

Министерство просвещения Республики Башкортостан  
Государственное автономное профессиональное образовательное  
учреждение

Уфимский колледж статистики, информатики и вычислительной техники

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОФОРМЛЕНИЮ ОТЧЕТА  
ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ**

**ПП.04.01 Производственная практика**

по модулю ПМ.04 Сопровождение и обслуживание программного  
обеспечение компьютерных систем

**Специальность СПО**

**09.02.07 Информационные системы и программирование**

**Квалификация**

**Программист**

**2025**

Одобрено  
предметной цикловой комиссией  
информатики  
«\_\_\_\_» \_\_\_\_\_ 2025 г.

Составлено в соответствии  
с Государственными требованиями  
к минимуму содержания  
и уровню подготовки выпускника  
по специальностям 09.02.07

Председатель  
предметной цикловой комиссии

Заместитель директора  
по учебной работе

\_\_\_\_\_ Фатхулова О.В.

\_\_\_\_\_ Курмашева З.З.

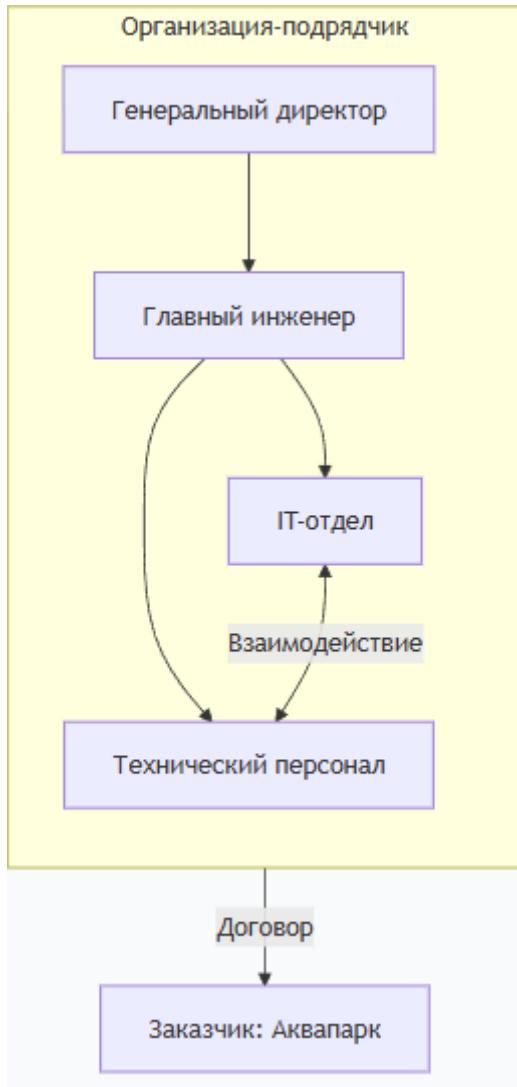
*Составители:*

Фатхулова О.В.

преподаватель  
специальных дисциплин УКСИВТ

## **Характеристика организационной и функциональной структуры системы управления предприятия с перечнем задач**

1. О компании: Акватехсервис, занимается обслуживанием бассейнов по всей России и продажей химии, количество сотрудников в компании 100+.
2. Организационная структура:



3. Функциональная структура вашего отдела: «В IT-отделе работают 3 человека: начальник отдела (Координирование задач и информирование), 2 специалиста ИТ (Обслуживание оборудований, администрирование АСУ ТП, Развёртывание сетевой инфраструктуры и тд)»

#### 4. Перечень задач отдела

«Основные задачи ИТ-отдела: 1) Обеспечение бесперебойной работы корпоративной сети и серверного оборудования; 2) Администрирование рабочих станций 3) Техническая поддержка пользователей 4) Защита данных и резервное копирование; 5) администрирование SCADA-систем 6) Интеграция датчиков и исполнительных механизмов 7) Плановая проверка оборудования  
8) Обеспечение отказоустойчивости и безопасности АСУ ТП.

## **Сопровождение и обслуживание программного обеспечения предприятия**

В ходе практики мною был проведён анализ существующей ИТ-инфраструктуры и систем автоматизации аквапарка, а также выполнены практические работы по их настройке и обслуживанию. Основное внимание уделялось системам, обеспечивающим безопасность и непрерывность технологических процессов.

### **2.1 Анализ аппаратного и программного обеспечения**

Парк пользовательских ПК: 3 станций на базе Intel Core i5, 8-16 ГБ ОЗУ.

Серверная: 3 физических сервера Dell (Windows Server 2019).

На рабочих станциях — Windows 10 Pro. На серверах — Windows Server 2019 Standard (роли: AD DS, DNS, DHCP, файловое хранилище). Для виртуализации используется VMware vSphere

Основное технологическое ПО: SCADA-система для мониторинга, СУБД Microsoft SQL Server и PostgreSQL для архивов данных.

### **2.2 Анализ сетевого обеспечения предприятия**

1. Корпоративная сеть: Для офисных ПК, серверов, IP-телефонии. Доступ в Интернет.
2. Технологическая сеть АСУ ТП: Для ПЛК, SCADA-серверов и рабочих станций операторов. Доступ в Интернет и в корпоративную сеть строго ограничен межсетевым экраном.

Основное активное оборудование: маршрутизатор Mikrotik RB4011, управляемые коммутаторы Cisco SG350, межсетевой экран NGFW Palo Alto PA-220.

Применённая сегментация повышает безопасность. Так же для мониторинга имеется настроенная система сбора сетевых логов Zabbix.

## 2.3 Анализ антивирусных программ

Для защиты от вредоносного ПО на предприятии используется комплекс MICROSOFT WINDOWS DEFENDER. Установлены на всех 3 рабочих станциях и 3 серверах. Управление осуществляется через встроенный интерфейс. Настроены ежедневные полные проверки в нерабочее время, политики контроля устройств USB.

## 2.4 Настройка защиты системы стандартными средствами операционной системы

Что было сделано:

### 1. Настройка Microsoft Defender:

- Включил защиту в реальном времени и облачную защиту для быстрого обнаружения новых вирусов.
- Активировал контролируемый доступ к папкам, чтобы защитить важные данные (архивы SCADA) от шифровальщиков-вымогателей.
- Настроил автоматические проверки по расписанию.

### 2. Ограничение запуска программ:

- Через Редактор локальной групповой политики создал правило AppLocker.
- Правило разрешает запуск программ только из системных папок (C:\Windows\, C:\Program Files\) и специального каталога с рабочим ПО. Это блокирует запуск непроверенных программ с флешек или из интернета.

### 3. Настройка сетевого экрана (брандмауэра Windows):

- Создал строгое правило для брандмауэра.
- Правило разрешает подключение к SCADA-серверу (по порту 4840) только с компьютеров в технологической сети аквапарка. Все остальные попытки соединения блокируются.