rocket lab

команда роста на аутсорсе
для системного улучшения ключевых метрик

Шаблон регламента использования ИИ в компании

Готовый шаблон внутреннего документа для безопасного и эффективного внедрения ИИ-инструментов

Введение: Цели и область применения

Настоящий Регламент определяет правила и процедуры использования систем искусственного интеллекта (ИИ) сотрудниками ООО «[Название компании]» (далее — Компания).

Цели Регламента:

* Обеспечение безопасного и этичного использования ИИ-инструментов.

* Снижение юридических, репутационных и операционных рисков, связанных с использованием ИИ.

* Защита конфиденциальных данных Компании и персональных данных клиентов/сотрудников.

* Содействие эффективному внедрению ИИ для повышения производительности и инноваций.

* Обеспечение соответствия требованиям законодательства, включая будущие нормы, такие как EU AI Act, который предусматривает штрафы до 35 млн евро или 7% годового мирового оборота за нарушение запрещенных практик (LBKP Legal, 2025).

Область применения:

Регламент распространяется на всех сотрудников Компании, использующих ИИ-инструменты в рамках своей профессиональной деятельности, а также на внешних подрядчиков и консультантов, работающих с данными Компании.

Основные понятия

Искусственный интеллект (ИИ)	Совокупность технологий, позволяющих компьютерным системам имитировать когнитивные функции человека, такие как обучение, рассуждение, принятие решений и понимание естественного языка.
Большие языковые модели (LLM)	Разновидность ИИ, обученная на огромных объемах текстовых данных и способная генерировать, обрабатывать и понимать человеческий язык (например, YandexGPT, GigaChat, ChatGPT).
Конфиденциальные данные	Информация, доступ к которой ограничен законодательством или внутренними политиками Компании (коммерческая тайна, ноу-хау, финансовые данные, стратегии). Разглашение такой информации может нанести ущерб Компании.

Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (ФИО, паспортные данные, адрес, телефон, email).
Промпт	Текстовый запрос или инструкция, подаваемая пользователем ИИ-системе для получения желаемого результата.

Принципы использования ИИ

- ☐ Ответственность и контроль человека (Human-in-the-loop)

  ИИ является инструментом поддержки, а не заменой человеческого интеллекта. Все результаты работы ИИ должны быть проверены и одобрены человеком перед использованием или публикацией. ИИ не должен принимать критические решения без участия человека.

- ☐ Конфиденциальность и защита данных

  Строго запрещено вводить конфиденциальные данные Компании, персональные данные клиентов или сотрудников в публичные ИИ-сервисы. Используйте только одобренные Компанией ИИ-инструменты и соблюдайте правила работы с данными.

- ☐ Соблюдение авторских прав

  Сотрудники обязаны проверять генерируемый ИИ контент на предмет возможного нарушения авторских прав третьих лиц. Компания не несет ответственности за контент, созданный ИИ и опубликованный без надлежащей проверки.

- ☐ Прозрачность и этичность

  При использовании ИИ для создания контента, который может быть воспринят как человеческий, необходимо указывать на его ИИ-происхождение, если это может ввести в заблуждение или является требованием законодательства. Запрещено использовать ИИ для создания дискриминационного, оскорбительного или противозаконного контента.

- ☐ Обучение и повышение грамотности

  Компания обеспечивает обучение сотрудников по безопасному и эффективному использованию ИИ-инструментов. Согласно EU AI Act, работодатели обязаны обеспечить надлежащее обучение сотрудников, чтобы они могли безопасно использовать системы ИИ (LBKP Legal, 2025).

Разрешенные и запрещенные сценарии использования ИИ

Разрешенные сценарии (с проверкой человека)	Запрещенные сценарии
Генерация черновиков текстов (письма, отчеты, посты для соцсетей), описаний товаров/услуг.	Ввод конфиденциальных данных Компании (коммерческая тайна, финансовые отчеты, стратегии) в публичные ИИ-сервисы.
Резюмирование и перефразирование общедоступной информации, длинных документов (без конфиденциальных данных).	Ввод персональных данных клиентов или сотрудников (ФИО, контакты, паспортные данные) в публичные ИИ-сервисы.
Мозговой штурм, генерация идей, концепций, заголовков.	Принятие критических бизнес-решений (финансовые инвестиции, кадровые решения, юридические заключения) исключительно на основе ИИ без участия и одобрения человека.
Перевод текстов, проверка грамматики и стилистики.	Использование ИИ для создания дискриминационного, оскорбительного, клеветнического или противозаконного контента.
Автоматизация рутинных задач (например, классификация входящих писем, ответы на типовые вопросы клиентов через одобренные чат-боты).	Нарушение авторских прав третьих лиц, создание или распространение плагиата с помощью ИИ.

Разрешенные сценарии (с проверкой человека)	Запрещенные сценарии
Создание тестовых данных для разработки ПО.	Использование ИИ для манипуляций, дезинформации или обмана.
Анализ общедоступных рыночных данных и трендов.	Использование ИИ для обхода систем безопасности Компании или нарушения ее внутренних политик.

Правила работы с данными

- [ ] Классификация данных

  Все данные Компании делятся на: публичные (общедоступные), внутренние (доступны сотрудникам, но не публичны), конфиденциальные (коммерческая тайна) и персональные данные (требуют особой защиты).

- [ ] Публичные и внутренние данные

  Могут использоваться в общедоступных ИИ-сервисах при условии, что это не нарушает внутренние политики Компании и не содержит скрытой конфиденциальной информации.

- [ ] Конфиденциальные и персональные данные

  Строго запрещено вводить эти типы данных в публичные ИИ-сервисы (например, ChatGPT, YandexGPT, GigaChat). Для работы с такими данными разрешено использовать только корпоративные, on-premise или Enterprise-версии ИИ-инструментов, одобренных ИТ-отделом Компании, которые гарантируют защиту данных и отсутствие их использования для обучения моделей.

- [ ] Enterprise-версии и on-premise решения

  При использовании корпоративных версий ИИ-платформ (например, Yandex Cloud, Microsoft Azure AI) или развертывании ИИ на собственных серверах, сотрудники должны следовать инструкциям ИТ-отдела и политике безопасности Компании.

- [ ] Анонимизация и псевдонимизация

  В случае необходимости анализа конфиденциальных или персональных данных с помощью ИИ, сотрудники обязаны провести их анонимизацию или псевдонимизацию в соответствии с внутренними инструкциями, чтобы исключить возможность идентификации субъектов данных.

Ответственность

- [ ] Ответственность сотрудников

  Сотрудники несут персональную ответственность за нарушение настоящего Регламента, включая несанкционированное разглашение конфиденциальных данных или нарушение авторских прав. Нарушения могут повлечь за собой дисциплинарные взыскания вплоть до увольнения, а также гражданско-правовую и уголовную ответственность в соответствии с законодательством РФ.

- [ ] Ответственность Компании

  Компания несет ответственность за обеспечение безопасной ИИ-инфраструктуры, обучение сотрудников и регулярный аудит использования ИИ. Компания стремится минимизировать риски, связанные с ИИ, но не несет ответственности за неправомерные действия сотрудников, нарушающих данный Регламент.

Обучение и поддержка

- [ ] Обязательное обучение

  Все сотрудники, использующие ИИ-инструменты, обязаны пройти вводный курс по безопасному и этичному использованию ИИ. Регулярные обновления и дополнительные тренинги будут проводиться по мере развития технологий и изменения законодательства. Согласно статье 4 EU AI Act, компании должны внедрять программы обучения с учетом знаний, роли и опыта сотрудников (LBKP Legal, 2025).

- [ ] Каналы поддержки

  По вопросам, связанным с использованием ИИ, сотрудники могут обращаться в ИТ-отдел (для технических вопросов) или в Отдел развития (для вопросов по сценариям использования и лучшим практикам). Контактные данные: [email ИТ-отдела], [email Отдела развития].

- [ ] Библиотека промптов

Компания будет поддерживать внутреннюю библиотеку эффективных промптов для типовых задач, доступную по ссылке: [Ссылка на внутренний ресурс/SharePoint].

Мониторинг и аудит

- ☐ Регулярный мониторинг

  ИТ-отдел Компании осуществляет мониторинг использования ИИ-инструментов для выявления потенциальных угроз безопасности и нарушений Регламента. Это включает анализ журналов доступа и использования корпоративных ИИ-систем.

- ☐ Внутренний аудит

  Не реже одного раза в год будет проводиться внутренний аудит соответствия использования ИИ настоящему Регламенту и применимому законодательству. Результаты аудита будут использоваться для корректировки политик и процессов.

- ☐ Обновление Регламента

  Настоящий Регламент подлежит пересмотру и обновлению не реже одного раза в год или по мере возникновения новых угроз, технологий и изменений в законодательстве.

Приложение: Пример библиотеки промптов для типовых задач

Задача	Пример промпта	Пояснение
Генерация черновика email	"Напиши черновик email для клиента [Имя клиента] с предложением о встрече для обсуждения нового продукта [Название продукта]. Укажи основные преимущества: [Преимущество 1], [Преимущество 2]. Тон: деловой, но дружелюбный."	Задайте роль, цель, ключевые пункты и желаемый тон.
Резюмирование статьи	"Прочитай следующую статью: [Вставьте текст статьи]. Сделай краткое резюме в 3-5 предложений, выделив основные идеи. Ориентируйся на аудиторию руководителей."	Укажите объем, целевую аудиторию и фокус.
Генерация идей для поста в соцсети	"Придумай 5 идей для поста в Telegram-канал о преимуществах использования ИИ в маркетинге. Для каждой идеи предложи заголовок и краткое описание. Целевая аудитория: малый и средний бизнес."	Определите количество идей, платформу, тему и аудиторию.
Перевод текста	"Переведи следующий текст на английский язык: [Вставьте текст]. Сохрани деловой стиль и терминологию."	Укажите язык перевода и требования к стилю.
Мозговой штурм по решению проблемы	"Представь, что ты консультант по оптимизации бизнес-процессов. Мы столкнулись с проблемой [Описание проблемы]. Предложи 3-5 креативных решений, используя ИИ-инструменты."	Задайте роль ИИ, опишите проблему и запросите конкретное количество решений.

Больше интересного в нашем блоге

развивайте бизнес-мышление с нашими исследованиями

Получить пользу →

rocketlab.bz

@rocketlab