



ТАЛИОН
ЭКСПЕРТ НЕО

ПРАВО
ТЕХНОЛОГИИ
БЕЗОПАСНОСТЬ
ДЛЯ БИЗНЕСА

ЧЕК-ЛИСТ

БЕЗОПАСНОЕ ВНЕДРЕНИЕ ИИ:

что настроить в компании

Практические шаги
для управляемого, защищённого
и ответственного
использования ИИ

- ☒ ОПРЕДЕЛИТЬ ПРАВИЛА
- ☒ ЗАЩИТИТЬ ДАННЫЕ
- ☒ ОЦЕНИТЬ РИСКИ
- ☒ ОБУЧИТЬ КОМАНДУ



ПОЛИТИКИ
ИИ



ЗАЩИТА
ДАННЫХ



КОНТРОЛЬ
РИСКОВ



БЕЗОПАСНОЕ ВНЕДРЕНИЕ ИИ

Шесть пунктов помогут подготовить компанию к безопасной работе с нейросетями

1 ПРАВИЛА ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ

- ✓ Определено, для каких рабочих задач разрешено использовать ИИ.
- ✓ Составлен список одобренных сервисов и запрещённых способов их использования.
- ✓ Сотрудники знают, какие сведения нельзя передавать нейросетям.



ДЕЙСТВИЕ:

Утвердите внутренние правила использования ИИ, указав, кто может разрешать новые сервисы и порядок согласования.

2 ДОСТУПЫ И УЧЁТНЫЕ ЗАПИСИ

- ✓ Доступ к ИИ-сервисам предоставляется только сотрудникам, которым он необходим.
- ✓ Для рабочих аккаунтов включена многофакторная аутентификация, если сервис её поддерживает.
- ✓ Определён порядок отключения доступа при увольнении сотрудника или завершении работы подрядчика.



ДЕЙСТВИЕ:

Назначьте ответственного за управление доступами. Проверьте, кто может просматривать историю запросов, загруженные файлы и общие рабочие пространства.

3 ЗАЩИТА ДАННЫХ И КОНФИДЕНЦИАЛЬНОСТЬ

- ✓ Перед использованием сервиса проверены условия хранения, обработки и удаления запросов и файлов.
- ✓ Установлены ограничения на передачу персональных данных, коммерческой тайны и документов клиентов.
- ✓ Сведения, составляющие реальную тайну, передаются только в одобренные сервисы и в соответствии с установленным в компании режимом конфиденциальности.
- ✓ Для задач, не требующих реальных данных, предусмотрено использование обезличенных или синтетических примеров.
- ✓ Если в ИИ-сервис передаются персональные данные, определены правовое основание обработки и порядок оформления поручения обработчику.
- ✓ Зафиксированы перечень передаваемых персональных данных, цели обработки, состав операций, требования к конфиденциальности и порядок удаления данных.
- ✓ Для зарубежных сервисов проверена необходимость и правомерность трансграничной передачи персональных данных.



ДЕЙСТВИЕ:

Согласуйте допустимые категории данных для каждого сервиса. При обработке персональных данных оформите поручение стороннему поставщику, зафиксировав цели, перечень данных, действия с ними и обязанность соблюдать конфиденциальность. Ответственность перед субъектами персональных данных сохраняется за компанией.



БЕЗОПАСНОЕ ВНЕДРЕНИЕ ИИ: что настроить в компании

Шесть пунктов помогут подготовить компанию к безопасному внедрению ИИ.

4 ИНТЕГРАЦИИ И ТЕХНИЧЕСКИЕ НАСТРОЙКИ

- ✓ Проверено, к каким корпоративным системам, документам и базам данных может обращаться ИИ.
- ✓ Доступы интеграций и API ограничены необходимым минимумом.
- ✓ Перед подключением плагинов, расширений и внешних инструментов проверены их права, источник и репутация разработчика.
- ✓ Настроено журналирование ключевых действий: загрузки файлов, обращений к корпоративным данным и передачи результатов ИИ.



ДЕЙСТВИЕ:

Подключайте только необходимые интеграции. Не предоставляйте ИИ доступ ко всей корпоративной базе, если для задачи достаточно отдельной папки или ограниченного набора данных.

5 ПРОВЕРКА ОТВЕТОВ И РЕШЕНИЙ ИИ

- ✓ Определены задачи, в которых результат ИИ обязательно проверяет сотрудник.
- ✓ Факты, цифры, ссылки и правовые выводы сверяются с надёжными первоисточниками.
- ✓ ИИ-результат не является единственным основанием для критически важных финансовых, кадровых или юридических решений без необходимой проверки.



ДЕЙСТВИЕ:

Определите роли проверяющего и утверждающего сотрудника для значимых результатов ИИ. Для существенных решений фиксируйте использованные источники, результат проверки, лицо, утвердившее итог.

6 ОБУЧЕНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

- ✓ Сотрудники знают правила безопасной работы с ИИ и умеют распознавать риски утечки данных.
- ✓ Определён порядок сообщения об ошибочной загрузке документа, раскрытии секрета или подозрительной активности.
- ✓ Для инцидентов установлен порядок оценки: какие данные затронуты, кому они принадлежат, есть ли признаки распространения и какие обязанности возникают у компании.
- ✓ Правила и настройки пересматриваются при подключении новых сервисов и изменении рабочих процессов.



ДЕЙСТВИЕ:

Проведите инструктаж сотрудников и подготовьте порядок реагирования на инциденты. При утечке ограничьте доступ, сохраните необходимые сведения для расследования, оцените масштаб происшествия и применимые обязанности по уведомлению Роскомнадзора, субъектов персональных данных или иных заинтересованных лиц.

Спасибо за внимание!

Этот чек-лист поможет вам безопасно и ответственно внедрять ИИ в бизнесе, минимизировать риски и использовать возможности новых технологий с максимальной пользой.

Об авторе



Ермохина Елена Анатольевна

-  руководитель ООО «Талион Эксперт Нео»
-  юрист
-  профессиональный медиатор
-  лектор Общества Знаний
-  член Союза юристов блогеров при АЮР
-  член Национальной Ассоциации Профессиональных Медиаторов «Паритет»

ГЛАВНЫЕ ПРИНЦИПЫ

-  ПРАВИЛА
ИСПОЛЬЗОВАНИЯ ИИ
-  ОГРАНИЧЕНИЕ
ДОСТУПОВ
-  ЗАЩИТА
ДАННЫХ
-  ПРОВЕРКА
РЕЗУЛЬТАТОВ
-  ОБУЧЕНИЕ
СОТРУДНИКОВ
-  КОНТРОЛЬ
РИСКОВ

“ Нейросети — мощный инструмент, но безопасность данных всегда начинается с вашей внимательности и правовой грамотности.