



Интерштурм

# Кодекс безопасной работы с ИИ

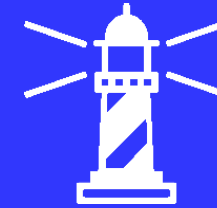
Практический мастер-класс.



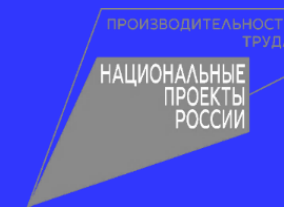
# Ксения Чуприцкая

генеральный директор компании Интершторм,  
бизнес-консультант, доверенный эксперт Национальной  
Технологической Инициативы, преподаватель РАНХиГС

- Обучение руководителей и команд навыкам работы с ИИ-сервисами.
- Разработка и внедрение ИИ-решений на основе генеративного ИИ
- Разработка стратегий цифровой трансформации компаний



**Интершторм AI –решения  
награды и достижения**



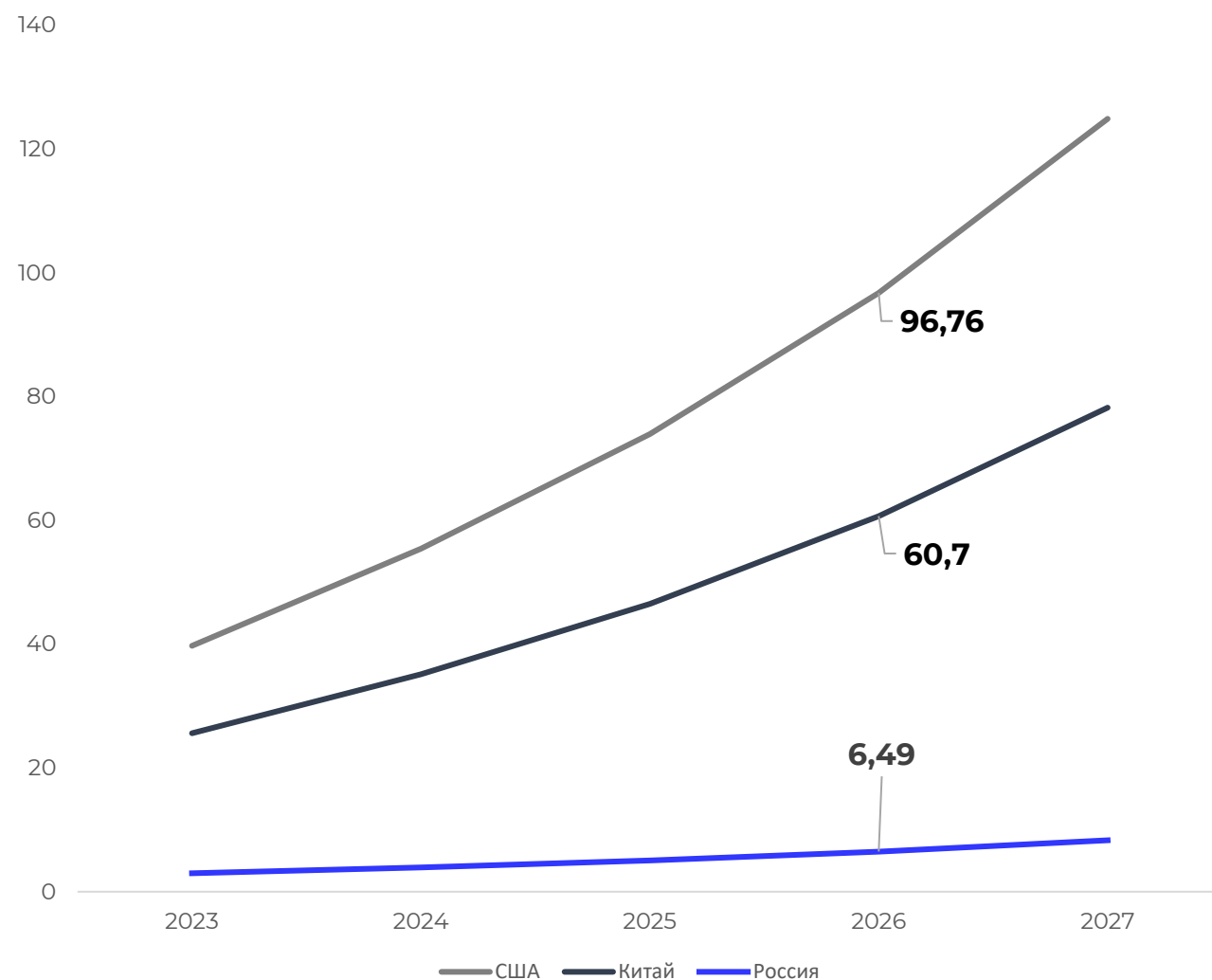
победитель конкурса  
"Лучшие практики  
наставничества" в  
категории прорывных  
технологий



лучшая практика в  
номинации  
«Компетенции и  
развитие персонала» и  
«Цифровая  
трансформация»

# Ландшафт: от экспериментов к массовым инвестициям

Объем рынка GenAI в динамике (млрд \$)



Организации:

- 95% используют технологию
- 40% масштабируют
- 8% подтвержденный ROI



# «Теневая ИИ-экономика»: масштаб и факты

Мировой контекст

90%

Сотрудников используют личные ИИ-инструменты для рабочих задач

40%

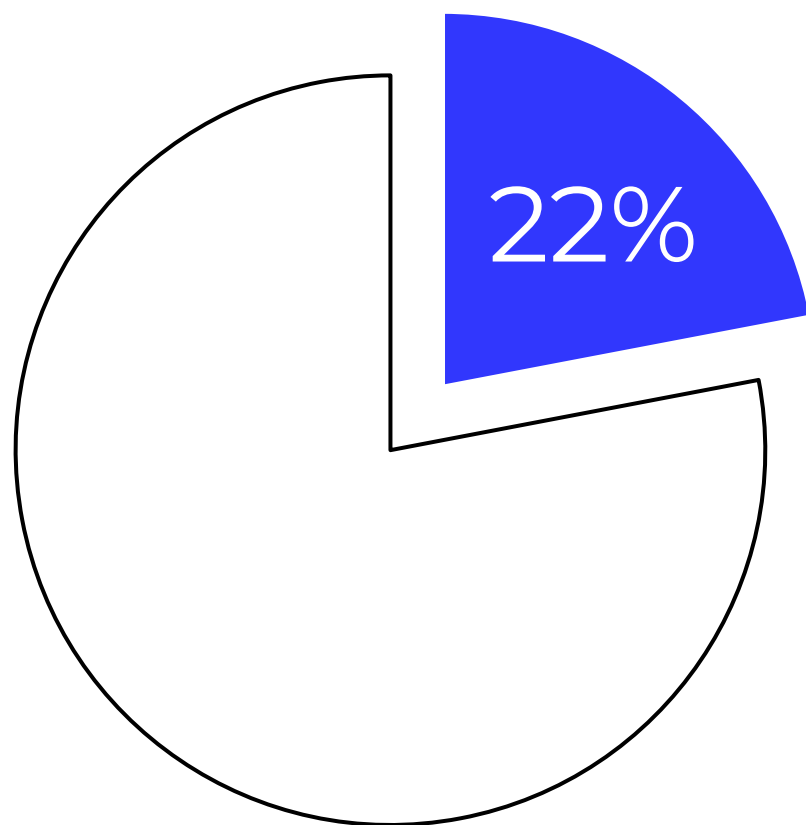
Организаций приобрели подписки на корпоративные LLM

5%

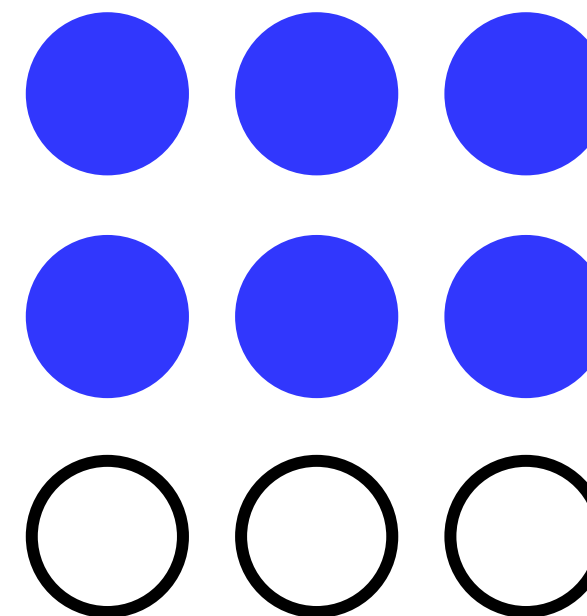
Положительный экономический эффект



## Разрыв представлений:



22 % руководителей уверены в том, что их кадры готовы к работе с ИИ

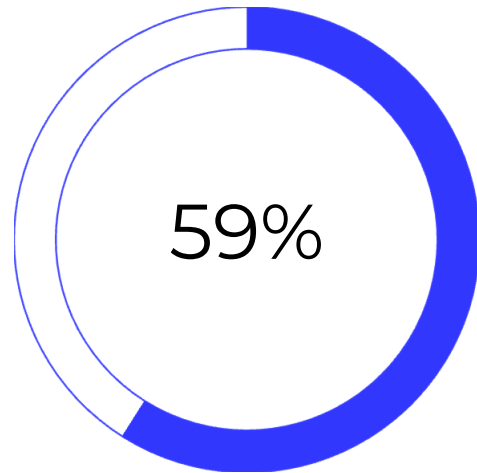


**В 3 РАЗА ЧАЩЕ**

сотрудники используют ИИ и делегируют ему >1/3 своей работы, чем предполагают их руководители



# Российский контекст



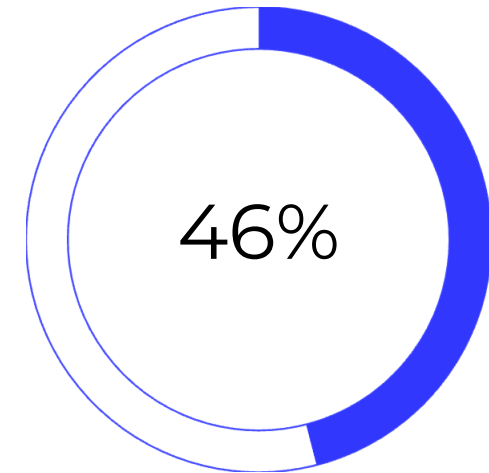
## Зарубежные модели

Компании подтверждают использование сотрудниками ChatGPT, DeepSeek, Perplexity

# x30

## Рост утечек

В 2025 году общедоступные ИИ-сервисы получили в 30 раз больше чувствительной информации



## Через ChatGPT

Всех конфиденциальных файлов и инструкций проходит только через ChatGPT

## Что утекает:

- Презентации
- Стратегии
- Аналитические таблицы
- Фрагменты кода
- Финансовые отчеты
- Юридические документы
- Клиентские базы

Источники: Исследование «Практика использования ИИ в российских компаниях», 196 компаний



## Российский контекст



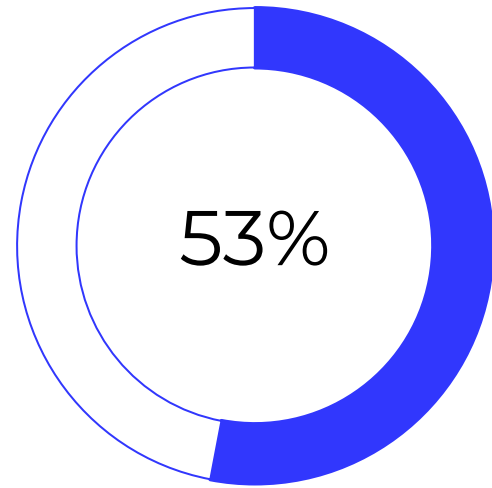
### Яндекс Правовые документы



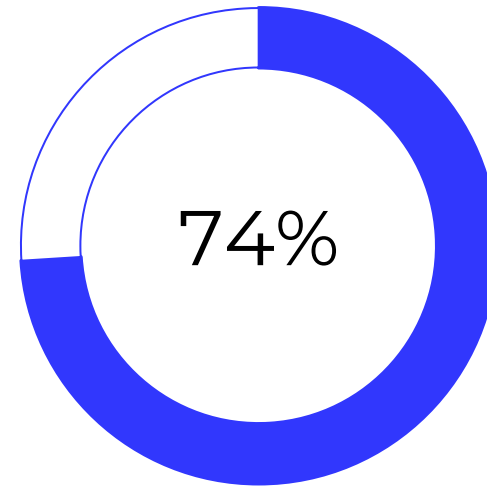
3.2. Пользователь согласен с тем, что Яндекс вправе использовать Запросы и Контент для любых целей и любыми способами по своему усмотрению на территории всего мира без ограничения по сроку, в том числе в целях совершенствования работы алгоритмов и технологий Яндекса, для размещения в Сервисах, в рекламных и маркетинговых материалах, для привлечения внимания к Технологии и Сервисам, их отдельным функциям, а также на иных принадлежащих Яндексу ресурсах, каналах и страницах, если иное не предусмотрено условиями отдельных Сервисов.



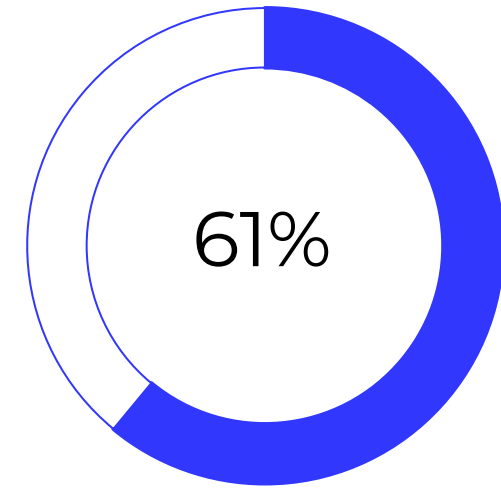
## Российский контекст



нет официальной позиции по ИИ



нет внутренних политик и регламентов



не назначен ответственный

ИИ – уже часть операционной деятельности, но происходит это стихийно, через индивидуальную инициативу, а не через корпоративную стратегию.



# Запретить теневой ИИ?

## Инструменты реализации:

01

### Блокировка доступа

На уровне NGFW/сетевой фильтрации

03

### Allowlist приложений

Запрет запуска стороннего ПО для доступа к ИИ

05

### Защита от фотографирования

экрана (видеоаналитика)

02

### DLP-системы

Блокировка передачи данных в ИИ-приложения, копирования больших фрагментов

04

### Запрет личных устройств

Для рабочих задач

06

### Жесткая политика

Разрешены только утвержденные корпоративные инструменты + обучение

**KPMG:** Лидеры рынка используют ИИ для роста выручки (33%), а не только для сокращения затрат (25%). Запретительная политика обычно фокусируется на сохранении статус-кво, убивая потенциал для роста.



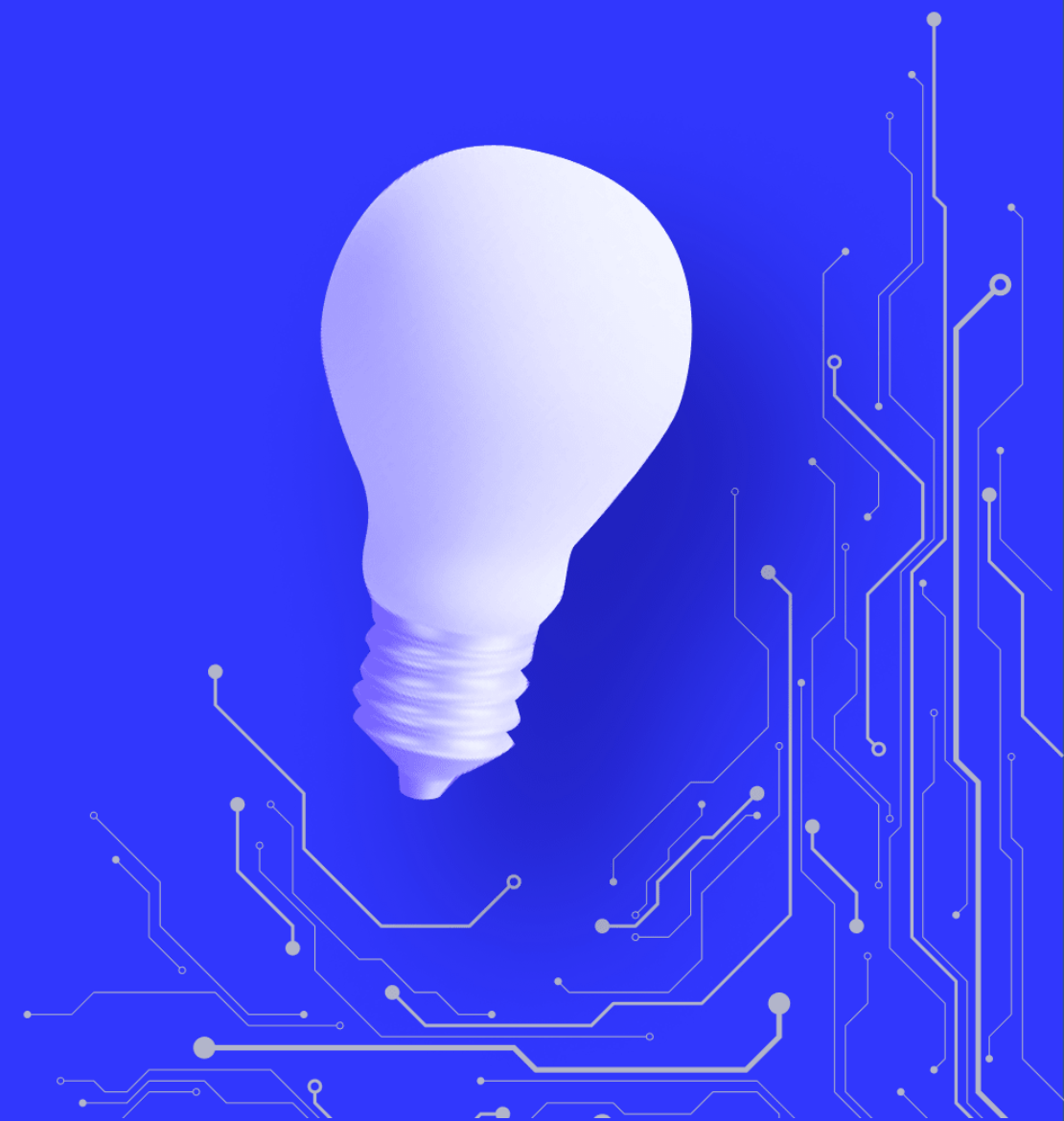
# Стратегии контроля корпоративного ИИ

Мера безопасности	Теневой ИИ	Свой контур (On-Prem)	Корп. ИИ-платформа
1. Обучение сотрудников	Критично важно (чтобы не обходили запреты)	Важно (работа с интерфейсом)	Ключевой драйвер (культура использования)
2. NGFW / CASB / DLP	Максимальная нагрузка (блокировка всего)	Умеренная (контроль периметра)	Минимальная (базовый фильтр)
3. Мониторинг трафика	Сложно и дорого (шифрованный трафик)	Средне (внутренние логи)	Готовые отчеты от вендора
4. Защита инфраструктуры (XDR, Сегментация)	Стандартная	Максимальная нагрузка (защита своих серверов ИИ)	Минимальная (инфраструктура у вендора)



**Практикум:**

**Кодекс безопасной работы с ИИ**



Чат конференции  
Код ИБ Санкт-Петербург

копируйте промпты для  
совместной работы над  
Кодексом безопасной работы  
с ИИ



DeepSeek

общедоступный ИИ-сервис  
для работы с текстовыми  
данными



# 1. Требования регулятора

промт для нейросети:

Сформулируй 10 ключевых требований по обеспечению информационной безопасности и комплаенса, которые не должны быть нарушены коммерческой организацией при передаче любых корпоративных данных (включая ПДн, КТ и данные КИИ) в сторонние публичные Большие Языковые Модели (LLM) типа ChatGPT/Gemini. Для каждого требования укажи, какой именно закон или подзаконный акт (наименование и/или номер) устанавливает данное ограничение или обязанность, имеющее прямое отношение к корпоративному сектору.

пример ответа:

№	КЛЮЧЕВОЕ ТРЕБОВАНИЕ	ПРЕДМЕТНЫЕ ОБЛАСТИ	РЕГУЛИРУЮЩИЙ НПА (НАИМЕНОВАНИЕ/НОМЕР)	ССЫЛКА НА ИСТОЧНИК (КОНТЕКСТ)
1	Исключение передачи персональных данных (ПДн) без надлежащей защиты или без достаточных правовых оснований.	ПДн	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (Ст. 7, 16)	<a href="#">Постановление Правительства РФ От 01.11.2012 N 1119 «Об Утверждении...»</a>
2	Обеспечение конфиденциальности информации, неразглашение коммерческой тайны и иной охраняемой законом информации.	КТ, другие конфиденциальные данные	Федеральный закон от 29.07.1998 № 123-ФЗ «О коммерческой тайне» (Ст. 10).	<a href="#">Справочник законодательства РФ в области информационной безопасности</a>
3	Запрет на несанкционированный сбор, запись и хранение информации о защищаемых данных, если это не предусмотрено внутренними нормативными актами (ЛНА).	Все типы данных	Приказ ФСТЭК России № 21 (Требование РСБ.3)	<a href="#">Комплаенс в информационной безопасности</a>
4	Оценка и устранение последствий нарушения безопасности информации, в том числе при передаче	ПДн, КИИ, КТ	Федеральный закон от 27.07.2006 № 152-ФЗ (Ст. 17 оценка вреда)	<a href="#">Приказ Роскомнадзора № 178 «Об утверждении</a>



## 2. Что такое чувствительная информация?

промпт для нейросети:

Приведи список типов информации, которые категорически нельзя вводить в открытые публичные нейросети (ChatGPT, Gemini и аналоги) сотрудниками коммерческой организации в России. Раздели их на категории. Для каждого типа приведи реалистичный пример из деловой переписки, документа или системы компании, где явно упоминается ее наименование, внутренние структуры, уникальные идентификаторы или сотрудники. Примеры должны наглядно демонстрировать, что ввод даже фрагмента такой информации в нейросеть создает риск утечки конфиденциальных сведений. Выведи в формате таблицы: Категория / Что НЕЛЬЗЯ вводить / Конкретный пример (с указанием вымышленной компании / подразделения / идентификаторов).

пример ответа:

КАТЕГОРИЯ	ЧТО НЕЛЬЗЯ ВВОДИТЬ	КОНКРЕТНЫЙ ПРИМЕР (С ВЫМЫШЛЕННОЙ КОМПАНИЕЙ / ПОДРАЗДЕЛЕНИЯ / ИДЕНТИФИКАТОРОВ)
1) Сведения, составляющие коммерческую тайну (внутренние регламенты, методики, планы)	Номенклатура, формулы, методики ценообразования, матрицы маржинальности, стратегия продаж, планы закупок, условия контрактов с контрагентами, внутренние KPI/нормативы, "best practices", которые не являются публичными	Письмо из "АО «СеверМаркет» / Дирекция по закупкам": «В коммерческое предложение для ООО «ТрансЛогист» вносим скидку по шкале 7–12% в зависимости от объема. Точная формула: $\text{margin} = (\text{Цена\_нетто} - \text{Себестоимость\_с\_раскладкой}) / \text{Цена\_нетто}$ . Маржинальность держим не ниже 18%».
2) Договорные/контрактные условия (если не публичны)	Точные цены, SLA, штрафы, условия поставки/оплаты, спорные формулировки, переговорные "рамки", исходники	Фрагмент договора "ООО «ТехСтройИнтеграция»": «Раздел 4.3: оплата 30% аванс + 70% по факту приемки в течение 10 банковских дней. Штраф: 0,1% от цены этапа за каждый день просрочки. Перенос сроков согласуется по процедуре "Change Request CR-77"».



# 3. Чек-лист безопасности при работе с ИИ

промпт для нейросети:

Преобразуй список примеров чувствительной информации и список рисков в чек-лист из 10 конкретных правил для сотрудников российской коммерческой компании, чтобы безопасно использовать публичные нейросети (ChatGPT, Gemini и аналоги) в рабочих целях в контуре компании.

Важно:

чек-лист, должен быть структурированным, лаконичным и практичным. Каждое правило должно начинаться с глагола-действия и сопровождаться наглядным примером.

Чек-лист должен охватывать проверку на конфиденциальность, обобщение задач и работу с результатом.

Представь его в следующем формате:

[Номер]. [Глагол-Действие] [Суть правила]. Пример: [Конкретный пример запроса/действия сотрудника].

Стиль: информационный, с элементами инструкции. Используй ✓/✗ для быстрой визуализации правил, добавь иконки ⚠ рядом с особо опасными пунктами

пример ответа:

- ✗ Не вводи персональные данные (ПДн) и спецкатегории. Пример: вместо «Сергей Иванов, +7(921)555-12-34, дата рождения 12.03.1989» используй «нужна форма ответа кандидату без персональных данных (подставьте ФИО и контакты локально)». ⚠
- ✗ Не передавай коммерческую тайну (цены, маржа, стратегии, roadmap, матрицы скидок). Пример: вместо «маржа 18-22%, скидочная матрица поставщиков A1/B2» — «сформируй шаблон стратегии переговоров без чисел и названий компаний».
- ✗ Не раскрывай условия договоров и клиентские базы. Пример: вместо «клиент "РостИнвест", SLA 99,95%, штраф 0,1%/день, график платежей» — «подготовь письмо-контур для согласования SLA, без реквизитов клиента и KPI».
- ✗ Не вводи ключи, токены, пароли, секреты и "Bearer ...". Пример: вместо «Authorization: Bearer eyJhbGciOiJI...» — «объясни, какие шаги диагностики выполнять при ошибке авторизации (без отправки токена/секрета)». ⚠
- ✗ Не передавай внутренние идентификаторы и привязанные к ним контекстные фрагменты. Пример: вместо «userId=7741c2f9, requestId=7b1a..., URL=/api/payments/ORDER-991234» — «нужен чек-лист расследования утечек по типу инцидента, без userId/requestId/номеров заказов». ⚠
- ✗ Не публикуй детали ИБ-инцидентов, уязвимостей и "как атаковали". Пример: вместо «CVE-XXXX, payloads, правила ModSecurity ID 104312, скрин параметров запроса» — «сформируй безопасный план уведомления и отчёта по инциденту без технических IOCs/эксплоитов». ⚠
- ✓ Обобщай задачу и обезличивай входные данные до "безопасного минимума". Пример: вместо «в отчёте: ООО "СеверМаркет", отдел 17, кандидат Иванов...» используй «в HR-отчёте: "компания/отдел не указаны", "кандидат обезличен", нужен текст для руководителя».
- ✓ Проси модель работать с шаблонами, а не с исходниками. Пример: «Сгенерируй шаблон письма/ответа по теме согласования договора, вставные поля: [Клиент], [Срок], [Пункты], без фактических данных».
- ✓ Проверяй результат на "утечки": названия систем, людей, документов, чисел и ссылок, которые не должны выходить за контур. Пример: после ответа LLM удали/замени места вроде «по адресу»



## 3. Чек-лист безопасности при работе с ИИ

промт для нейросети:

Преобразуй список примеров чувствительной информации и список рисков в чек-лист из 10 конкретных правил для сотрудников российской коммерческой компании, чтобы безопасно использовать публичные нейросети (ChatGPT, Gemini и аналоги) в рабочих целях в контуре компании.

Важно:

чек-лист, должен быть структурированным, лаконичным и практичным. Каждое правило должно начинаться с глагола-действия и сопровождаться наглядным примером.

Чек-лист должен охватывать проверку на конфиденциальность, обобщение задач и работу с результатом.

Представь его в следующем формате:

[Номер]. [Глагол-Действие] [Суть правила]. Пример: [Конкретный пример запроса/действия сотрудника].

Стиль: информационный, с элементами инструкции. Используй ✓/✗ для быстрой визуализации правил, добавь иконки ⚠ рядом с особо опасными пунктами

пример ответа:

- ✗ Не вводи персональные данные (ПДн) и спецкатегории. Пример: вместо «Сергей Иванов, +7(921)555-12-34, дата рождения 12.03.1989» используй «нужна форма ответа кандидату без персональных данных (подставьте ФИО и контакты локально)». ⚠
- ✗ Не передавай коммерческую тайну (цены, маржа, стратегии, roadmap, матрицы скидок). Пример: вместо «маржа 18-22%, скидочная матрица поставщиков A1/B2» — «сформируй шаблон стратегии переговоров без чисел и названий компаний».
- ✗ Не раскрывай условия договоров и клиентские базы. Пример: вместо «клиент "РостИнвест", SLA 99,95%, штраф 0,1%/день, график платежей» — «подготовь письмо-контур для согласования SLA, без реквизитов клиента и KPI».
- ✗ Не вводи ключи, токены, пароли, секреты и "Bearer ...". Пример: вместо «Authorization: Bearer eyJhbGciOi...» — «объясни, какие шаги диагностики выполнять при ошибке авторизации (без отправки токена/секрета)». ⚠
- ✗ Не передавай внутренние идентификаторы и привязанные к ним контекстные фрагменты. Пример: вместо «userId=7741c2f9, requestId=7b1a..., URL=/api/payments/ORDER-991234» — «нужен чек-лист расследования утечек по типу инцидента, без userId/requestId/номеров заказов». ⚠
- ✗ Не публикуй детали ИБ-инцидентов, уязвимостей и «как атаковали». Пример: вместо «CVE-XXXX, payloads, правила ModSecurity ID 104312, скрин параметров запроса» — «сформируй безопасный план уведомления и отчёта по инциденту без технических IOCs/эксплоитов». ⚠
- ✓ Обобщай задачу и обезличивай входные данные до «безопасного минимума». Пример: вместо «в отчёте: ООО "СеверМаркет", отдел 17, кандидат Иванов...» используй «в HR-отчёте: "компания/отдел не указаны", "кандидат обезличен", нужен текст для руководителя».
- ✓ Проси модель работать с шаблонами, а не с исходниками. Пример: «Сгенерируй шаблон письма/ответа по теме согласования договора, вставные поля: [Клиент], [Срок], [Пункты], без фактических данных».
- ✓ Проверяй результат на «утечки»: названия систем, людей, документов, чисел и ссылок, которые не должны выходить за контур. Пример: после ответа LLM удали/замени места вроде «по адресу



# 3. Кодекс безопасного применения открытых ИИ-сервисов

промпт для нейросети:

Задача: проанализируй весь контекст диалога. На основе анализа создай текст документа “Кодекс безопасного применения открытых ИИ-сервисов” для сотрудников коммерческой организации в России. Требования к Кодексу:

Включи уровни критичности рисков

Преобразуй чек-лист в раздел “Пошаговый алгоритм безопасного использования”.

Каждый запрет сопровождай реальным примером из нашего списка

добавь раздел: рекомендации по внедрению и усилению защиты, включи организационные меры

пример ответа:

## Кодекс безопасного применения открытых ИИ-сервисов (ChatGPT/Gemini и аналоги) в коммерческой организации (Россия)

Документ устанавливает единые правила безопасного использования публичных ИИ-сервисов сотрудниками в рабочих целях. Цель — предотвращение утечек конфиденциальной информации, соблюдение комплаенса по персональным данным, коммерческой тайне и требованиям безопасности информации.

### 1) Термины и границы применения

**Открытые публичные ИИ-сервисы** — доступные через интернет решения сторонних провайдеров (например, ChatGPT, Gemini), куда пользователь направляет текст/данные через веб-интерфейс или открытые API.

**Конфиденциальная информация** — в т.ч. коммерческая тайна, персональные данные, сведения об ИТ/ИБ, инцидентах, внутренние регламенты, договорные условия, сведения, относящиеся к КИИ.

**Запрещённое действие** — действие, которое приводит к передаче в открытую публичную LLM запрещённых категорий сведений либо к существенному риску их раскрытия.

### 2) Уровни критичности рисков (для принятия решений)

Риски оцениваются до ввода данных и после получения результата.

УРОВЕНЬ	ОБОЗНАЧЕНИЕ	КРИТЕРИИ	ТРЕБУЕМОЕ ДЕЙСТВИЕ
Высокий	●	Есть идентификаторы (ФИО/employeeid/userid/contractid), инциденты ИБ с контекстом, уязвимости/IOCs, секреты/токены, данные КИИ	Ввод запрещён ❌, альтернативы обязательны
Средний	●	Есть названия подразделений/систем/клиентов + числовые/процессные детали, которые могут быть	Обобщить/обезличить ✅, затем ввести только ..



# Ксения Чуприцкая

генеральный директор компании Интершторм,  
бизнес-консультант, доверенный эксперт Национальной  
Технологической Инициативы, преподаватель РАНХиГС



@kseniamehere



+7 916 922 89 25



[www.interstorm.ru](http://www.interstorm.ru)



[Забрать полезные материалы по AI](#)