Федерации.

В зависимости от тяжести нарушения и наступивших последствий применяются: замечание, выговор, увольнение по основаниям, предусмотренным Трудовым кодексом Российской Федерации.

Основания для расторжения трудового договора за однократное грубое нарушение (в частности, за разглашение охраняемой законом тайны, ставшей известной работнику в связи с выполнением трудовых обязанностей) предусмотрены статьёй 81 Трудового кодекса Российской Федерации. Конкретную формулировку этого абзаца согласуйте с юристом: она должна опираться на ваш трудовой договор, Положение о коммерческой тайне и режим коммерческой тайны, фактически введённый в организации. Без введённого режима ссылаться на разглашение коммерческой тайны нельзя.

12.2. Материальная ответственность

В случае причинения Работодателю прямого действительного ущерба вследствие нарушения настоящей Политики работник несёт материальную ответственность в порядке, установленном главой 39 Трудового кодекса Российской Федерации, в том числе полную материальную ответственность по основаниям, предусмотренным статьёй 243 Трудового кодекса Российской Федерации (включая разглашение охраняемой законом тайны - пункт 7 части первой статьи 243).

12.3. Иная ответственность

За действия, образующие состав административного правонарушения или преступления, работник несёт ответственность в соответствии с законодательством Российской Федерации, в том числе:

- по статье 13.11 Кодекса Российской Федерации об административных правонарушениях - за нарушение законодательства о персональных данных;
- по статье 183 Уголовного кодекса Российской Федерации - за незаконное получение и разглашение сведений, составляющих коммерческую тайну;
- по статье 272.1 Уголовного кодекса Российской Федерации - за неправомерное использование, передачу, сбор и хранение персональных данных.

Привлечение к дисциплинарной и материальной ответственности по настоящему разделу не освобождает работника от ответственности по иным основаниям.

12.4. Неисполнение требований Части II

Разовое несоблюдение требований Части II (не описана задача, не зафиксировано использование ИИ, нет плана проверки) устраняется в рабочем порядке: задача возвращается на доработку, недостающее дополняется, случай разбирается на ежемесячном разборе.

Систематическое неисполнение требований Части II после двух письменных замечаний технического руководителя рассматривается как ненадлежащее исполнение работником трудовых обязанностей с последствиями по пункту 12.1.

Правила Части II вводятся как стандарт работы, а не как мера наказания.

13. Заключительные положения

13.1. Настоящий документ вводится в действие приказом директора Работодателя.

13.2. Работник знакомится с документом под роспись до начала выполнения трудовых обязанностей, связанных с разработкой программного обеспечения. Лист ознакомления приведён в Приложении № 1.

13.3. Документ подлежит пересмотру не реже одного раза в год либо при существенных изменениях законодательства Российской Федерации, появлении новых классов ИИ-инструментов, изменении состава клиентов и проектов Работодателя.

13.4. Изменения в разрешённый перечень ИИ-инструментов и Перечень сведений, составляющих коммерческую тайну, вносятся приказом директора без полного пересмотра документа.

13.5. Изменения в Часть II (порядок работы на задаче) вносятся приказом директора по предложению технического руководителя, в том числе по итогам ежемесячных сводок (пункт 11.3).

13.6. Вопросы, не урегулированные настоящим документом, решаются в соответствии с законодательством Российской Федерации, иными локальными нормативными актами Работодателя.

Приложение № 1. Лист ознакомления

С Политикой и регламентом использования ИИ при разработке программного обеспечения `<наименование организации>` ознакомлен(а), требования понятны, обязуюсь соблюдать.

ФИО работника	Должность	Дата	Подпись

Приложение № 2. Форма уведомления о предполагаемом использовании ИИ-инструмента вне разрешённого перечня

Техническому руководителю
`<наименование организации>`
от _____ (ФИО, должность работника)

Уведомление

Прошу рассмотреть возможность использования ИИ-инструмента, не входящего в разрешённый перечень, на следующих условиях:

1. Наименование инструмента: _____
2. Наименование провайдера: _____
3. Страна размещения серверов: _____
4. Сайт инструмента: _____
5. Цель использования (категории задач): _____
6. Предполагаемые категории обрабатываемых данных:
   - персональные данные граждан РФ: да / нет;
   - сведения, составляющие коммерческую тайну: да / нет;
   - данные клиентов: да / нет.
7. Наличие корпоративного тарифа с режимом приватности: ___
8. Соответствие ФЗ-152 при предполагаемом использовании: ___

Дата: _____
Подпись работника: _____

Решение технического руководителя: _____
Дата: _____
Подпись: _____

Приложение № 3. Карточка использования ИИ

Заполняется в описании запроса на слияние или комментарием в задаче. 5-10 строк, без пересказа переписки с ИИ.

```
Категория задачи: простая / обычная / сложная / критичная
Инструмент: (Cursor, Claude Code, Copilot, ...)

Для чего использовал ИИ:
Какие ограничения дал:
Что ИИ предложил:
Что принял:
Что отверг и почему:
Что проверил руками:
```

Пример:

```
Категория задачи: сложная
Инструмент: Claude Code

Для чего использовал ИИ: обмен заказами с 1С, разбор входящего формата
Какие ограничения дал: не менять структуру таблицы заказов, не трогать
  очередь, использовать существующий класс обмена
Что ИИ предложил: отдельная таблица очереди и перенос обмена на неё
Что принял: разбор входящего формата, обработку ошибок формата
Что отверг: отдельную таблицу очереди - ломает существующий обмен,
  согласовано с техническим руководителем 14.08
Что проверил руками: повторная загрузка того же файла, битый файл,
  файл с 5000 позиций, откат миграции
```

Приложение № 4. Чек-лист плана проверки

- [ ] Основной сценарий работает и совпадает с описанием задачи
- [ ] Ошибки и некорректный ввод обработаны, сообщения понятны
- [ ] Граничные случаи: пусто, ноль, максимальный объём, одновременная работа
- [ ] Повторный запуск не портит данные и не создаёт дублей
- [ ] Права доступа: проверено под пользователем с меньшими правами
- [ ] Данные: что стало с накопленными данными, миграция обратима
- [ ] Старое поведение: соседние места не сломались
- [ ] Логи и мониторинг: ошибка будет видна, а не потеряется молча
- [ ] Для критичной задачи: проверено на копии данных клиента
- [ ] Результат проверки записан в задачу

Приложение № 5. Памятка работнику (рекомендуется к раздаче отдельно)

Можно:

- работать с инструментами из разрешённого перечня (пример: Cursor, Claude через корпоративную учётную запись, GitHub Copilot Business, GigaChat for Business, YandexGPT) - в рамках трудовых задач;
- использовать ИИ для написания кода, объяснения чужого кода, написания тестов, документирования, проверки кода;

- запускать ИИ-агентов в изолированных ветках с обязательным ревью перед слиянием.

Нельзя:

- кидать клиентский код, токены, конфигурации, дампы базы в личный ChatGPT, Claude.ai или иной личный аккаунт;
- кидать персональные данные граждан РФ в зарубежные ИИ-сервисы;
- ссылаться на "это ИИ написал" как на оправдание дефекта кода - отвечает работник, который коммитит;
- публиковать фрагменты клиентского кода в публичных чатах и форумах.

Порядок на задаче:

1. Определи категорию: простая, обычная, сложная, критичная.
2. Опиши задачу сам: что, зачем, что не входит, что затрагиваем, риски, как проверю.
3. Сложная или критичная - согласуй подход с техническим руководителем до кода.
4. Дай ИИ контекст и ограничения, попроси сначала план и риски, потом код.
5. Иди маленькими шагами, после каждого проверяй сам.
6. Заполни карточку использования ИИ.
7. Пройди чек-лист проверки, запиши результат в задачу.

Сомневаешься - спроси технического руководителя до отправки данных.

Откуда взялся этот документ

Собран в августе 2026 из двух независимых текстов: правового черновика (обращение с данными, перечни инструментов, ответственность) и процессного регламента, который написал разработчик, разбиравший реальные ошибки в работе команды с ИИ.

Несущее решение - две части с разным статусом. Если смешать правовые требования с процессными в один список, получается, что за незаполненное поле в описании задачи формально положен выговор. Так документы не соблюдают: их перестают выполнять целиком. Поэтому обращение с данными - это дисциплинарная ответственность, а порядок работы на задаче - основание вернуть задачу на доработку и тема для ежемесячного разбора.

Документ можно брать за основу, менять под себя и вводить у себя. Ссылка на источник приветствуется, но не обязательна.