



AI и информационная безопасность: 42 ответа на рабочие вопросы

Краткая памятка · extended-mind.ru · источники актуальны на 19.10.2026

Главный принцип: решение зависит от конкретной задачи, состава данных и способа их обработки. Малый размер бизнеса или миллионы пользователей сервиса данные не защищают: раскрытый в чате API-ключ позволит выгрузить базу клиентов, а технические сбои (как в ChatGPT в марте 2023 г. или базе DeepSeek в январе 2025 г.) делают переписку и ключи доступными посторонним без целенаправленной слежки.

Базовое правило. Перед загрузкой спросите себя: «Что именно получит внешний сервис и на каких условиях я вправе это передать?». Проверьте права на документ, условия обработки у поставщика AI и внутренние правила организации (работаете самостоятельно — закон и обязательства перед клиентом). Документ передавать нельзя, а сам сервис разрешён — задайте вопрос без загрузки файла, а реальные цифры и имена внесите сами без участия AI.

Серые зоны: 12 привычных действий

Действие	Что упускают	№
Только перевёл текст / проверил запятые	Облачный сервис получает весь переданный материал — даже ради одной запятой	<u>2</u>
В российской программе свой AI-агент	За интерфейсом может стоять внешний, в т. ч. зарубежный провайдер	<u>4</u>
Купил Pro-подписку, работаю из дома	Личная подписка не заменяет корпоративного разрешения; важны защита ПК и способ доступа	<u>6</u>
Удалил чат / включил временный чат	Не гарантирует удаления файлов, журналов (логов), резервных копий и записей в поисковом индексе	<u>9</u>
Описал словами / дал сводные цифры	Сводные данные и сама формулировка вопроса могут выдать конкретных людей и планы компании	<u>21</u>
Попросил AI удалить из файла фамилии и цены	Для очистки сервис сначала получает исходник; очищать нужно там, где разрешён исходник	<u>25</u>
Заменил ФИО на «Сотрудник 1» / скриншот / по абзацу	Косвенные признаки выдают человека; коды не гарантируют обезличивания; формат не скрывает текст	<u>26, 27</u>
Закрасил суммы в PDF / удалил лист Excel	Под плашкой остаётся извлекаемый текст; в таблице — скрытые сведения и кэш сводных таблиц	<u>28</u>
Только открыл боковую панель AI	Помощник может читать вкладку и передавать фрагменты в поисковых запросах	<u>31</u>
Попросил выжимку входящего письма	Скрытая команда в письме может изменить действия помощника в пределах выданных ему прав	<u>32</u>
Отправил текст ошибки с ключом доступа (API)	Ключ даёт доступ к системе; удалить сообщение недостаточно — ключ нужно отозвать или заменить	<u>35, 39</u>
Переслал саммари / дал ссылку на чат	Пересказ сохраняет закрытые сведения; ссылка может открыть всю историю и файлы	<u>38</u>

1. Задача, данные и инструмент

1 Что проверить перед первым запросом?

- **Задача:** какой результат нужен и какие сведения реально необходимы. Для формулы хватит вымышленных значений; для реального договора нужен официально разрешённый для таких договоров способ обработки.
- **Данные и права:** есть ли ПДн (персональные данные — сведения, по которым человека можно определить прямо или косвенно), закрытая информация, документы клиентов, чужие авторские произведения; вправе ли вы так их использовать.
- **Инструмент и режим:** какой сервис получит сведения, через какую учётную запись и с какими активными подключениями. Работаете сами — учитывайте закон, обязательства перед клиентом и условия сервиса.

2 Исправить ошибки или перевести — это передача данных?

Да, если функция отправляет текст в облако: при переводе, сокращении, проверке орфографии или распознавании картинки (OCR) сервис получает весь отправленный фрагмент, изображение или документ. Выясните, где физически выполняется операция; внешней передачи нет только при локальной обработке на вашем устройстве или сервере компании.

3 Правил по AI нет или они противоречат друг другу?

Отсутствие регламента по AI не создаёт ни полного запрета, ни разрешения передавать тайны вовне: уже действуют законы РФ, договоры с клиентами, режим конфиденциальности и правила рабочих устройств.

- Уточните у руководителя и ИБ разрешённые задачи, данные и сервисы либо приоритет противоречащих документов.
- Пока ждёте ответа — поручайте AI только задачи без корпоративных данных (если сам сервис разрешён). Неизвестно, разрешён ли сам сервис, — решайте задачу без AI.

2. Корпоративный сервис

4 Корпоративный чат и внутренняя модель — одно и то же?

Нет: адрес страницы и логотип компании не определяют, кто фактически получит данные. Схемы:

1. **Локальная LLM (языковая модель):** развёрнута на собственной инфраструктуре организации.
2. **Корпоративное облако:** аккаунтами и настройками управляет организация, но вычисления выполняет внешний поставщик.
3. **«Обёртка»:** чат на сервере компании, но запросы пересылаются сторонней организации.

«Встроенный агент» в российской программе может вести к зарубежной модели (страна разработчика интерфейса этого не определяет). Даже при локальной модели внешними могут оставаться распознавание файлов, веб-поиск и подключения. Уточните у ИТ/ИБ: какие категории данных, в каком режиме и с какими функциями можно обрабатывать.

5 Сервис разрешён — можно загружать любые файлы?

Нет: разрешение действует для связки **«задача + данные + сервис + режим»**. Изменили формулировку запроса в рамках той же задачи и тех же данных — новая проверка не нужна. Меняются тип данных, подключения или полномочия помощника — сверьтесь с порядком; если он сценарий не охватывает — согласуйте с ИБ/ИТ.

6 Платная подписка, рабочая почта, домашний компьютер что-то меняют?

Они меняют отдельные настройки, но разрешения на передачу корпоративных данных не дают.

- **Личная платная подписка:** остаётся публичной офертой, а не корпоративным договором с компанией.
- **Рабочая почта:** связывает аккаунт с организацией, но не делает его корпоративным.
- **Домашний компьютер:** не отменяет обязательств перед работодателем или клиентом; на неуправляемом устройстве может не быть корпоративных средств защиты.

Используйте только предусмотренные организацией аккаунт и способ доступа.

7 Поставщик обещает не обучать модель на моих данных. Достаточно?

Нет: обучение модели, текущая обработка запроса и хранение данных — три разные операции. Сервис может сохранять историю, файлы и логи, а также давать к ним доступ своему персоналу для расследования инцидентов и проверки правил. Отдельно проверяйте: обучение, сроки хранения логов, доступ персонала и субподрядчиков, географию серверов, порядок удаления и работу доп. функций ([Microsoft Foundry: конфиденциальность данных](#)).

3. Персональные данные

10 Можно ли обрабатывать ПДн во внутренней LLM?

Да, если для конкретной операции установлены законная цель, правовое основание, ролевой доступ, защита и порядок работы. Сама локальная установка модели прав не даёт; право сотрудника видеть файл ≠ право обрабатывать его любым способом (например, загружать в общую базу знаний или дообучать общего бота).

Организация определяет ([ст. 3, 5, 6, 18.1, 19, 22 152-ФЗ](#)): цель (совместимую с изначальной целью сбора); правовое основание (простое удобство автоматизации им не является); минимальный состав сведений; круг лиц с доступом (включая распознавание, поиск, логи, резервные копии); меры защиты, сроки хранения и удаление. Локальность не освобождает оператора от локальных актов, защиты и уведомления РКН (кроме прямых исключений закона).

Сотруднику: сверить задачу с порядком; если не охватывает — к ответственному за ПДн до загрузки. Для уже предусмотренного порядком случая новая юр. проверка не нужна. Пример: для графика отпусков передают ФИО, подразделение и даты — без сканов паспортов, окладов и диагнозов.

8 Российская модель или сервер в России позволяют передавать рабочие данные?

Сами по себе — нет. Они не решают автоматически вопросы законной цели обработки, наличия договора, доступа персонала провайдера, места хранения резервных копий и дальнейших передач; кроме того, место хранения файла и место вычисления ответа могут различаться. Требования [ст. 6, 18.1, 19 152-ФЗ](#) сохраняются; при обработке по поручению нужны законные условия поручения и меры защиты. Если условия неизвестны — обратитесь к ответственному за ПДн.

9 Если удалить чат, данные исчезнут?

Не обязательно: сведения могут остаться в файловом хранилище, технических журналах, резервных копиях и поисковом индексе. Временный чат (Temporary Chat) также оценивайте по документации: отсутствие видимой истории не означает отсутствия логов у подключённых инструментов. Пример: в [Azure AI Search](#) без специальной настройки фрагменты удалённого файла остаются в поисковом индексе. Сроки и механику удаления выясняйте до загрузки.

11 Для работы с AI всегда нужно согласие человека?

Не всегда. Само внедрение AI не доказывает ни потребности в новом согласии, ни достаточности старого — сверяйте фактическую цель и способ обработки.

- **Внутри компании:** основанием может служить исполнение договора с человеком или требование закона.
- **Поручение внешнему провайдеру:** по общему правилу нужны согласие субъекта и договор поручения с обязательными условиями защиты ([ч. 3 ст. 6 152-ФЗ](#)); закон может предусматривать исключения. Обычная покупка подписки поручение не подтверждает.
- **Требования к согласию ([ст. 9 152-ФЗ](#)):** конкретное, предметное, информированное, сознательное и однозначное; оформляется отдельно от иных документов (а в установленных законом случаях — строго в письменной форме); минимизацию и защиту данных не отменяет.

12 Резюме, зарплаты и сведения о здоровье через AI?

- **Резюме и зарплаты (обычные ПДн):** анализ только в специально разрешённом контуре под конкретную цель (право хранить резюме для найма не разрешает загружать его в любой внешний AI).
- **Сведения о здоровье (специальная категория):** исходный запрет обработки, кроме случаев закона (ст. 10 152-ФЗ). Законное хранение больничного в кадрах не позволяет включать его в базу знаний AI.
- **Практика:** для графика работы с учётом болезни передавайте только период отсутствия без диагноза.

13 Можно ли отправлять свои ПДн с рабочего компьютера?

Можно, если правила компании допускают такое использование устройства и сервиса, а в документе нет данных других людей и секретов работодателя (расчётный листок, рабочая переписка и отчёт могут их содержать). В корпоративном AI-аккаунте историю чатов и хранилища могут видеть администраторы; даже из своего резюме предварительно уберите паспортные данные и адрес.

14 Запись встречи и AI-расшифровка. Голос — биометрия?

Записывать и расшифровывать можно, если порядок организации охватывает эту встречу, инструмент и обработку. Простого предупреждения участников в начале звонка недостаточно, а согласие юрлица-клиента не отменяет прав конкретных физлиц на созвоне.

Аудиозапись считается биометрией (ст. 11 152-ФЗ), когда характеристики голоса используют для установления личности. Текстовый протокол — другая задача, но запись и расшифровка могут содержать обычные ПДн, сведения о здоровье и закрытые рабочие данные.

- Используйте только проверенный организацией инструмент и режим.
- Порядок неизвестен — до записи уточните у руководителя или ответственного за процесс; без ответа бота не подключайте, ведите протокол обычным способом.

15 Загрузить файл, добавить в базу знаний, обучить модель — разные действия?

Да: кардинально различаются цель, сроки хранения и круг лиц с доступом.

- **Разовый анализ в чате:** хранение зависит от условий сервиса; слово «разовый» не гарантирует удаления после ответа.
- **База знаний с RAG (поиск фрагментов документов и добавление их к запросу):** саму модель не дообучают; кто увидит сведения, зависит от разграничения прав доступа ([Azure AI Search](#)).
- **Дообучение (Fine-tuning):** данные меняют саму модель; цель и техническая возможность прекратить использование данных оцениваются отдельно.

Разрешение на разовый чат не даёт права включать документ в RAG или датасет для дообучения. Удаление исходного файла не гарантирует уничтожения производных записей (152-ФЗ).

16 Поручить AI решения о кандидатах, сотрудниках, клиентах?

Подготовку проекта заключения или предварительное сравнение по критериям — можно (при разрешённой обработке данных). Принимать окончательное решение, порождающее юридические последствия или иначе затрагивающее права и законные интересы человека, на основании **исключительно автоматизированной обработки** запрещено, кроме случаев письменного согласия или федеральных законов (ст. 16 152-ФЗ; при этом нужно разъяснить порядок оценки, последствия и обеспечить право на возражение, а в кадрах учитывать и трудовые нормы). Финальное решение принимает живой ответственный специалист после личной проверки.

17 Передавать ПДн в иностранный AI-сервис?

Только в разрешённом организацией процессе после юридической и технической проверки. Ни согласие человека, ни оплата тарифа, ни локальная копия таблицы в РФ сами по себе схему законной не делают.

- **Локализация при сборе:** с 01.07.2025 при сборе ПДн граждан РФ запрещено использовать зарубежные базы для записи, систематизации, накопления, хранения, уточнения и извлечения ПДн, кроме прямых исключений закона (ч. 5 ст. 18 152-ФЗ).

- **Трансграничная передача:** регулируется [ст. 12 152-ФЗ](#) с учётом [поправки от 26.07.2026](#) (участие страны в Конвенции Совета Европы отдельным основанием больше не служит; важна категория страны в перечне РКН). До начала передачи оператор обязан запросить у иностранного провайдера сведения о защите данных и подать уведомление в Роскомнадзор (РКН).

До подтверждения схемы ответственным за ПДн (DPO), юристами и ИБ — используйте разрешённый локальный/российский контур или задавайте вопросы без реальных ПДн.

4. Внутренние, клиентские и чужие материалы

18 Внутренние документы без грифа конфиденциальности?

Можно, если содержание, инструмент и действие разрешены для задачи; само отсутствие грифа этого не подтверждает. Режим коммерческой тайны требует мер по [ст. 10 98-ФЗ](#), но и без грифа файл может содержать ПДн, клиентские условия, финансовые планы или сведения, защищаемые трудовым договором. Статус неизвестен — уточните у владельца сведений; пока вопрос не решён — запрашивайте пустую структуру без закрытых данных.

19 Можно ли передать AI документ клиента или подрядчика?

Только после проверки договора с клиентом, NDA, а также прав на ПДн и авторские материалы внутри файла.

- Получение файла от клиента для работы не даёт права передавать его стороннему AI-провайдеру.
- Ваш NDA с поставщиком AI не отменяет запрета в договоре с клиентом на передачу третьим лицам.
- Письменное разрешение компании-клиента не заменяет законного основания обработки ПДн упомянутых в документе людей.

20 Документ, резюме, контакты уже опубликованы в интернете?

Публикация в открытом доступе не разрешает любую последующую обработку. Открытые резюме и контакты остаются ПДн: учитывайте условия и запреты субъекта при распространении и наличие законного основания ([ст. 10.1 152-ФЗ](#)). Проверяйте, что загружаете чистую публичную версию документа без внутренних рабочих комментариев коллег, и соблюдайте авторские права.

21 Безопасно ли отправлять только сводные цифры или описание задачи?

Не всегда. «Средняя зарплата отдела» из одного человека прямо раскрывает его доход; динамика выручки выдаёт компанию по специфике ниши; запрос *«Помогите составить письмо о закрытии филиала»* раскрывает управленческий план, если организация понятна по аккаунту или истории чатов. Убирайте реальные названия и редкие обстоятельства, а для расчётов используйте вымышленные цифры с той же математической структурой.

22 Корпоративный шаблон, логотип, картинка?

Можно, если разрешены содержание, права на использование и обработка в сервисе. Шаблон презентации часто хранит внутренние реквизиты, старые комментарии и примеры; офисное фото — лица людей и экраны мониторов на фоне. Лицензия на купленную картинку может не разрешать её загрузку в сторонние нейросети. Для подбора дизайна безопаснее описать фирменные цвета и макет словами.

23 Подписанный документ или доверенность?

Сам текст — по общим правилам (ПДн, конфиденциальность). **Закрытый ключ электронной подписи (ЭП), пароль от носителя (токена) и коды подтверждения не передавать в AI никогда.** Не путайте открытый сертификат и закрытый ключ (он позволяет подписывать документы от имени владельца). Подлинность ЭП языковая модель технически и юридически не подтверждает — для этого нужны криптографические средства.

24 Купленный курс, платная статья, запись чужого выступления?

Покупка даёт права только в рамках лицензии/договора и не разрешает копировать материал во внешний AI, загружать в общую базу знаний или распространять переработку.

- Воспроизведение и использование требуют согласия правообладателя; отсутствие прямого запрета согласием не считается (ст. 1229, 1270 ГК РФ).
- Свободное использование в личных целях (ст. 1273 ГК РФ) нельзя автоматически переносить на коммерческую работу команды.

- Цитирование (ст. 1274 ГК РФ) требует подходящей цели, оправданного объёма, указания автора и источника и не легализует загрузку целой книги или курса в облако.

Нужных прав нет — обсуждайте тему с AI без загрузки файла.

5. Подготовка файла

25 Попросить AI обезличить документ?

Нет, если этому инструменту изначально не разрешено получать исходные данные: чтобы удалить фамилии и цены, внешний сервис сначала полностью получает исходник. Очищать документ можно только в разрешённом для исходника инструменте или вручную, после чего обязательно перепроверить текст глазами. Если после очистки документ потерял смысл для анализа — работайте в системе, которой разрешён исходник; если её нет — без AI.

26 Достаточно заменить фамилии на «Сотрудник 1»?

Замена кодами может быть частью обезличивания, но сама по себе не подтверждает его достаточность и не разрешает загрузку в AI. Человека легко узнать по уникальной должности, точным датам, редкой ситуации или малому отделу; кроме того, удаление ФИО не снимает режим коммерческой тайны с цен и условий сделки. По [Приказу РКН № 140](#) при введении идентификаторов (замене определяющих человека сведений кодами) таблицы соответствия и исходные данные хранят отдельно от обезличенного массива, ключ не передают третьим лицам, а достаточность метода и действия оценивают и учитывают. Применяйте установленный организацией способ (она определяет применимость приказа № 140 к процессу); если его нет — уточните у ответственного за ПДн до передачи.

27 Только фрагмент, скриншот или изменённые числа?

- **Фрагменты:** даже один абзац может содержать ключевое коммерческое условие, а отправка по кускам в одном чате собирает почти полный документ у провайдера.
- **Скриншот:** распознаётся моделью, включая имена, телефоны, адресную строку и случайно попавшие в кадр соседние окна.
- **Изменённые числа:** пара искажённых цифр не гарантирует ни обезличивания ПДн, ни снятия коммерческой тайны. Для разбора формулы создавайте полностью вымышленный пример.

28 Что проверить в файле, кроме видимого текста?

- **Office:** комментарии, непринятые исправления, свойства автора, скрытые строки и листы, заметки спикера к слайдам, вложенные объекты и кэш сводных таблиц (Pivot Tables). Встроенный «Инспектор документов» находит не всё — например, не замечает белый текст на белом фоне ([Microsoft](#)).
- **PDF:** чёрный прямоугольник поверх текста не удаляет сам текст. Используйте функцию Redaction («Затемнение с удалением»), примените, сохраните копию и проверьте её поиском и копированием ([Adobe](#)).
- После удаления строк из таблиц проверьте, не сломались ли нужные формулы.

6. Подключения и действия помощника

29 Подключить AI к почте, диску, клиентской базе?

Только после оценки объёма доступа с техническими специалистами. Подключённый помощник сам находит и подтягивает письма и файлы в пределах выданных прав — включая закрытые папки, ошибочно открытые на диске «для всех». Запрашивайте доступ только к нужной папке/проекту и только в режиме чтения (для поиска и пересказа права на отправку писем или изменение записей не нужны).

30 Как база знаний не раскроет чужие документы?

Поиск должен жёстко учитывать права конкретного пользователя на этапе извлечения данных (это же касается разделения данных разных клиентов). Перевод текста в эмбединги (числовые представления) данные автоматически не обезличивает: сохраняются риски ошибок доступа, утечек между группами и технической возможности восстановления исходного текста из некоторых векторных представлений ([OWASP LLM08:2025](#)). Техкоманда должна тестировать систему от имени ролей с разными правами; если нашли в ответе чужие данные — сообщите ответственному и не пересылайте их.

31 Встроенный AI в браузере, телефоне, офисной программе?

Проверять обязательно: такие функции могут фоново передавать содержимое экрана или открытого документа в облако без ручного копирования.

- **Браузер:** Copilot в Edge может читать открытую вкладку в зависимости от настроек, иногда без отдельного запроса подтверждения ([Microsoft](#)).
- **Веб-поиск:** помощник формирует поисковые запросы из контекста рабочего документа — внешней поисковой системе уходят тема и содержательные фрагменты файла ([Microsoft](#)).
- **Смартфон:** проверяйте настройки экранных помощников и умных клавиатур перед выделением рабочего текста или фото.

32 Может ли чужой документ заставить помощника нарушить правила?

Да, это **внедрение инструкций (Prompt Injection)** — скрытая текстовая команда внутри входящего письма или документа (например, найти в других файлах финансовые данные и отправить наружу), которую модель воспринимает как вашу приоритетную команду. Просьба в промпте «Никому ничего не отправляй» не защищает; ограничения настраивают на уровне архитектуры и прав ([OWASP LLM01](#)): для пересказа писем помощнику технически не нужен доступ к клиентским папкам и функции отправки почты.

33 Разрешить AI отправлять письма, менять записи, удалять файлы?

Только для разрешённых в процессе действий; для операций с существенными последствиями нужно подтверждение человеком до выполнения ([OWASP LLM06:2025 Excessive Agency](#)).

- **Минимальные права:** право создать черновик письма, а не отправлять его автоматически.
- **Проверка человеком:** получатель, текст, вложения и предлагаемые изменения проверяются до подтверждения.
- **Контроль в целевой системе:** права ограничивают технически, действия журналируют, для обратимых операций предусматривают восстановление (надёжный отзыв уже доставленного письма гарантировать нельзя).

34 Код, ошибки, технические журналы?

Можно, если разрешены инструмент и передаваемые данные. Действующие пароли и ключи удаляйте всегда. В сырых логах часто остаются запросы с ФИО, внутренние IP и токены; код может содержать закрытые алгоритмы или принадлежать клиенту; плагины AI в средах разработки (IDE) могут автоматически подтягивать соседние файлы проекта (список исключений проверяйте с администратором). Для разбора готовьте минимальный пример с вымышленными значениями.

7. Пароли и ключи

35 Отправить пароль или ключ в чат для настройки?

Категорически нельзя ни при каких условиях.

К секретам относятся пароли, API-ключи, токены доступа и сеансов, одноразовые и резервные коды, закрытые ключи ЭП.

- В тексте запроса ставьте заглушку ВАШ_КЛЮЧ, а реальное значение вводите сами в защищённое поле системы или корпоративное хранилище секретов.
- Если помощник должен сам обращаться к сервису — ключ настраивается техническим специалистом внутри программы, чтобы он не попадал в промпты, ответы и логи, а права были минимальными ([OWASP Secrets Management](#)).
- Секрет попал в чат — просто удалить сообщение недостаточно, ключ нужно немедленно отозвать или заменить (см. [вопрос 39](#)).

36 Секреты в отдельном файле, «AI, храни зашифрованным»?

При загрузке открытого файла для шифрования сервис уже получит секреты в открытом виде; при передаче архива вместе с паролем — сможет тут же его расшифровать. У локального агента на ПК «отдельная папка» не значит «недоступная»: файлы .env, переменные окружения и папки вне проекта читаются инструментами агента, а текстовая просьба «не читай» доступ не закрывает.

1. Храните секреты в менеджере паролей или хранилище секретов; если нужен файл — шифруйте его проверенным локальным средством **до отправки** (не используя придуманные самой языковой моделью схемы шифрования).
2. Ключ расшифрования храните отдельно от данных и вне доступа помощника.
3. Технически заблокируйте для модели чтение файлов с ключами и их вывод в ответы и логи ([OWASP Cryptographic Storage](#)).

8. Проверка и передача результата

37 Сервис безопасен — можно доверять выводам?

Нет: **безопасность обработки данных и фактическая правильность ответа проверяются отдельно.**

- Сверяйте расчёты с исходными цифрами и формулой, ссылки на законы — с актуальной редакцией нормы, выводы — с текстом документа; каждую приведённую ссылку открывайте и проверяйте.
- На ответ «ошибок не найдено» уточняйте, что именно проверялось.

- Код и команды запускайте сначала в изолированной тестовой среде; для решений с последствиями назначайте профильного проверяющего специалиста.

38 Переслать ответ коллегам или дать общую ссылку на чат?

Проверьте, какие сведения остались в ответе и кому их разрешено передавать. Краткое саммари может сохранить имена, суммы и суть коммерческой тайны — пересказ моделью ограничений не снимает. При создании общей ссылки на диалог проверяйте, что именно она открывает (один ответ, всю историю чата или загруженные исходные файлы) и кто может по ней перейти.

9. Ошибка или нехватка правил

39 Данные уже отправлены не туда?

Немедленно прекратите передачу и сообщите в ИБ, ответственному за ПДн (DPO) и руководителю.

1. **Вводные для расследования:** время, сервис, аккаунт, состав сведений, ID операции/чата. **Сам секретный файл или раскрытый пароль в письме повторно не пересылайте!**

2. **Отзыв секретов:** скомпрометированные ключи и пароли немедленно отозвать (заменить), обновить в зависимых сервисах и проверить логи использования ([руководство GitHub](#)).

3. **Оценка инцидента и сроки РКН:** не всякая ошибочная отправка означает публичную утечку, но ситуацию оперативно оценивает ответственный за ПДн по ч. 3.1 ст. 21 152-ФЗ. При установлении неправомерной или случайной передачи/доступа к ПДн, повлекших нарушение прав людей, оператор уведомляет РКН **в течение 24 часов**, а о результатах внутреннего расследования — **в течение 72 часов** с момента выявления.
4. **Уведомление клиента (при работе по поручению):** строго по договорной процедуре; «полного удаления данных» не обещать до официального подтверждения поставщиком сервиса.

40 Разрешённый инструмент слабый, а срок горит?

Срочность правил безопасности не отменяет. Разделите задачу:

- Если внешний сервис разрешён для общих задач — подготовьте в нём структуру, список вопросов или проверьте логику **на вымышленном примере**, а реальные данные внесите вручную в разрешённой корпоративной системе.
- Если без закрытых данных нельзя, а подходящего AI нет — выполните работу без AI и подайте заявку руководству и ИТ (какой бизнес-результат нужен, какие данные задействованы и чего не хватает текущему решению).
- Если проблема регулярная — сравните с руководителем и ИТ другой режим/сервис, локальное решение, изменение процесса или обычную автоматизацию (с учётом затрат и требований к данным: локальность сама по себе решение лучшим или допустимым не делает).

41 Как задать ИТ, юристу или ИБ предметный вопрос?

Отправьте карточку описания операции (без приложения самого секретного файла в общий чат):

- **Задача:** какой результат нужен и зачем.
- **Данные:** откуда берутся и что содержат (ПДн, NDA, чужие авторские материалы).
- **Инструмент:** название сервиса, тариф, тип аккаунта и режим работы.
- **Действия помощника:** что именно читает, может ли менять или отправлять данные.
- **Условия обработки:** кто получает, где и сколько хранят, какие внешние функции включены (*укажите, какие из этих условий вам нужно помочь уточнить*).
- **Проверка результата:** кто проверит ответ и кому он будет доступен.
- **Вопрос:** допустима ли операция и какие условия нужно выполнить для запуска?

42 Что руководителю установить в первую очередь?

1. Перечень разрешённых сочетаний «Задача + Категория данных + Сервис + Режим» с примерами и чёткой границей нового согласования.
2. Корпоративные аккаунты и обязательная двухфакторная аутентификация (где поддерживается).
3. Правила хранения, удаления и подключения новых источников данных.
4. Требования к проверке ответов и подтверждению действий помощника человеком.
5. Быстрый и понятный канал сообщения об инциденте.
6. Ответственный за пересмотр правил (при смене поставщика, тарифа, договора, политики обучения, сроков хранения, подключений или после инцидентов).

Практический ориентир (не норма права РФ): руководство WIPO по генеративному AI.

Чек-лист: семь проверок перед работой с данными в AI

1. **Задача:** какие сведения реально необходимы для результата и нельзя ли обойтись вымышленным примером.
2. **Права на данные:** предусмотрены ли цель и основание обработки ПДн, ограничения конфиденциальности, клиентских договоров и авторских прав; неясное уточните у ответственного до передачи.
3. **Способ обработки:** допустимый сервис, тип аккаунта, режим работы, активные подключения, правила хранения и удаления.
4. **Минимальный материал:** убрать лишнее, **никогда не вставлять пароли и ключи**, проверить скрытые слои (скрытые листы и строки, непринятые исправления, кэш сводных таблиц, физическое удаление текста в PDF через Redaction вместо чёрных плашек) и сохранить смысл задачи.
5. **Доступ и действия:** только нужные папки и минимум полномочий (чтение вместо автоматической отправки писем или изменения записей).
6. **Проверка результата:** кто сверит факты, расчёты, нормы законов и код; кому можно пересылать ответ; какие действия подтверждает человек.
7. **Реагирование:** контакты службы ИБ и ответственного за ПДн под рукой на случай ошибочной отправки или компрометации ключей.

Если существенное условие безопасности неизвестно — уточните его до отправки спорных данных, а общую часть задачи выполните без закрытых сведений в разрешённом инструменте.