УТВЕРЖДАЮ

Директор ООО «МастерДрон»  
Борисенко А. А.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

**Политика   
в отношении персональных данных в  
 ООО «МастерДрон»**

Санкт-Петербург, 2025

# Общие положения

## Назначение Политики

* + 1. Политика в отношении администрирования сетей и работы с персональными данными в ООО «МастерДрон» (далее — Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ГОСТ Р 57580-2017 «Безопасность информационных технологий» и принятыми в соответствии с ними Приказами ФСТЭК России и ФСБ России.
    2. Политика вступает в силу с момента ее утверждения директором или иным уполномоченным лицом Предприятия.
    3. Политика подлежит пересмотру в ходе периодического анализа, но не реже одного раза в год, ответственного за организацию обработки персональных данных  
       на Предприятии, а также в случаях изменения законодательства Российской Федерации  
       в области персональных данных.
    4. Политика подлежит опубликованию на официальном сайте Предприятия ([https://*master-dron.ru*](https://master-dron.ru)*)*

## Цели Политики

## Обеспечение конфиденциальности, целостности и доступности персональных данных сотрудников и клиентов, минимизация рисков, связанных с утечкой, несанкционированным доступом или искажением персональных данных.

## Роль политики в реализации целей

## Политика работы с персональными данными направлена на защиту персональных данных сотрудников и клиентов, обеспечение их конфиденциальности, целостности и доступности, а также на соблюдение законодательства в области обработки персональных данных. Это способствует достижению целей информационной безопасности: конфиденциальности, целостности и доступности информации.

## Область действия

* + 1. Политика работы с персональными данными распространяется на: все подразделения организации, обрабатывающие персональные данные сотрудников и клиентов; все информационные системы, используемые для обработки персональных данных.
    2. Настоящей Политикой должны руководствоваться все работники Предприятия, осуществляющие обработку персональных данных или имеющие к ним доступ.

## Вид деятельности, на обеспечение информационной безопасности которой направлено действие положений политики

* Обработка персональных данных сотрудников (кадровый учет, расчет заработной платы).
* Обработка персональных данных клиентов (ведение клиентских баз, обработка заказов).
* Хранение и архивирование персональных данных.
  1. **Совокупность информационных технологий и технологических процессов**
     1. **Информационных технологии**
        1. Системы управления базами данных (СУБД).
        2. CRM-системы.
        3. ERP-системы.
        4. Средства криптографической защиты информации.
        5. Системы резервного копирования и восстановления данных.
     2. **Технологические процессы:**
        1. Сбор и ввод персональных данных (например, заполнение анкет, регистрация клиентов, оформление трудовых договоров).
        2. Обработка данных (например, кадровый учет, расчет заработной платы, обработка заказов клиентов).
        3. Хранение данных (в защищенных базах данных, с использованием шифрования и ограниченного доступа).
        4. Передача данных (внутри организации и внешним контрагентам с использованием защищенных каналов связи, таких как VPN или TLS).
        5. Уничтожение данных (по истечении срока хранения или при достижении цели обработки, с использованием безопасных методов уничтожения, таких как стирание данных или физическое уничтожение носителей).
        6. Мониторинг и аудит доступа к персональным данным (ведение журналов событий, анализ подозрительной активности).
        7. Реагирование на инциденты, связанные с утечкой или несанкционированным доступом к персональным данным.
  2. **Субъекты (роли), на которых распространяется действие политики:**
     1. Отдел кадров;
     2. Бухгалтерия;
     3. IT-отдел;
     4. Отдел маркетинга и продаж;
     5. Сотрудники, имеющие доступ к персональным данным;
     6. Внешние подрядчики и партнеры, обрабатывающие персональные данные от имени организации.

1. **Требования и правила**
   1. Конфиденциальность: Персональные данные должны быть доступны только авторизованным лицам.
   2. Целостность: Данные должны быть защищены от несанкционированного изменения.
   3. Доступность: Данные должны быть доступны авторизованным пользователям в рамках их рабочих задач.
   4. Сбор данных: Персональные данные собираются только в объеме, необходимом для выполнения конкретных задач.
   5. Хранение: Данные хранятся в защищенных системах с ограниченным доступом.
   6. Передача: Передача данных третьим лицам возможна только с согласия субъекта данных или в рамках законодательства.
   7. Уничтожение: Данные уничтожаются по истечении срока хранения или при достижении цели обработки.
2. **Функции субъектов над управляемыми объектами**
   1. Отдел кадров: Ведение и обновление баз данных сотрудников.
   2. Бухгалтерия: Обработка и хранение финансовых данных.
3. **Положения по контролю реализации политики**
   1. **Организация контроля**
      1. **Ответственные за контроль:**

* Контроль выполнения политики возлагается на отдел информационной безопасности (ИБ) совместно со специалистом по безопасности данных.
* Руководитель ИТ-отдела отвечает за организацию и координацию контрольных мероприятий.
  + 1. **Периодичность контроля:**
* Проведение плановых проверок не реже одного раза в квартал.
* Внеплановые проверки в случае выявления инцидентов или подозрений на нарушения.
  1. **Методы контроля**
     1. **Аудит документации:**
* Проверка журналов изменений конфигураций сетевого оборудования.
* Анализ документации по настройке и эксплуатации сетевых устройств.
  + 1. **Мониторинг сетевой активности:**
* Постоянный мониторинг сетевого трафика с использованием систем SIEM (Security Information and Event Management).
* Анализ журналов событий на предмет несанкционированного доступа или попыток нарушения конфиденциальности ПДн.
  + 1. **Тестирование на проникновение:**
* Проведение регулярных тестов на проникновение (penetration testing) для выявления уязвимостей. Выявление уязвимостей в системах обработки ПДн, которые могут привести к утечке данных.
* Использование автоматизированных инструментов для сканирования сети. Проверка защищенности инфраструктуры, где хранятся и обрабатываются ПДн.
  + 1. **Проверка соблюдения правил:**
* Контроль за соблюдением политик обработки ПДн: Проверка, что сотрудники соблюдают установленные правила работы с персональными данными.
* Проверка наличия и актуальности средств защиты: Контроль за использованием антивирусного ПО, шифрования данных и других средств защиты на устройствах, где обрабатываются ПДн.
  + 1. **Анализ инцидентов:**
* Исследование причин и последствий утечек ПДн: Анализ инцидентов, связанных с нарушением конфиденциальности персональных данных.
* Разработка рекомендаций по предотвращению утечек: Внедрение мер, направленных на минимизацию рисков повторения инцидентов.
  1. **Процедуры контроля**
     1. **Планирование контрольных мероприятий:**
* Исследование причин и последствий инцидентов ИБ.
* Разработка рекомендаций по предотвращению подобных инцидентов в будущем
  + 1. **Проведение проверок:**
* Сбор и анализ данных о выполнении требований политики.
* Проведение интервью с сотрудниками для выявления возможных нарушений.
  + 1. **Фиксация результатов:**
* Составление отчетов по результатам проверок.
* Ведение журнала контрольных мероприятий.
  + 1. **Устранение нарушений:**
* Разработка плана мероприятий по устранению выявленных нарушений.
* Контроль за выполнением корректирующих действий.
  1. **Отчетность**
     1. **Формирование отчетов:**
* Ежеквартальные отчеты о выполнении требований политики.
* Отчеты по результатам тестов на проникновение и аудитов.
  + 1. **Представление отчетов:**
* Предоставление отчетов руководителю ИТ-отдела и высшему руководству.
* Обсуждение результатов на совещаниях по информационной безопасности.
  1. **Ответственность за нарушения**
     1. **Выявление нарушений:**
* Фиксация фактов нарушений требований политики.
* Проведение расследования для установления причин нарушений.
  + 1. **Применение санкций:**
* Наложение дисциплинарных взысканий на сотрудников, допустивших нарушения.
* В случае серьезных нарушений — передача дела в компетентные органы.

1. **Ответственность за реализацию и поддержку документа**

* Ответственность за реализацию политики возлагается на отдел кадров и руководителя ИТ-отдела.
* Отдел ИБ отвечает за контроль выполнения требований.

1. **Условия пересмотра документа**

Данная политика может быть пересмотрена, если:

* Произошли изменения законодательства в области ИБ.
* Были внедрены новые технологий.
* Возникли новые, не рассмотренные ранее, угрозы ИБ.
* В результате аудитов и инцидентов были сделаны выводы о необходимости пересмотра данной политики.