УТВЕРЖДАЮ

Директор ООО «МастерДрон»  
Борисенко А. А.

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

**Политика   
в отношении администрирования сетей в  
 ООО «МастерДрон»**

Санкт-Петербург, 2025

# Общие положения

## Назначение Политики

## Политика в отношении администрирования сетей на заводе по производству гражданских дронов 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 Приказы ФСТЭК России и ФСБ России.

* + 1. Политика вступает в силу с момента ее утверждения директором или иным уполномоченным лицом Предприятия.
    2. 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.
    3. Политика подлежит опубликованию на официальном сайте Предприятия ([https://*master-dron.ru*](https://master-dron.ru)*)*

## Цели Политики

## Целью Политики является обеспечение конфиденциальности и целостности данных, а также обеспечение доступности сетевых ресурсов и минимизация рисков кибератак.

## Роль политики в реализации целей

* + 1. Политика администрирования сетей направлена на обеспечение безопасности сетевой инфраструктуры завода, защиту данных от несанкционированного доступа, минимизацию рисков кибератак и обеспечение стабильной работы сетевых ресурсов. Это способствует достижению целей информационной безопасности: конфиденциальности, целостности и доступности информации.

## Область действия

* + 1. Область действия политики распространяется на: Корпоративную сеть завода, Сети производственных цехов, Серверное оборудование, Сетевые устройства (маршрутизаторы, коммутаторы, точки доступа), Системы удалённого доступа (VPN).
    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

* Администрирование корпоративной сети.
* Обеспечение безопасности данных, передаваемых по сети.
* Управление доступом к сетевым ресурсам.
* Мониторинг сетевой активности.
* Реагирование на сетевые инциденты.
  1. **Совокупность информационных технологий и технологических процессов**
     1. **Сетевые технологии:** Ethernet, Wi-Fi, VPN
     2. Сетевые устройства: маршрутизаторы, коммутаторы, межсетевые экраны
     3. **Системы мониторинга:** Zabbix, Nagios
     4. **Технологические процессы:** настройка сетевого оборудования, управление трафиком, резервное копирование конфигураций
  2. **Субъекты (роли), на которых распространяется действие политики**
* Сетевые администраторы.
* Отдел информационной безопасности.
* Руководитель ИТ-отдела.
* Сотрудники, использующие сетевые ресурсы.

1. **Требования и правила**
   1. **Требования и правила управление доступом**
      1. **Аутентификация и авторизация:**

* Для доступа к сетевым ресурсам должна использоваться строгая аутентификация (двухфакторная аутентификация для администраторов).
* Учетные записи пользователей должны создаваться только после утверждения заявки руководителем подразделения.
* Пароли должны соответствовать требованиям сложности: минимум 12 символов, использование заглавных и строчных букв, цифр и специальных символов.
* Пароли должны обновляться каждые 90 дней.
  + 1. **Управление правами доступа:**
* Права доступа должны предоставляться в соответствии с принципом минимальных привилегий (только те права, которые необходимы для выполнения должностных обязанностей).
* Регулярный пересмотр прав доступа (не реже одного раза в квартал) для выявления и устранения избыточных прав.
* Удаление учетных записей уволенных сотрудников в течение одного рабочего дня.
  1. **Требования и правила управление доступом**
     1. **Использование межсетевых экранов (firewall):**
* Все входящие и исходящие соединения должны фильтроваться с использованием межсетевых экранов.
* Правила фильтрации должны регулярно пересматриваться и обновляться.
  + 1. **Шифрование данных**
* Все данные, передаваемые по сети, должны шифроваться с использованием современных криптографических алгоритмов (например, AES-256).
* Для удаленного доступа к корпоративной сети должны использоваться VPN-соединения**.**
  + 1. **Защита от вредоносного ПО:**
* На всех сетевых устройствах и конечных точках должно быть установлено антивирусное ПО с регулярным обновлением баз сигнатур.
* Проведение регулярного сканирования сети на наличие вредоносного ПО.
  1. **Требования и правила для мониторинга сетевой активности**
     1. **Ведение журналов событий:**
* Все сетевые устройства должны вести журналы событий, включая информацию о попытках доступа, изменениях конфигураций и аномальной активности.
* Журналы событий должны храниться не менее 6 месяцев.
  + 1. **Анализ сетевого трафика:**
* Регулярный мониторинг сетевого трафика для выявления подозрительной активности (например, необычно высокий объем трафика, попытки доступа к закрытым ресурсам).
* Использование систем предотвращения вторжений (IPS) для автоматического блокирования атак.
  1. **Требования и правила при реагировании на инциденты**
     1. **Процедура реагирования:**
* При обнаружении подозрительной активности или инцидента ИБ сотрудник обязан немедленно сообщить в отдел информационной безопасности.
* Отдел ИБ должен провести анализ инцидента и принять меры для его устранения.
  + 1. **План восстановления:**
* Разработка и регулярное обновление плана восстановления после инцидентов.
* Проведение тренировок по отработке действий в случае кибератак.
  1. **Требования и правила к резервному копированию и восстановлению**
     1. **Резервное копирование:**
* Регулярное резервное копирование конфигураций сетевого оборудования (не реже одного раза в неделю).
* Хранение резервных копий в защищенном месте с ограниченным доступом.
  + 1. **Восстановление:**
* Проведение тестового восстановления из резервных копий не реже одного раза в квартал для проверки их работоспособности
  1. **Требованию и правила обновления ПО и патчинга**
     1. **Обновление ПО:**
* Своевременное обновление программного обеспечения сетевых устройств и операционных систем.
* Установка патчей для устранения уязвимостей в течение 7 дней после их выпуска**.**
  + 1. **Управление изменениями:**
* Все изменения в конфигурации сетевого оборудования должны согласовываться с отделом ИБ и фиксироваться в журнале изменений.
  1. **Требования и правила к обучению и информированию сотрудников**
     1. **Обучение:**
* Проведение регулярных тренингов по основам информационной безопасности для сотрудников.
* Информирование о новых угрозах и способах их предотвращения.
  + 1. **Тестирование:**
* Проведение тестов на знание правил ИБ и действий в случае инцидентов.
  1. **Требования и правила к аудиту и контролю**
     1. **Проведение аудитов:**
* Регулярный аудит выполнения требований политики (не реже одного раза в квартал).
* Проведение тестов на проникновение для выявления уязвимостей
  + 1. **Контроль за соблюдением правил:**
* Мониторинг соблюдения правил использования сетевых ресурсов.
* Наложение санкций за нарушение требований политики
  1. **Требования и правила к оптимизации сетевой инфраструктуры**
     1. **Регулярное внесение улучшений**
* Регулярный анализ производительности и безопасности сети.
* Внедрение новых технологий для повышения уровня защиты**.**
  + 1. **Документирование:**
* Ведение документации по настройке и конфигурации сетевого оборудования.
* Регулярное обновление документации при внесении изменений

1. **Функции субъектов над управляемыми объектами**
2. Функции сетевых администраторов:
   1. Настройка и обслуживание сетевого оборудования.
   2. Управление доступом к сетевым ресурсам.
3. Функции отдела информационной безопасности:
   1. Анализ журналов событий.
   2. Проведение аудитов безопасности.
4. Функции других сотрудников:
   1. Соблюдение правил использования сетевых ресурсов.
5. **Положения по контролю реализации политики**
   1. **Организация контроля**
      1. **Ответственные за контроль:**

* Контроль выполнения политики возлагается на отдел информационной безопасности (ИБ) совместно с сетевыми администраторами.
* 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 для выявления подозрительной активности.
  + 1. **Тестирование на проникновение:**
* Проведение регулярных тестов на проникновение (penetration testing) для выявления уязвимостей.
* Использование автоматизированных инструментов для сканирования сети.
  + 1. **Проверка соблюдения правил:**
* Контроль за соблюдением правил использования сетевых ресурсов сотрудниками.
* Проверка наличия и актуальности антивирусного ПО на всех устройствах.
  + 1. **Анализ инцидентов:**
* Исследование причин и последствий инцидентов ИБ.
* Разработка рекомендаций по предотвращению подобных инцидентов в будущем
  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 сетевых администраторов 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 внедрение новых технологий.
* Возникли новые, не рассмотренные ранее, угрозы ИБ.
* В результате аудитов и инцидентов были сделаны выводы о необходимости пересмотра данной политики.