МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т. Ф. ГОРБАЧЕВА»
Филиал КузГТУ в г. Белово

Кафедра инженерно-экономическая

ПП.06.01 «Сопровождение информационных систем»

Методические рекомендации
по выполнению производственной практики
для специальности
09.02.07 «Информационные системы и программирование»

Составитель: Витвицкий М.Н.
Рассмотрены и утверждены на заседании кафедры
Протокол № 6 от 14.02.2026 г.
Рекомендовано учебно-методической комиссией специальностей СПО в качестве электронного издания для использования в учебном процессе
Протокол № 6 от 17.02.2026 г.

Долганова Жанна Александровна
Подписано цифровой подписью: Долганова Жанна Александровна
Дата: 2026.02.18 11:14:33 +07'00'

Белово 2026

СОДЕРЖАНИЕ

ОРГАНИЗАЦИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Первоначальные профессиональные навыки обучающиеся по основным профессиональным образовательным программам получают во время прохождения учебных и производственных практик. Практика имеет целью комплексное освоение обучающимися всех видов профессиональной деятельности по специальности (профессии) среднего профессионального образования, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по специальности (профессии).

Практика по профилю специальности направлена на формирование у обучающегося общих и профессиональных компетенций, приобретение практического опыта и реализуется в рамках профессиональных модулей ОП СПО по каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО по специальности.

Производственная практика проводится в организациях и учреждениях в отделах и подразделениях IT. Организацию и руководство практикой по профилю специальности (профессии) осуществляют руководители практики из числа профессорско-преподавательского состава филиала КузГТУ в г.Белово и руководитель практики от организации.

Руководитель практики из числа лиц, относящихся к профессорско-преподавательскому составу филиала:

- разрабатывает содержание и планируемые результаты практики;

- осуществляет общее руководство практикой;

- контролирует реализацию программы практики и условия проведения практики, в том числе требования охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми;

- формирует группы в случае применения групповых форм проведения практики;

- определяет процедуру оценки общих и профессиональных компетенций обучающегося, освоенных им в ходе прохождения практики;

- разрабатывает формы отчетности и оценочный материал прохождения практики.

Руководитель практики из числа лиц, относящихся к сотрудникам IT-отдела в организации где проходит практика:

- согласовывает содержание и планируемые результаты практики;

- осуществляет руководство практикой в организации;

- организует реализацию программы практики и условия проведения практики, в том числе требования охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми;

- оценивает применение общих и профессиональных компетенций обучающегося, используемых им в ходе прохождения практики.

Обучающиеся в период прохождения практики обязаны:

- выполнять задания, предусмотренные программами практики;

- соблюдать действующие в организации для прохождения практики правила его внутреннего трудового распорядка;

- соблюдать требования охраны труда и пожарной безопасности.

Результаты практики определяются программами практики, разрабатываемыми руководителями практики из числа профессорско-преподавательского состава филиала КузГТУ в г.Белово. По результатам практики руководителем практики формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению профессиональных компетенций в период прохождения практики.

В период прохождения практики обучающимся ведется дневник практики. По результатам практики обучающимся составляется отчет. В качестве приложения к дневнику практики обучающийся оформляет графические, аудио-, фото-, видеоматериалы, подтверждающие практический опыт, полученный на практике.

Аттестация по итогам учебной практики проводится с учетом (или на основании) результатов ее прохождения, подтверждаемых аттестационным листом.

Отчет по практике является основным документом, характеризующим работу обучающегося во время практики. Отчет составляется в соответствии с программой практики и содержит следующие разделы:

1. Титульный лист

2. Задание на производственную практику

3. Введение

4. Теоретические основы в соответствии с темами практики

5. Реализация поставленной задачи

6. Выводы

7. Список используемой литературы

Комплект документов, оформляемых при прохождении производственной практики, а также титульный лист отчета по производственной практике приведены в Приложении А-Д.

КОНТРОЛЬ РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ ЗАДНИЙ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Контроль результатов по производственной практике студентов осуществляться в пределах времени, отведенного на обязательные учебные занятия, может проходить в письменной, устной или смешанной форме, с представлением продукта деятельности учащегося.

В качестве форм и методов контроля работы обучающихся, могут быть использованы, зачеты, тестирование, самоотчеты по этапам практики, практические задания, и др., которые могут осуществляться на учебном занятии или вне его.

Общими критериями оценки результатов работы обучающегося являются:

- уровень применения студентом навыков и компетенций;
- умение обучающегося использовать теоретические знания при выполнении практических задач;
- полнота сформированных общих и профессиональных компетенций;
- обоснованность и четкость выполнения производственных задач;
- оформление необходимого материала в соответствии с требованиями.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА 06.01 «Сопровождение информационных систем».

Производственная практика — это метод обучения студентов в высших учебных заведениях, направленный на приобретение практических навыков и опыта работы в определенной отрасли. Она является важной составляющей образовательного процесса и представляет собой переход от теоретических знаний к их практическому применению.

Цель производственной практики 06.01 «Сопровождение информационных систем».

Комплексное освоение обучающимися вида профессиональной деятельности «Сопровождение информационных систем», формирование общих и профессиональных компетенций, приобретение необходимого опыта практической работы по специальности.

Задачи производственной практики 06.01 «Сопровождение информационных систем».

Осуществление инсталляции, настройки и сопровождения информационных систем.

Выполнение регламентов по обновлению, техническому сопровождению и восстановлению данных информационной системы.

Сохранение и восстановление базы данных информационной системы.

Организация доступа пользователей к информационной системе в рамках компетенции конкретного пользователя.

Модификация отдельных модулей информационной системы.

Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Работа с профессиональной документацией и взаимодействие с коллегами и руководством.

Сбор материала для будущей дипломной работы, анализ производственных процессов, участие в проектной деятельности.

Производственная практика осуществляется в форме:

1. Выполнения поставленных учебных и производственных задач

Задания по производственной практике

№ раздела (темы)	Вопросы, выносимые на изучение	Количество часов
Тема 1. Сопровождение информационных систем.	Задание1.1. Настройка доступа к сетевым устройствам.	6
	Задание 1.2. Настройка политики безопасности.	6
	Задание1.3. Создание резервной копии информационной системы.	6
	Задание1.4. Создание резервной копии базы данных	6
	Задание1.5. Восстановление данных.	6
	Задание1.6. Восстановление информационной системы.	6
	Задание1.7. Сбор информации об ошибках. Формирование отчетов об ошибках.	6
	Задание1.8. Выполнение обслуживания информационной системы в соответствии с пользовательской документацией.	6
	Задание1.9. Обслуживание локальной сети.	6
	Задание1.10. Обслуживание системы видеонаблюдения.	6
	Задание1.11. Обслуживание облачной информационной системы.	6
Тема 2. Документирование процессов внедрения и сопровождения информационных систем.	Задание2.1. Разработка сценария внедрения информационной системы для рабочего места.	6
	Задание2.2. Разработка технического задания на внедрение информационной системы.	6
	Задание2.3. Разработка графика разработки и внедрения информационной системы.	6
	Задание2.4. Разработка перечня обучающей документации на информационную систему.	6
	Задание2.5. Разработка технического задания на	6

	сопровождение информационной системы.	
	Задание2.6. Формирование предложений о расширении информационной системы.	6
	Задание2.7. Разработка руководства оператора.	6
Промежуточная аттестация в форме: зачета.		

Типовые вопросы на защиту отчета

1. Классификация информационных систем.

2. Этапы внедрения информационной системы.

3. Основные задачи сопровождения информационной системы.

4. Способы идентификации ошибок, возникающих в процессе эксплуатации системы.

5. Способы коррекции ошибок, возникающих в процессе эксплуатации системы.

6. Способы резервного копирования информации.

7. Способы настройки сетевого оборудования.

8. Особенности эксплуатации облачных информационных систем.

9. Методы разработки сценариев внедрения информационных систем.

10. Методы разработки технического задания.

11. Методы разработки календарных графиков разработки и внедрения информационных систем.

12. Состав эксплуатационной документации на информационную систему.

13. Требования к оформлению эксплуатационной документации на информационную систему.

14. Состав обучающей документации на информационную систему.

15. Методы разработки эксплуатационной документации на информационную систему.

ТЕМА 1. СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ.

Практические рекомендации**.**

При организация работы **отдать больше внимания:**

1. Планирование времени: распределение задач, приоритизации, контроль сроков.

2. Коммуникация: взаимодействие с сотрудниками организации, общение с пользователями, **о**тчетность**.**

Контроль качества **осуществлять через**: **т**естирование изменений**, п**роверка работоспособности**, о**ценка производительности**, н**епрерывное улучшение **(а**нализ проблем**, о**птимизация процессов**, в**недрение лучших практик**)/**

Критерии эффективности:

Время реакции на инциденты**;**

Процент успешно решенных проблем**;**

Количество критических ошибок**;**

Удовлетворенность пользователей**.**

Метрики качества:

Доступность системы**;**

Производительность**;**

Безопасность**;**

Соответствие требованиям**.**

Задание 1.1. Настройка доступа к сетевым устройствам.

Общие принципы настройки доступа

Основные правила безопасности:

- Минимизация открытых портов.
- Использование надежных паролей.
- Применение многофакторной аутентификации.
- Регулярный аудит прав доступа.

Настройка доступа в Windows.

1. Базовая настройка.

- **Групповая политика безопасности:**
  - Настройка правил доступа через GPO.
  - Управление правами пользователей.

- Настройка аудита событий.

- **Настройка файрвола:**

```
powershell
New-NetFirewallRule -DisplayName "RemoteAccess" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 22
```

2. Настройка удаленного доступа

- **Remote Desktop:**
  - Включение удаленного доступа.
  - Настройка правил брандмауэра.
  - Ограничение IP-адресов.
- **PowerShell Remoting:**

```
powershell
Enable-PSRemoting -Force
Set-PSSessionConfiguration -Name Microsoft.PowerShell -Permission "NT AUTHORITY\Authenticated Users"
```

Настройка доступа в Linux.

1. Базовая конфигурация.

- **SSH-сервер:**
  - Редактирование файла `/etc/ssh/sshd_config`
  - Настройка портов и ключей.
  - Ограничение доступа по IP.
- **Файрвол UFW:**

```
bash
sudo ufw allow from 192.168.1.0/24
sudo ufw allow ssh
sudo ufw enable
```

2. Управление пользователями.

- **Создание групп:**

```
bash
sudo groupadd admin_group
sudo usermod -aG admin_group username
```

- **Настройка sudo прав:**

```bash
sudo visudo
# Добавление строки:
%admin_group ALL=(ALL) NOPASSWD:ALL
```

Межплатформенная интеграция.

1. Настройка единого доступа.

- **Active Directory интеграция:**
  - Настройка Samba для Linux.
  - Использование Kerberos.
  - LDAP-аутентификация.
- **Настройка Samba:**

```bash
sudo apt-get install samba
sudo nano /etc/samba/smb.conf
# Настройка параметров безопасности
```

Мониторинг и аудит

1. Инструменты мониторинга.

- **Windows:**
  - Event Viewer.
  - Performance Monitor.
  - PowerShell Logging.
- **Linux:**
  - Journalctl.
  - Auditd.
  - Rsyslog.

2. Настройка журналирования.

- **Логирование подключений:**

```bash
# Для Linux
sudo sysctl kernel.sysrq=1
sudo sysctl fs.suid_dumpable=2
```

- **Настройка ротации логов:**

```
bash
sudo nano /etc/logrotate.conf
# Настройка параметров ротации
```

Рекомендации по безопасности

1. **Регулярное обновление:**
- Проверка обновлений безопасности.
- Установка патчей.
- Обновление конфигураций.
2. **Тестирование доступа:**
- Проверка прав доступа.
- Тестирование уязвимостей.
- Стресс-тестирование.
3. **Документация:**
- Ведение журнала изменений.
- Документирование настроек.
- Создание инструкций по восстановлению.

Примеры типичных конфигураций.

Пример конфигурации SSH.

```
bash
# /etc/ssh/sshd_config
Port 22
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
UsePrivilegeSeparation yes
KeyRegenerationInterval 3600
ServerKeyBits 1024
SyslogFacility AUTH
LogLevel INFO
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
RSAAuthentication yes
```

PubkeyAuthentication yes

IgnoreRhosts yes

RhostsRSAAuthentication no

HostbasedAuthentication no

PasswordAuthentication no

ChallengeResponseAuthentication no

Пример конфигурации Windows Firewall.

powershell

New-NetFirewallRule -DisplayName "SSH Access" -Direction Inbound -LocalPort 22 -Protocol TCP -Action Allow -RemoteAddress <IP-адрес>

New-NetFirewallRule -DisplayName "RDP Access" -Direction Inbound -LocalPort 3389 -Protocol TCP

Задание 1.2. Настройка политики безопасности.

Настройка политики безопасности в Windows

1. Использование редактора локальной групповой политики (GPO).

Для настройки параметров безопасности в Windows используется редактор локальной групповой политики (gpedit.msc). Он позволяет управлять правами пользователей, параметрами безопасности, настройками брандмауэра и другими аспектами.

Чтобы открыть редактор, нужно:

нажать Win + R, ввести gpedit.msc и нажать Enter;

в консоли развернуть разделы: Конфигурация компьютера → Параметры Windows → Параметры безопасности → Локальные политики.

2. Настройка учётных записей и паролей.

В разделе Account Policies можно настроить политику паролей (минимальная длина, срок действия, история паролей) и политику блокировки учётных записей (количество неудачных попыток входа, время блокировки).

Рекомендуется использовать многофакторную аутентификацию и запретить использование стандартных учётных записей (например, Administrator).

3. Управление правами пользователей.

В разделе Local Policies → User Rights Assignment можно назначать права пользователям и группам. Например, ограничить доступ к управлению системными службами или запретить запуск определённых приложений.

4. Настройка параметров безопасности.

В разделе Local Policies → Security Options можно настроить:

контроль учётных записей (UAC);

параметры брандмауэра;

ограничения на использование съёмных носителей;

параметры шифрования данных.

5. Аудит и журналирование.

В разделе Audit Policy можно настроить аудит событий (вход/выход из системы, доступ к файлам, изменения в системе). Это позволяет отслеживать подозрительную активность.

6. Обновление системы и ПО.

Регулярно устанавливайте обновления Windows и программного обеспечения. Используйте Центр обновления Windows или групповые политики для централизованного управления обновлениями.

7. Использование антивирусного ПО и брандмауэра.

Настройте встроенный брандмауэр Windows или используйте сторонние решения. Установите антивирусное ПО и регулярно обновляйте его базы данных.

Настройка политики безопасности в Linux

1. Управление учётными записями и правами.

Избегайте использования root-аккаунта для повседневной работы. Используйте sudo или su для получения привилегий суперпользователя.

Создавайте отдельных пользователей с минимальными необходимыми правами. Для настройки sudo используйте команду visudo и редактируйте файл /etc/sudoers.

2. Настройка SSH.

Отключите вход от имени root: в файле /etc/ssh/sshd_config установите PermitRootLogin no.

Отключите аутентификацию по паролю: установите PasswordAuthentication no и используйте SSH-ключи для доступа.

Измените порт SSH на нестандартный (например, с 22 на 58291) для снижения риска автоматизированных атак.

3. Использование Fail2Ban.

Установите и настройте утилиту Fail2Ban для блокировки IP-адресов после нескольких неудачных попыток подключения к SSH. В файле /etc/fail2ban/jail.local можно настроить таймаут блокировки и другие параметры.

4. Настройка брандмауэра.

Используйте iptables, ufw или firewalld для фильтрации трафика. Например, с помощью ufw можно разрешить доступ только с определённых IP-адресов:

bash

sudo ufw allow from 192.168.1.0/24

sudo ufw allow ssh

sudo ufw enable

5. Регулярные обновления.

Регулярно обновляйте ядро Linux и программное обеспечение с помощью менеджера пакетов (apt, yum, dnf и т. д.).

6. Контроль целостности системы.

Используйте инструменты вроде AIDE или Tripwire для отслеживания изменений в системных файлах.

7. Ограничение доступа к файловым системам.

При монтировании разделов используйте опции noexec, nodev и nosuid в файле /etc/fstab, чтобы ограничить выполнение бинарных файлов, доступ к устройствам и изменение прав доступа.

8. Аудит и логирование.

Настройте журналирование событий с помощью journalctl или rsyslog. Анализируйте логи на предмет подозрительной активности.

Общие рекомендации

Тестирование изменений. Перед применением политик на производственных системах тестируйте их в изолированной среде.

Резервное копирование. Регулярно создавайте резервные копии конфигурационных файлов и важных данных.

Обучение персонала. Проводите тренинги по информационной безопасности для пользователей и администраторов.

Регулярный аудит. Периодически проверяйте настройки безопасности и обновляйте политики в соответствии с новыми угрозами.

Соблюдение этих рекомендаций поможет повысить уровень безопасности систем и снизить риски несанкционированного доступа.

Задание1.3. Создание резервной копии информационной системы.

Создание резервной копии информационной системы (бэкапа) — ключевая мера для защиты данных и быстрого восстановления работы после сбоев, атак или других инцидентов. Подходы к резервному копированию различаются в зависимости от операционной системы.

Резервное копирование в Windows

Встроенные инструменты

В Windows можно использовать функцию «Создание образа системы». Для этого нужно:

Открыть «Панель управления», перейти в раздел «Система и безопасность», затем в «Резервное копирование и восстановление (Windows 7)».

Выбрать «Создание образа системы».

Указать место для сохранения копии. Подойдёт внешний жёсткий диск, SSD, сетевой накопитель или сервер. Важно: нельзя сохранять образ на том же диске, где установлена система — в случае сбоя копия будет недоступна.

Выбрать диски для архивации (по умолчанию включаются системный и зарезервированный разделы).

Запустить процесс копирования, который может занять от нескольких минут до нескольких часов в зависимости от объёма данных.

После создания образа можно дополнительно сформировать диск восстановления системы. Он понадобится для загрузки компьютера и доступа к средствам восстановления Windows.

Сторонние программы

Для более гибких возможностей (выборочное копирование, расписание задач, шифрование) можно использовать сторонние приложения, например:

Киберпротект — позволяет копировать отдельные файлы, содержимое всего компьютера или ОС, создавать клоны системных дисков, восстанавливать систему.

Handy Backup — предлагает инструменты для резервного копирования с защитой личных данных.

Macrium Reflect Free — поддерживает создание инкрементальных и дифференциальных резервных копий, автоматическое расписание.

Aomei Backupper Standard — позволяет создавать образы жёстких дисков и восстанавливать систему из них.

Рекомендации:

Регулярно обновляйте резервные копии согласно расписанию, адаптированному под частоту изменения данных.

Храните копии в нескольких местах (локально и в облаке, например) для повышения надёжности.

Тестируйте восстановление из бэкапа, чтобы убедиться в целостности данных и работоспособности процесса.

Используйте надёжные носители и контролируйте их состояние.

Резервное копирование в Linux

Утилита tar

Для создания архивов можно использовать команду tar. Например, чтобы создать сжатый архив с исключением некоторых директорий, выполните:

bash

sudo tar -cvzf backup.tgz --exclude=/proc --exclude=/lost+found --exclude=/backup.tgz --exclude=/mnt --exclude=/sys --exclude=/web /

Полученный архив нужно хранить отдельно и при необходимости использовать для восстановления данных.

Clonezilla

Это инструмент для создания образов дисков и разделов. Процесс включает:

Загрузка с ISO-образа Clonezilla Live.

Выбор языка и раскладки клавиатуры.

Запуск Clonezilla и выбор режима (например, device-image для создания образа раздела).

Указание места сохранения образа (локальное устройство, сеть и т. д.).

Выбор раздела для бэкапа и запуск процесса.

Rsync

Утилита для синхронизации данных и создания резервных копий с возможностью исключения файлов и директорий. Пример команды:

bash

sudo rsync -a /локальная_директория логин@ip_адрес:/удалённая_директория

Для безопасности лучше использовать авторизацию по ключу.

Timeshift

Инструмент для создания снимков системы, который позволяет восстанавливать её в определённом состоянии. Установка в Ubuntu и производных:

bash

sudo add-apt-repository -y ppa:teejee2008/timeshift

sudo apt-get update

sudo apt-get install timeshift

После установки нужно настроить тип снимка (Rsync или Btrfs), место хранения, частоту и уровни копирования.

Рекомендации для Linux:

Регулярно создавайте резервные копии критически важных данных: настроек системы (директория /etc), пользовательских данных (/home), баз данных (используйте mysqldump для MySQL, pg_dump для PostgreSQL).

Используйте сжатие данных для экономии места (gzip, bzip2, lzma и т. д.).

Настройте ротацию копий, чтобы удалять устаревшие данные и освобождать место.

Для баз данных делайте логические копии (дампы), а не физические архивы файлов, чтобы избежать проблем с целостностью данных.

Храните резервные копии на удалённых носителях или в облаке.

Тестируйте восстановление, чтобы убедиться в работоспособности бэкапов.

Общие рекомендации

Независимо от ОС:

Регулярность. Настройте расписание резервного копирования в соответствии с частотой изменения данных.

Проверка целостности. Периодически проверяйте резервные копии на предмет ошибок и полноты данных.

Безопасность. Используйте шифрование для защиты чувствительных данных при хранении и передаче.

Документация. Ведите учёт настроек резервного копирования, мест хранения копий и инструкций по восстановлению.

Тестирование восстановления. Регулярно проводите тестовое восстановление, чтобы убедиться в работоспособности процесса и доступности данных.

Соблюдение этих рекомендаций поможет минимизировать риски потери данных и ускорить восстановление работы системы после сбоев.

Задание1.4. Создание резервной копии базы данных.

Основные принципы резервного копирования.

Ключевые принципы:

Регулярность — создание копий по расписанию.

Надёжность хранения — размещение копий в разных местах.

Контроль целостности — проверка работоспособности копий.

Минимизация простоев — копирование без остановки системы.

Разделение доступа — ограничение прав на создание копий.

Методы резервного копирования.

Основные типы:

Полное копирование — создание полной копии всей базы.

Инкрементное — копирование только измененных данных.

Дифференциальное — копирование с момента последнего полного бэкапа.

Инструменты резервного копирования.

Для SQL Server.

Создание резервной копии:

Через SQL Server Management Studio:

Правый клик по базе данных → Задачи → Создать резервную копию.

Выбор параметров и пути сохранения.

Через T-SQL:

sql

BACKUP DATABASE [ИмяБазы]

TO DISK = 'путь_к_файлу.bak'

WITH NOFORMAT, NOINIT, NAME = 'ИмяБазы-Full Database Backup'

Для MySQL

Использование mysqldump:

bash

mysqldump -u[пользователь] -p[пароль] [имя_базы] > [имя_файла].sql

Варианты использования:

Копирование нескольких баз:

bash

mysqldump -u[пользователь] -p --databases база1 база2 > backup.sql

Копирование всех баз:

bash

mysqldump -u[пользователь] -p --all-databases > all_databases.sql

Для PostgreSQL.

Использование pg_dump:

bash

pg_dump -U имя_пользователя имя_базы > backup.sql

Автоматизация процесса.

Способы автоматизации:

Cron-задачи для Linux.

Планировщик задач Windows.

Специализированные инструменты:

Barman для PostgreSQL.

pgBackRest.

Wal-G.

Практические рекомендации.

Подготовка к копированию:

Проверка активности пользователей.

Оценка свободного места.

Проверка прав доступа.

Хранение копий:

Использование разных носителей.

Организация системы ротации.

Шифрование важных данных.

Регулярная проверка целостности.

Проверка резервных копий.

Этапы проверки:

Тестирование восстановления на тестовом сервере.

Проверка размера файлов.

Контроль версий.

Документирование процесса.

Восстановление данных.

Порядок действий:

Остановка системы (при необходимости).

Проверка целостности резервной копии.

Запуск процесса восстановления.

Проверка работоспособности после восстановления.

Безопасность и контроль.

Меры защиты:

Ограничение доступа к копиям.

Шифрование чувствительных данных.

Регулярное обновление паролей.

Ведение журнала операций.

Документация процесса.

Обязательные элементы:

Инструкция по созданию копий.

Схема хранения.

Порядок восстановления.

Контакты ответственных лиц.

Журнал операций.

Мониторинг и отчётность.

Параметры контроля:

Успешность операций.

Время выполнения.

Размер копий.

Доступность хранилищ.

Уведомления об ошибках.

Задание1.5. Восстановление данных.

Общие принципы восстановления

Основные правила:

- Всегда создавать резервные копии.
- Не записывать новые данные на поврежденный носитель.
- Использовать специализированное ПО.
- Проводить восстановление на другом носителе.
- Документировать все действия.

Восстановление в Windows.

Системные инструменты.

Корзина Windows:

- Простой способ восстановления недавно удаленных файлов.
- Правый клик → Восстановить.
- Проверка папки “Удаленные файлы”.

Восстановление из резервной копии:

1. Открыть “Панель управления”.
2. Перейти в “Система и безопасность”.
3. Выбрать “Резервное копирование и восстановление”.
4. Нажать “Восстановить мои файлы”.

Командная строка.

Команда RECOVER:

```
cmd
RECOVER путь_к_файлу
```

Команда ATTRIB:

```
cmd
ATTRIB -H -R -S /S /D C:*.*
```

Специализированное ПО для Windows.

Популярные утилиты:

- **Recuva** — восстановление с жестких дисков и флешек.

- **EaseUS Data Recovery Wizard** — работа с поврежденными носителями.
- **Wondershare Recoverit** — восстановление различных типов файлов.
- **Disk Drill** — поддержка более 400 форматов файлов.

Восстановление в Linux.

Встроенные инструменты.

TestDisk:

- Восстановление удаленных разделов.
- Поиск и восстановление потерянных данных.
- Проверка файловой системы.

Photorec:

- Восстановление файлов без учета структуры папок.
- Поддержка различных файловых систем.
- Сохранение в указанную директорию.

Команды восстановления.

Создание образа диска:

```
bash
sudo dd if=/dev/DISKNAME of=/PATH/TO/IMAGE.dd conv=sync,noerror
```

Проверка файловой системы:

```
bash
fsck /dev/partition
```

Практические рекомендации.

Подготовка к восстановлению.

- **Оценка ситуации:**
  - Определение типа повреждения.
  - Оценка важности данных.
  - Выбор метода восстановления.
- **Необходимые инструменты:**
  - Внешний носитель для сохранения.
  - Специализированное ПО.
  - Загрузочный носитель.

Процесс восстановления.

1. Остановка использования поврежденного носителя.

2. Создание копии данных.

3. Выбор метода восстановления.

4. Запуск процесса восстановления.

5. Проверка восстановленных данных.

Типичные проблемы и решения.

Проблемы:

- Физическое повреждение носителя.
- Логическое повреждение файловой системы.
- Форматирование.
- Вирусная атака.

Решения:

- Использование специализированного ПО.
- Обращение в профессиональные сервисы.
- Создание резервных копий.
- Регулярное тестирование носителей.

Безопасность при восстановлении.

Меры предосторожности:

- Не устанавливать программы на восстанавливаемый диск.
- Использовать антивирусное ПО.
- Проверять целостность восстановленных данных.
- Документировать все действия.

Документация процесса.

Обязательные элементы:

- Описание проблемы.
- Используемые инструменты.
- Хронология действий.
- Результаты восстановления.
- Рекомендации по предотвращению.

Тестирование после восстановления.

Проверка:

- Целостность файлов.
- Соответствие размеров.

- Возможность открытия.
- Отсутствие ошибок.
- Полнота восстановления.

Задание1.6. Восстановление информационной системы.

Восстановление информационной системы

Общие принципы восстановления

Основные цели восстановления:

- Минимизация времени простоя
- Сохранение критически важных данных
- Восстановление работоспособности системы
- Обеспечение безопасности процесса

Этапы восстановления системы

1. **Предварительная оценка ситуации:**

- Определение причины сбоя
- Оценка масштаба повреждений
- Выбор стратегии восстановления
- Подготовка необходимых ресурсов

2. **Подготовка к восстановлению:**

- Создание резервных копий
- Проверка инструментов восстановления
- Настройка окружения
- Подготовка документации

3. **Процесс восстановления:**

- Запуск процедуры восстановления
- Мониторинг процесса
- Контроль промежуточных результатов
- Документирование действий

Восстановление в Windows

Инструменты и методы:

- **Системное восстановление:**

```
cmd
rstrui.exe
```

- **Восстановление из бэкапа:**

```
cmd
wbadmin start recovery
```

- **Использование DISM:**

```
cmd
DISM /Online /Cleanup-Image /RestoreHealth
```

Практические шаги:

- Проверка целостности системных файлов
- Восстановление загрузочных файлов
- Проверка состояния служб
- Тестирование работоспособности

Восстановление в Linux

Основные утилиты:

- **fsck** — проверка файловой системы

```
bash
sudo fsck /dev/sdXn
```

- **testdisk** — восстановление разделов

```
bash
sudo testdisk
```

- **photorec** — восстановление данных

```
bash
sudo photorec
```

Порядок действий:

- Проверка состояния файловой системы
- Восстановление загрузчика
- Монтирование разделов
- Восстановление данных

Практические рекомендации

Для Windows:

- Регулярное создание точек восстановления
- Использование надежных инструментов резервного копирования
- Проверка целостности системных файлов

- Создание загрузочных носителей

Для Linux:

- Настройка регулярных бэкапов
- Использование RAID-массивов
- Мониторинг состояния системы
- Документирование всех изменений

Тестирование после восстановления

Основные проверки:

- Проверка целостности данных
- Тестирование производительности
- Проверка безопасности
- Функциональное тестирование

Документация процесса

Обязательные элементы:

- План восстановления
- Инструкции по восстановлению
- Список используемых инструментов
- Журнал операций
- Результаты тестирования

Меры предосторожности

Безопасность:

- Проверка источников данных
- Использование антивирусного ПО
- Контроль доступа
- Шифрование данных

Резервирование:

- Создание копий перед восстановлением
- Хранение резервных копий в разных местах
- Регулярное тестирование бэкапов
- Проверка версий ПО

Типичные проблемы и их решения

Проблемы:

- Повреждение системных файлов
- Сбои в работе служб
- Потеря данных
- Нарушение целостности базы данных

Решения:

- Использование резервных копий
- Применение инструментов восстановления
- Обращение к специалистам
- Тестирование перед внедрением изменений

Автоматизация восстановления

Инструменты:

- Системы мониторинга
- Скрипты автоматизации
- Плагины для управления восстановлением
- Специализированное ПО

Рекомендации по автоматизации:

- Настройка уведомлений о сбоях
- Создание сценариев автоматического восстановления
- Регулярное тестирование автоматизированных процессов
- Документирование всех автоматизированных процедур

Задание1.7. Сбор информации об ошибках. Формирование отчетов об ошибках.

Основные принципы сбора информации

Ключевые компоненты:

- Систематизация ошибок
- Документирование проблем
- Анализ причин возникновения
- Отслеживание решений

Инструменты сбора информации

Windows

Системные инструменты:

- **Event Viewer** — журнал событий системы
- **Performance Monitor** — мониторинг производительности

- **Reliability Monitor** — отслеживание стабильности
- **Task Manager** — мониторинг процессов

Команды для сбора информации:

```
cmd
systeminfo
msinfo32
ver
wmic os get Caption,OSArchitecture,Version
```

Linux

Системные утилиты:

- **dmesg** — сообщения ядра
- **syslog** — системные журналы
- **top/htop** — мониторинг процессов
- **vmstat** — статистика виртуальной памяти

Команды мониторинга:

```
bash
uname -a
free -h
df -h
cat /var/log/syslog
```

Формирование отчетов об ошибках

Структура отчета:

- Идентификатор ошибки
- Дата и время возникновения
- Описание проблемы
- Шаги воспроизведения
- Ожидаемый результат
- Фактический результат
- Скриншоты/логи
- Версия ПО
- Конфигурация системы

Практические рекомендации

Windows

Сбор информации:

- Анализ журналов событий через Event Viewer
- Проверка отчетов Reliability Monitor
- Сбор дампов памяти
- Анализ отчетов об ошибках Windows

Инструменты:

- **Windows Error Reporting**
- **Microsoft Support Diagnostic Tool**
- **Process Monitor**
- **ProcDump**

Linux

Сбор данных:

- Анализ системных логов
- Сбор информации о процессах
- Мониторинг ресурсов
- Проверка состояния служб

Утилиты:

- **apport** — система отчетов об ошибках
- **abrt** — анализ сбоев приложений
- **crash** — анализ дампов ядра
- **sosreport** — создание отчетов о системе

Стандарты документирования

Обязательные элементы отчета:

- Заголовок и идентификатор
- Приоритет ошибки
- Среда воспроизведения
- Шаги для воспроизведения
- Вложения (логи, скриншоты)
- Статус исправления

Автоматизация сбора данных

Инструменты автоматизации:

- **Zabbix** — мониторинг и сбор данных
- **Nagios** — мониторинг состояния системы
- **ELK Stack** — сбор и анализ логов
- **Prometheus** — мониторинг метрик

Анализ собранных данных

Методы анализа:

- Корреляция событий
- Временной анализ
- Сравнительный анализ
- Статистический анализ

Формирование итоговых отчетов

Компоненты итогового отчета:

- Резюме проблемы
- Анализ причин
- Предложенные решения
- Результаты тестирования
- Рекомендации по предотвращению

Безопасность при работе с данными

Меры защиты:

- Шифрование конфиденциальной информации
- Контроль доступа к данным
- Регулярное обновление инструментов
- Проверка целостности данных

Примеры форматов отчетов

Windows:

```
xml
<ErrorReport>
    <ID>ERR-001</ID>
    <Date>2024-01-17</Date>
    <Description>Ошибка при запуске приложения</Description>
    <Steps>
        <Step>Запуск приложения</Step>
```

```
        <Step>Открытие файла</Step>
    </Steps>
</ErrorReport>
```

Linux:

```
json
{
    "error_id": "ERR-001",
    "timestamp": "2024-01-17T12:00:00Z",
    "description": "Ошибка при запуске сервиса",
    "logs": [
        {"level": "error", "message": "Service failed to start"},
        {"level": "warning", "message": "Resource limit reached"}
    ]
}
```

Рекомендации по улучшению процесса

Оптимизация:

- Создание шаблонов отчетов
- Автоматизация сбора данных
- Регулярный анализ статистики
- Обучение персонала
- Внедрение лучших практик

Задание1.8. Выполнение обслуживания информационной системы в соответствии с пользовательской документацией.

Выполнение обслуживания информационной системы в соответствии с пользовательской документацией требует строгого следования инструкциям производителя, учёта особенностей операционной системы и регулярного выполнения предусмотренных процедур. Это включает обновление ПО, управление учётными записями, настройку безопасности, резервное копирование данных и мониторинг состояния системы.

В Windows

1. Обновление системы и ПО

Регулярно проверяйте наличие обновлений через «Центр обновления Windows» (Параметры → Обновление и безопасность → Центр обновления Windows). Устанавливайте критические и рекомендуемые обновления для обеспечения безопасности и стабильности системы.

Для обновления до новой версии Windows (например, с Windows 10 до Windows 11) используйте официальный инструмент Media Creation Tool или другие рекомендованные методы. Перед обновлением проверьте совместимость системы с помощью утилиты PC Health Check.

Обновляйте драйверы устройств через диспетчер устройств или встроенные инструменты Windows. Если автоматическое обновление не работает, используйте сайты производителей оборудования.

2. Управление учётными записями и безопасность

Настройте сложные пароли для всех учётных записей. Включите политику блокировки учётной записи после нескольких неудачных попыток ввода пароля.

Используйте двухфакторную аутентификацию или биометрические данные (Windows Hello) для повышения безопасности входа.

Настройте брандмауэр и антивирус (например, Microsoft Defender) в соответствии с рекомендациями производителя. Включите защиту в режиме реального времени, облачную защиту и автоматическую отправку образцов подозрительных файлов.

Запретите вход по паролю для учётной записи администратора, если используется вход по PIN-коду или биометрии.

3. Резервное копирование данных

Регулярно создавайте резервные копии важных файлов на внешние носители, в облако или с помощью встроенных инструментов (например, «История файлов» в Windows 10/11).

Перед переустановкой системы или обновлением сохраните все данные с системного диска.

4. Мониторинг и устранение неполадок

Используйте встроенные средства диагностики (например, «Средство проверки системных файлов» — sfc /scannow в командной строке с правами администратора) для выявления и исправления повреждённых системных файлов.

Анализируйте журналы событий (Event Viewer) для выявления ошибок и предупреждений.

При возникновении проблем обращайтесь к официальной документации Microsoft или используйте средства устранения неполадок в «Параметрах».

5. Настройка параметров системы

Отключайте неиспользуемые службы и компоненты для уменьшения поверхности атаки.

Настройте параметры энергопотребления, дисплея и других параметров в соответствии с требованиями пользователя и рекомендациями производителя.

В Linux

1. Обновление системы и ПО

Используйте менеджер пакетов (APT для Debian/Ubuntu, YUM для CentOS/RHEL и т. д.) для проверки и установки обновлений. Команды для проверки обновлений: sudo apt update (для Ubuntu/Debian) или sudo yum check-update (для CentOS/RHEL).

Для дистрибутивов с долгосрочным поддержкой (LTS) следуйте рекомендациям производителя по частоте обновлений.

Рассмотрите использование инструментов автоматизации обновлений (например, Unattended Upgrades для Ubuntu/Debian, Yum Cron для CentOS/RHEL).

2. Управление учётными записями и безопасность

Запретите использование учётных записей с пустыми паролями. Настройте пароли для всех пользователей.

Ограничьте доступ к команде su и настройте права на использование sudo через файл /etc/sudoers.

Отключите вход суперпользователя по SSH (установите PermitRootLogin no в /etc/ssh/sshd_config).

Используйте SSH-ключи вместо паролей для удалённого доступа.

3. Резервное копирование данных

Регулярно создавайте резервные копии важных данных с помощью инструментов вроде rsync, tar или специализированных программ.

Храните копии в нескольких местах, включая локальные носители и облачные сервисы.

4. Мониторинг и аудит

Используйте инструменты вроде top, htop, vmstat для мониторинга процессов и ресурсов системы.

Анализируйте логи с помощью journalctl (для систем на базе systemd) или dmesg для сообщений ядра.

Проводите аудит прав доступа к файлам и SUID/SGID-приложениям.

5. Настройка параметров системы

Настройте права доступа к файлам и директориям в соответствии с принципом наименьших привилегий.

Используйте межсетевой экран (например, iptables или FirewallD) для контроля сетевого трафика.

Рассмотрите внедрение дополнительных мер безопасности, таких как Fail2Ban для блокировки подозрительных IP-адресов.

Общие рекомендации

Следуйте официальной документации. Всегда обращайтесь к руководству пользователя, документации дистрибутива или сайту производителя для получения актуальных инструкций.

Тестируйте изменения в изолированной среде. Перед применением настроек или обновлений на производственной системе проверяйте их в тестовой среде.

Регулярно проводите аудит безопасности. Оценивайте настройки системы на предмет уязвимостей и соответствия политике безопасности.

Используйте надёжные источники ПО. Устанавливайте программы только из официальных репозиториев или проверенных источников.

Сохраняйте логи изменений. Фиксируйте все значимые действия (обновления, изменения конфигурации и т. д.) для возможности отката или анализа проблем.

При возникновении сложностей или нестандартных ситуаций обращайтесь в поддержку производителя или к квалифицированным специалистам.

Задание1.9. Обслуживание локальной сети.

Обслуживание локальной сети включает регулярную проверку оборудования, настройку параметров, мониторинг состояния, устранение неполадок и обеспечение безопасности. Подходы могут различаться в зависимости от операционной системы.

В Windows

1. Проверка физического подключения и оборудования

Убедитесь, что все сетевые кабели правильно подключены и не повреждены.

Проверьте индикаторы маршрутизатора или коммутатора — они могут указать на проблему с подключением.

Регулярно осматривайте сетевое оборудование (роутеры, коммутаторы, точки доступа Wi-Fi) на предмет перегрева или других видимых повреждений.

2. Настройка и проверка IP-адресов

Убедитесь, что все устройства в сети имеют уникальные IP-адреса и находятся в одной подсети. При использовании DHCP проверьте настройки сервера DHCP, чтобы избежать конфликтов адресов.

При необходимости назначьте статические IP-адреса через параметры сетевого подключения («Параметры» → «Сеть и Интернет» → «Ethernet/Wi-Fi» → «Параметры IP»).

3. Настройка общего доступа и сетевого обнаружения

В «Центре управления сетями и общим доступом» (или в параметрах сети) включите сетевое обнаружение, общий доступ к файлам и принтерам.

Убедитесь, что все компьютеры в сети принадлежат к одной рабочей группе.

Настройте разрешения доступа к папкам и принтерам, используя вкладку «Доступ» в свойствах папки или принтера.

4. Проверка и настройка брандмауэра и безопасности

Убедитесь, что брандмауэр не блокирует необходимый сетевой трафик. В Windows можно настроить правила брандмауэра в «Панели управления» → «Система и безопасность» → «Брандмауэр Windows».

Проверьте настройки антивируса — иногда он может блокировать сетевой доступ.

5. Использование инструментов диагностики

Запускайте встроенный инструмент устранения неполадок сети через значок сети в области уведомлений на панели задач.

При необходимости выполните «Сброс сети» в Windows 10 — это удалит и переустановит сетевые адаптеры и компоненты.

Используйте команды в командной строке (например, ipconfig для проверки конфигурации сети, ping для проверки связности).

6. Обновление драйверов и ПО

Регулярно обновляйте драйверы сетевых адаптеров через «Диспетчер устройств».

Следите за обновлениями Windows и сетевого оборудования (роутеров, коммутаторов).

7. Мониторинг и аудит

Регулярно проверяйте журналы событий (Event Viewer) на предмет ошибок, связанных с сетью.

Используйте сторонние программы для мониторинга сети, если требуется расширенный контроль (например, PRTG Network Monitor, Zabbix).

В Linux

1. Проверка сетевого интерфейса и конфигурации

Используйте команду ip addr для просмотра списка интерфейсов и их IP-адресов.

Проверьте настройки сети через конфигурационные файлы (например, /etc/network/interfaces или настройки Netplan в современных дистрибутивах).

Для временного изменения настроек можно использовать команды ip, ifup, ifdown.

2. Диагностика связности

Используйте ping для проверки доступности устройств в сети.

Команда traceroute поможет отследить маршрут до целевого хоста.

arp -n позволяет проверить соответствие IP- и MAC-адресов в локальной сети.

3. Настройка маршрутизации

Проверьте таблицу маршрутизации с помощью ip route.

При необходимости добавьте или измените маршруты вручную.

4. Управление DNS

Настройте DNS-серверы в конфигурации сети (например, через Netplan).

Используйте nslookup или dig для проверки разрешения доменных имён.

5. Мониторинг и анализ трафика

Используйте ss для просмотра сетевых соединений и статистики.

Инструменты вроде Wireshark или tcpdump помогут анализировать сетевой трафик.

Для мониторинга нагрузки на сеть можно использовать nethogs, dstat или iptraf.

6. Обновление ПО и безопасности

Регулярно обновляйте систему и сетевые компоненты с помощью apt, yum или других менеджеров пакетов.

Настройте брандмауэр (например, ufw) для контроля входящего и исходящего трафика.

Ограничьте права доступа к конфигурационным файлам (например, chmod 600 /etc/network/interfaces).

7. Аудит и резервное копирование

Регулярно проверяйте конфигурацию сети на предмет ошибок и уязвимостей.

Создавайте резервные копии конфигурационных файлов (например, /etc/network/interfaces, Netplan-конфигураций).

Общие рекомендации

Документация и схемы сети. Ведите документацию по конфигурации сети, включая схемы подключения, IP-адреса устройств, настройки оборудования. Это упростит диагностику и обслуживание.

Резервирование оборудования. Рассмотрите использование резервных маршрутизаторов, коммутаторов или источников питания для повышения надёжности.

Обучение пользователей. Проводите обучение пользователей правилам работы в сети, чтобы минимизировать риски ошибок и несанкционированного доступа.

Планирование нагрузки. Следите за нагрузкой на сеть и при необходимости оптимизируйте её (например, распределяя трафик по разным каналам или обновляя оборудование).

Регулярное обслуживание и проактивный подход помогут поддерживать локальную сеть в работоспособном состоянии и минимизировать простои.

Задание1.10. Обслуживание системы видеонаблюдения.

Общие рекомендации по обслуживанию.

Основные задачи обслуживания:

- Мониторинг работоспособности системы.

- Проверка качества видеопотока.
- Контроль хранения архива.
- Обновление программного обеспечения.
- Техническое обслуживание оборудования.

Обслуживание в Windows.

Настройка операционной системы:

- Установка последних обновлений Windows.
- Настройка режима высокой производительности.
- Отключение автоматического обновления системы.
- Синхронизация системного времени.
- Отключение функций целостности памяти.

Регулярное обслуживание:

- Проверка свободного места на дисках.
- Мониторинг производительности системы.
- Контроль температуры оборудования.
- Проверка целостности архива.
- Тестирование резервного копирования.

Инструменты мониторинга:

- Встроенные средства Windows.
- Специализированное ПО системы видеонаблюдения.
- Системы мониторинга серверов.
- Журналы событий.

Обслуживание в Linux.

Настройка системы:

- Оптимизация параметров ядра Linux.
- Настройка планировщика задач.
- Конфигурация сетевых параметров.
- Настройка файловой системы.
- Настройка мониторинга.

Регулярные проверки:

- Проверка работоспособности сервисов.
- Мониторинг использования ресурсов.

- Контроль целостности данных.
- Проверка прав доступа.
- Тестирование производительности.

Техническое обслуживание оборудования.

Камеры и датчики:

- Проверка крепления.
- Очистка объективов.
- Проверка кабелей.
- Тестирование работы механизмов поворота.
- Проверка ИК-подсветки.

Серверное оборудование:

- Очистка от пыли.
- Проверка системы охлаждения.
- Контроль температуры.
- Проверка блоков питания.
- Тестирование RAID-массивов.

Программное обслуживание.

Обновление ПО:

- Проверка совместимости новых версий.
- Тестирование на тестовом стенде.
- Постепенное внедрение обновлений.
- Создание резервных копий перед обновлением.

Настройка параметров:

- Оптимизация качества видео.
- Настройка детекции движения.
- Настройка записи архива.
- Настройка уведомлений.
- Настройка прав доступа.

Резервное копирование.

Стратегия резервного копирования:

- Регулярное создание резервных копий конфигурации.
- Настройка автоматического резервного копирования.

- Хранение копий в разных местах.
- Проверка возможности восстановления.
- Документирование процесса.

Мониторинг и устранение неполадок.

Основные метрики мониторинга:

- Доступность камер.
- Качество видеопотока.
- Свободное место на дисках.
- Производительность системы.
- Ошибки в журналах.

Устранение типичных проблем:

- Проверка сетевых подключений.
- Тестирование питания.
- Проверка настроек видеопотоков.
- Анализ журналов ошибок.
- Тестирование резервного оборудования.

Безопасность системы.

Меры защиты:

- Регулярное обновление паролей.
- Настройка файрвола.
- Ограничение доступа к системе.
- Шифрование данных.
- Защита от несанкционированного доступа.

Документация и отчётность.

Ведение документации:

- Журнал обслуживания.
- Протоколы проверок.
- Отчёты о неисправностях.
- Инструкции по обслуживанию.
- Схемы системы.

Рекомендации по оптимизации.

Оптимизация производительности:

- Настройка битрейта видео.
- Оптимизация хранения архива.
- Балансировка нагрузки.
- Настройка приоритетов.
- Оптимизация сетевых настроек.

Регулярное выполнение всех перечисленных рекомендаций позволит обеспечить стабильную работу системы видеонаблюдения и минимизировать риски возникновения нештатных ситуаций.

Задание1.11. Обслуживание облачной информационной системы.

Общие принципы обслуживания.

Ключевые аспекты обслуживания:

- Мониторинг производительности
- Управление ресурсами.
- Обеспечение безопасности.
- Резервное копирование.
- Масштабирование системы.

Обслуживание в Windows.

Настройка операционной системы:

- Оптимизация параметров виртуализации.
- Настройка автоматического обновления.
- Конфигурация сетевых параметров.
- Настройка планировщика задач.

Регулярное обслуживание:

- Мониторинг использования ресурсов.
- Проверка целостности данных.
- Тестирование отказоустойчивости.
- Обновление компонентов.
- Проверка прав доступа.

Обслуживание в Linux

Базовая настройка:

- Оптимизация ядра системы.
- Настройка файрвола.

- Конфигурация системы хранения.
- Настройка мониторинга.
- Оптимизация сетевых параметров.

Регулярные проверки:

- Проверка работоспособности сервисов.
- Мониторинг нагрузки.
- Анализ логов.
- Тестирование резервного копирования.
- Проверка безопасности.

Мониторинг и управление

Основные метрики:

- Загрузка CPU.
- Использование памяти.
- Сетевой трафик.
- Время отклика сервисов.
- Доступность ресурсов.

Инструменты мониторинга:

- Системы мониторинга облачных платформ.
- Встроенные средства ОС.
- Специализированное ПО.
- Системы оповещения.

Безопасность системы.

Меры защиты:

- Регулярное обновление ПО.
- Настройка файрвола.
- Шифрование данных.
- Управление доступом.
- Резервное копирование.

Резервное копирование.

Стратегия резервного копирования:

- Регулярное создание резервных копий.
- Тестирование восстановления.

- Хранение копий в разных локациях.
- Автоматизация процессов.
- Документирование процедур.

Масштабирование и оптимизация.

Оптимизация производительности:

- Балансировка нагрузки.
- Оптимизация хранения.
- Настройка кэширования.
- Оптимизация запросов.
- Мониторинг узких мест.

Обслуживание приложений.

Регулярные задачи:

- Обновление версий ПО.
- Проверка зависимостей.
- Тестирование совместимости.
- Оптимизация настроек.
- Документирование изменений.

Документация и отчётность.

Ведение документации:

- Журнал обслуживания.
- Отчёты о производительности.
- Протоколы изменений.
- Инструкции по обслуживанию.
- Схемы архитектуры.

Устранение неполадок.

Порядок действий при сбоях:

- Определение причины сбоя.
- Оценка влияния на систему.
- Разработка плана восстановления.
- Реализация решения.
- Документирование инцидента.

Автоматизация процессов.

Автоматизируемые задачи:

- Резервное копирование.
- Мониторинг состояния.
- Обновление ПО.
- Масштабирование ресурсов.
- Тестирование системы.

Рекомендации по оптимизации.

Оптимизация затрат:

- Анализ использования ресурсов.
- Оптимизация хранения.
- Настройка автомасштабирования.
- Оптимизация сетевых настроек.
- Использование скидок и специальных предложений.

Регулярное выполнение всех перечисленных рекомендаций позволит обеспечить стабильную работу облачной информационной системы и минимизировать риски возникновения нештатных ситуаций. Важно помнить о необходимости постоянного мониторинга и адаптации системы к изменяющимся условиям эксплуатации.

ТЕМА 2. ДОКУМЕНТИРОВАНИЕ ПРОЦЕССОВ ВНЕДРЕНИЯ И СОПРОВОЖДЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ.

Актуальность документирования процессов.

В современных условиях развития информационных технологий **документирование процессов** внедрения и сопровождения информационных систем приобретает особую значимость. Это обусловлено следующими факторами:

- Растущей сложностью информационных систем.
- Необходимостью обеспечения непрерывности бизнес-процессов.
- Важностью сохранения знаний о системе.
- Потребностью в стандартизации процедур обслуживания.

Цели и задачи документирования.

Основная цель документирования процессов заключается в создании единой системы документации, обеспечивающей:

- Прозрачность всех этапов работы с информационной системой.
- Возможность передачи знаний между участниками проекта.
- Стандартизацию процессов внедрения и сопровождения.
- Контроль качества выполняемых работ.

Ключевые аспекты документирования.

Процесс документирования охватывает следующие основные направления:

- Подготовка технической документации.
- Создание пользовательских руководств.
- Формирование эксплуатационной документации.
- Документирование изменений и обновлений.
- Ведение журналов сопровождения.

Значение документации в жизненном цикле системы.

Документация является неотъемлемой частью жизненного цикла информационной системы и обеспечивает:

- Эффективное внедрение системы.
- Качественное сопровождение.
- Своевременное устранение неполадок.
- Оптимизацию процессов обслуживания.
- Повышение эффективности использования системы.

Принципы эффективного документирования.

Основные принципы построения системы документации включают:

- Актуальность информации.
- Полнота описания процессов.
- Доступность для целевой аудитории.
- Структурированность материалов.
- Удобство использования.

Структура документации.

Система документации должна включать следующие компоненты:

- Проектная документация.
- Техническая документация.
- Пользовательская документация.
- Эксплуатационная документация.

- Документация по сопровождению.

Роль документации в управлении изменениями.

Управление изменениями невозможно без качественной системы документирования, которая позволяет:

- Отслеживать все изменения в системе.
- Оценивать их влияние на работу системы.
- Контролировать процесс внедрения изменений.
- Обеспечивать обратную совместимость.

В современных условиях грамотное документирование процессов внедрения и сопровождения информационных систем становится ключевым фактором успешного функционирования любой организации, использующей информационные технологии в своей деятельности. Правильно выстроенная система документации позволяет минимизировать риски, оптимизировать процессы и обеспечить эффективное использование информационных ресурсов.

Задание2.1. Разработка сценария внедрения информационной системы для рабочего места.

Общие положения

Сценарий внедрения — это последовательность действий, направленных на успешное развертывание информационной системы на рабочем месте пользователя.

Предварительная подготовка.

Необходимые условия:

- Наличие технической документации.
- Подготовленное рабочее место.
- Доступ к сетевым ресурсам.
- Резервное копирование данных.

Этапы внедрения для Windows.

1. **Подготовка системы:**

- Обновление Windows до актуальной версии.
- Проверка системных требований.
- Настройка параметров безопасности.
- Создание резервной точки восстановления.

2. **Установка компонентов:**

- Установка необходимого ПО.
- Настройка системных служб.
- Конфигурация сетевых параметров.
- Установка драйверов устройств.

3. **Развертывание ИС:**

- Установка основного программного обеспечения.
- Настройка параметров подключения.
- Конфигурация пользовательского интерфейса.
- Интеграция с существующими системами.

4. **Тестирование:**

- Проверка работоспособности.
- Тестирование основных функций.
- Проверка безопасности.
- Оценка производительности.

Этапы внедрения для Linux.

1. **Подготовка системы:**

- Обновление пакетов системы.
- Проверка зависимостей.
- Настройка репозиториев.
- Создание резервных копий.

2. **Установка компонентов:**

- Установка базового ПО.
- Настройка системных служб.
- Конфигурация сети.
- Установка необходимых библиотек.

3. **Развертывание ИС:**

- Установка основного ПО.
- Настройка конфигурационных файлов.
- Конфигурация прав доступа.
- Интеграция с инфраструктурой.

4. **Тестирование:**

- Проверка работоспособности.

- Тестирование функционала.
- Проверка безопасности.
- Оценка производительности.

Практические рекомендации

Для Windows:

- Использовать групповые политики для стандартизации настроек.
- Применять инструменты удаленного развертывания.
- Настраивать автоматическое обновление.
- Документировать все изменения.

Для Linux:

- Использовать системы управления пакетами.
- Настраивать автоматическую установку обновлений.
- Применять конфигурационные менеджеры.
- Документировать все изменения в системе.

Контроль качества внедрения.

Основные метрики:

- Время отклика системы.
- Стабильность работы.
- Безопасность данных.
- Удобство использования.

Документация процесса.

Обязательные документы:

- План внедрения.
- Инструкция по установке.
- Руководство пользователя.
- Журнал изменений.
- Отчет о тестировании.

Устранение типичных проблем.

Основные проблемы и решения:

- Конфликты ПО — проверка совместимости.
- Проблемы с сетью — настройка сетевых параметров.
- Ошибки установки — проверка системных требований.

- Проблемы безопасности — настройка прав доступа.

Обучение пользователей.

Этапы обучения:

- Знакомство с интерфейсом.
- Обучение базовым функциям.
- Обучение продвинутым возможностям.
- Решение типовых задач.

Мониторинг после внедрения.

Ключевые показатели:

- Производительность системы.
- Частота обращений в поддержку.
- Удовлетворенность пользователей.
- Частота возникновения ошибок.

Рекомендации по оптимизации.

Оптимизация процесса:

- Автоматизация рутинных задач.
- Стандартизация настроек.
- Документирование лучших практик.
- Регулярный анализ эффективности.

Успешное внедрение информационной системы требует тщательного планирования, профессионального подхода и внимательного отношения к деталям на каждом этапе процесса.

Задание2.2. Разработка технического задания на внедрение информационной системы.

Общие положения.

Техническое задание (ТЗ) — это основополагающий документ, определяющий требования, условия и порядок внедрения информационной системы.

Структура технического задания.

Основные разделы ТЗ:

- Общие сведения.
- Назначение и цели создания системы.

- Характеристики объекта автоматизации.
- Требования к системе.
- Состав и содержание работ.
- Порядок контроля и приемки.
- Требования к документированию.
- Источники разработки.

Особенности разработки ТЗ для Windows.

Специфические требования:

- Совместимость с Windows-инфраструктурой.
- Интеграция с Active Directory.
- Требования к клиентским рабочим местам.
- Поддержка групповых политик.
- Требования к антивирусной защите.

Особенности разработки ТЗ для Linux.

Специфические требования:

- Поддержка дистрибутивов Linux.
- Требования к пакетной базе.
- Настройка прав доступа.
- Интеграция с системами управления.
- Требования к безопасности.

Ключевые компоненты ТЗ.

Функциональные требования:

- Описание основных функций системы.
- Интерфейс пользователя.
- Интеграция с другими системами.
- Требования к производительности.
- Обработка данных.

Нефункциональные требования:

- Надежность.
- Безопасность.
- Масштабируемость.
- Удобство сопровождения.

- Совместимость.

Требования к аппаратному обеспечению.

Для Windows:

- Конфигурация серверов.
- Требования к рабочим станциям.
- Сетевое оборудование.
- Системы хранения данных.

Для Linux:

- Спецификации серверов.
- Требования к виртуализации.
- Сетевая инфраструктура.
- Резервное копирование.

Требования к программному обеспечению.

Компоненты системы:

- Операционные системы.
- Серверное ПО.
- Клиентские приложения.
- Средства мониторинга.
- Инструменты администрирования.

Порядок разработки ТЗ.

Этапы создания:

1. Анализ требований заказчика.
2. Формирование предварительного варианта.
3. Согласование с заинтересованными сторонами.
4. Внесение корректировок.
5. Утверждение окончательного варианта.

Контроль качества ТЗ.

Критерии оценки:

- Полнота описания требований.
- Четкость формулировок.
- Реализуемость требований.
- Соответствие стандартам.

- Актуальность информации.

Документационное обеспечение.

Необходимые документы:

- Схема архитектуры системы.
- Диаграммы процессов.
- Спецификации интерфейсов.
- План внедрения.
- График выполнения работ.

Рекомендации по внедрению.

Практические советы:

- Учитывать особенности целевой платформы.
- Предусмотреть масштабируемость системы.
- Обеспечить отказоустойчивость.
- Заложить механизмы мониторинга.
- Продумать процедуры обслуживания.

Тестирование и приемка.

Этапы проверки:

- Предварительные испытания.
- Опытная эксплуатация.
- Приемочные испытания.
- Документирование результатов.
- Оформление акта приемки.

Качественно разработанное техническое задание является фундаментом успешного внедрения информационной системы и обеспечивает:

- Четкое понимание целей проекта.
- Единое видение результатов всеми участниками.
- Эффективное управление процессом внедрения.
- Контроль качества выполнения работ.
- Своевременное достижение поставленных целей.

Задание2.3. Разработка графика разработки и внедрения информационной системы.

Общие положения.

График разработки — это документ, определяющий последовательность, сроки и взаимосвязь работ по созданию и внедрению информационной системы.

Этапы разработки графика.

1. **Подготовительный этап:**

- Анализ требований к системе.
- Оценка ресурсов.
- Определение рисков.
- Формирование команды проекта.

2. **Планирование работ:**

- Разбивка проекта на этапы.
- Определение зависимостей между задачами.
- Расчет необходимых ресурсов.
- Оценка сроков выполнения.

Структура графика внедрения.

Основные компоненты:

- Календарный план работ.
- Ресурсный план.
- Матрица рисков.
- План коммуникаций.
- План контроля качества.

Особенности для Windows-систем.

Специфические этапы:

- Интеграция с Active Directory.
- Настройка групповых политик.
- Внедрение антивирусной защиты.
- Конфигурация файрвола.
- Настройка резервного копирования.

Особенности для Linux-систем.

Специфические этапы:

- Настройка репозиториев.
- Конфигурация пакетного менеджера.
- Настройка прав доступа.

- Внедрение системы мониторинга.
- Настройка автоматизации.

Практические рекомендации по составлению графика.

Ключевые моменты:

- Учет технических особенностей платформы.
- Предусмотрение времени на тестирование.
- Заложение резервов на устранение непредвиденных проблем.
- Учет сезонности и загруженности персонала.
- Планирование обучения пользователей.

Компоненты графика внедрения.

Обязательные элементы:

- **Фаза проектирования:**
  - Анализ требований.
  - Разработка архитектуры.
  - Создание прототипов.
- **Фаза разработки:**
  - Программирование.
  - Тестирование модулей.
  - Интеграция компонентов.
- **Фаза внедрения:**
  - Установка ПО.
  - Настройка окружения.
  - Миграция данных.
- **Фаза обучения:**
  - Подготовка документации.
  - Проведение тренингов.
  - Консультации пользователей.

Методы визуализации графика.

Рекомендуемые инструменты:

- Диаграмма Ганта.
- Сетевой график.
- Календарь проекта.

- Дорожная карта.
- Матрица ответственности.

Контроль выполнения графика.

Механизмы контроля:

- Регулярные статус-встречи.
- Отчеты о выполнении работ.
- Мониторинг критических задач.
- Управление рисками.
- Корректировка плана.

Документационное обеспечение.

Необходимые документы:

- План-график проекта.
- Технико-экономическое обоснование.
- Протоколы согласования.
- Акты выполненных работ.
- Отчетность по этапам.

Оптимизация графика.

Способы улучшения:

- Автоматизация рутинных операций.
- Параллельное выполнение независимых задач.
- Оптимизация коммуникаций.
- Использование типовых решений.
- Применение современных методологий управления проектами.

Типичные проблемы и их решения.

Основные риски:

- Срыв сроков — создание буферов времени.
- Нехватка ресурсов — планирование заранее.
- Технические проблемы — тестирование на ранних этапах.
- Сопротивление пользователей — активное вовлечение в процесс.

Рекомендации по адаптации графика.

Важные аспекты:

- Учет специфики организации.

- Гибкость планирования.
- Возможность масштабирования.
- Учет отраслевых особенностей.
- Соответствие стандартам.

Грамотно составленный график разработки и внедрения информационной системы позволяет:

- Эффективно управлять проектом.
- Контролировать сроки выполнения работ.
- Оптимизировать использование ресурсов.
- Своевременно реагировать на изменения.
- Обеспечить качественное внедрение системы.

Задание2.4. Разработка перечня обучающей документации на информационную систему.

Общие положения.

Обучающая документация — это комплекс материалов, обеспечивающих эффективное освоение и использование информационной системы пользователями.

Структура обучающей документации

Основные компоненты:

- Руководство пользователя.
- Руководство администратора.
- Инструкция по установке.
- FAQ (часто задаваемые вопросы).
- Справочная система.
- Обучающие материалы.

Специфика разработки для Windows.

Обязательные разделы:

- Работа с интерфейсом Windows.
- Интеграция с Active Directory.
- Настройка групповых политик.
- Работа с файловой системой.
- Использование стандартных инструментов Windows.

Специфика разработки для Linux.

Ключевые разделы:

- Основы работы с командной строкой.
- Управление пакетами.
- Настройка прав доступа.
- Работа с файловыми системами.
- Конфигурация сетевых служб.

Основные типы обучающих материалов.

Типология документации:

- **Руководства пользователя:**
  - Пошаговые инструкции.
  - Описание функционала.
  - Примеры использования.
- **Обучающие курсы:**
  - Видеоуроки.
  - Интерактивные тренинги.
  - Практические задания.
- **Справочные материалы:**
  - Глоссарий терминов.
  - Схемы и диаграммы.
  - Чек-листы.

Требования к содержанию документации.

Базовые принципы:

- Понятность изложения.
- Структурированность информации.
- Актуальность данных.
- Полнота охвата.
- Практическая применимость.

Методы представления информации.

Форматы материалов:

- Текстовые документы.
- Видеоматериалы.

- Интерактивные руководства.
- Инфографика.
- Схемы и диаграммы.

Процесс разработки документации.

Этапы создания:

1. Анализ целевой аудитории.
2. Определение структуры документации.
3. Подготовка контента.
4. Тестирование материалов.
5. Корректировка и утверждение.

Рекомендации по оформлению.

Основные правила:

- Единый стиль оформления.
- Использование наглядных материалов.
- Четкая структура разделов.
- Наличие системы навигации.
- Актуальность примеров.

Организация обучения пользователей.

Формы обучения:

- Офлайн-тренинги.
- Онлайн-курсы.
- Вебинары.
- Самостоятельное обучение.
- Практические семинары.

Контроль эффективности обучения.

Методы оценки:

- Тестирование знаний.
- Практические задания.
- Обратная связь от пользователей.
- Анализ обращений в поддержку.
- Мониторинг использования системы.

Поддержка актуальности документации.

Механизмы обновления:

- Регулярный аудит материалов.
- Внесение изменений при обновлении системы.
- Актуализация примеров.
- Добавление новых разделов.
- Удаление устаревшей информации.

Особые рекомендации.

Важные аспекты:

- Учет уровня подготовки пользователей.
- Использование понятной терминологии.
- Наличие примеров из практики.
- Пошаговые инструкции.
- Возможность быстрого поиска информации.

Грамотно разработанная обучающая документация обеспечивает:

- Быстрое освоение системы пользователями.
- Снижение количества ошибок при работе.
- Повышение эффективности использования системы.
- Сокращение затрат на техническую поддержку.
- Улучшение пользовательского опыта.

Задание2.5. Разработка технического задания на сопровождение информационной системы.

Общие положения.

Техническое задание на сопровождение — это документ, определяющий требования, условия и порядок технического обслуживания информационной системы.

Структура ТЗ на сопровождение

Основные разделы:

- Общие сведения о системе.
- Цели и задачи сопровождения.
- Требования к сопровождению.
- Состав работ по сопровождению.
- Порядок контроля и приемки.

- Требования к документации.

Особенности сопровождения для Windows.

Специфические требования:

- Интеграция с Active Directory.
- Управление групповыми политиками.
- Мониторинг системных событий.
- Контроль обновлений Windows.
- Обеспечение совместимости с Windows-приложениями.

Особенности сопровождения для Linux.

Специфические требования:

- Управление пакетами и зависимостями.
- Настройка системных сервисов.
- Мониторинг системных журналов.
- Управление правами доступа.
- Обеспечение безопасности Linux-систем.

Компоненты сопровождения.

Обязательные работы:

- Техническая поддержка пользователей.
- Обновление программного обеспечения.
- Резервное копирование.
- Мониторинг работоспособности.
- Устранение ошибок.

Требования к сопровождению.

Функциональные требования:

- Оперативность реагирования на инциденты.
- Документирование всех изменений.
- Ведение журнала сопровождения.
- Регулярное тестирование системы.
- Подготовка отчетов.

Организация процесса сопровождения.

Ключевые элементы:

- План сопровождения.

- График работ.
- Распределение обязанностей.
- Система отчетности.
- Порядок взаимодействия.

Контроль качества сопровождения.

Критерии оценки:

- Время реакции на инциденты.
- Процент успешно решенных проблем.
- Количество критических ошибок.
- Удовлетворенность пользователей.
- Соответствие SLA.

Документационное обеспечение.

Необходимые документы:

- Регламенты сопровождения.
- Инструкции по устранению типовых проблем.
- Журналы сопровождения.
- Отчеты о проделанной работе.
- Акты выполненных работ.

Практические рекомендации.

Для Windows-систем:

- Использовать централизованное управление через Active Directory.
- Внедрить систему мониторинга событий безопасности.
- Регулярно проводить аудит безопасности.
- Автоматизировать процессы обновления.

Для Linux-систем:

- Настроить систему мониторинга системных журналов.
- Внедрить автоматизированное резервное копирование.
- Регулярно обновлять пакеты безопасности.
- Использовать системы контроля версий.

Порядок разработки ТЗ.

Этапы создания:

1. Анализ текущей системы.

2. Определение требований к сопровождению.
3. Разработка плана работ.
4. Согласование с заказчиком.
5. Утверждение документа.

Особые требования к сопровождению.

Важные аспекты:

- Обеспечение непрерывности работы.
- Защита данных.
- Соблюдение требований безопасности.
- Оптимизация производительности.
- Масштабируемость решений.

Оценка эффективности сопровождения.

Показатели эффективности:

- Время восстановления после сбоев.
- Количество предотвращенных инцидентов.
- Удовлетворенность пользователей.
- Экономическая эффективность.
- Качество технической поддержки.

Качественно разработанное ТЗ на сопровождение обеспечивает:

- Четкое понимание задач сопровождения.
- Единые стандарты обслуживания.
- Эффективное использование ресурсов.
- Своевременное устранение проблем.
- Повышение надежности системы.

Задание2.6. Формирование предложений о расширении информационной системы.

Общие положения.

Расширение ИС — это процесс модернизации и дополнения существующей информационной системы новыми функциями и возможностями для повышения эффективности работы.

Этапы формирования предложений.

1. **Анализ текущего состояния.**

- Оценка производительности системы.
- Выявление узких мест.
- Анализ пользовательских запросов.
- Изучение статистики использования.

2. **Определение потребностей.**

- Сбор требований от пользователей.
- Анализ бизнес-процессов.
- Выявление проблемных областей.
- Формулировка целей расширения.

Специфика предложений для Windows.

Ключевые направления расширения:

- Интеграция с Active Directory.
- Внедрение групповых политик.
- Расширение возможностей резервного копирования.
- Улучшение системы безопасности.
- Оптимизация работы с периферийным оборудованием.

Специфика предложений для Linux.

Основные направления развития:

- Настройка систем мониторинга.
- Автоматизация процессов.
- Улучшение системы прав доступа.
- Оптимизация производительности.
- Расширение возможностей виртуализации.

Структура предложений по расширению.

Обязательные компоненты:

- Описание текущей ситуации.
- Обоснование необходимости изменений.
- Перечень предлагаемых решений.
- Оценка ресурсов.
- План реализации.
- Ожидаемые результаты.

Практические рекомендации.

При формировании предложений:

- Учитывать совместимость с существующей инфраструктурой.
- Оценивать влияние на производительность.
- Просчитывать затраты на внедрение.
- Анализировать риски.
- Предусматривать тестирование.

Методология оценки предложений.

Критерии оценки:

- Соответствие бизнес-целям.
- Экономическая эффективность.
- Техническая реализуемость.
- Влияние на пользователей.
- Сроки внедрения.

Документация предложений.

Обязательные разделы:

- Техническое описание.
- План внедрения.
- Оценка ресурсов.
- График реализации.
- План тестирования.
- Инструкция по эксплуатации.

Реализация предложений.

Этапы внедрения:

- Подготовка инфраструктуры.
- Тестирование в пилотной зоне.
- Масштабирование решения.
- Обучение пользователей.
- Мониторинг результатов.

Контроль качества расширения.

Методы контроля:

- Тестирование функциональности.
- Мониторинг производительности.

- Анализ пользовательского опыта.
- Оценка безопасности.
- Проверка соответствия требованиям.

Рекомендации по сопровождению.

Важные аспекты:

- Документирование изменений.
- Обучение персонала.
- Обновление документации.
- Мониторинг эффективности.
- Сбор обратной связи.

Экономическое обоснование.

Ключевые показатели:

- Стоимость внедрения.
- Сроки окупаемости.
- Экономия ресурсов.
- Повышение эффективности.
- Рост производительности.

Типичные ошибки при расширении.

Основные риски:

- Недостаточное тестирование.
- Игнорирование обратной связи.
- Отсутствие плана отката.
- Недооценка ресурсов.
- Пренебрежение документацией.

Качественно сформированные предложения по расширению ИС должны обеспечивать:

- Повышение эффективности работы системы.
- Улучшение пользовательского опыта.
- Рост производительности.
- Снижение затрат на обслуживание.
- Соответствие современным требованиям безопасности.

Задание2.7. Разработка руководства оператора.

Общие положения.

Руководство оператора — это документ, предназначенный для пользователей информационной системы, содержащий инструкции по работе с системой и описание всех необходимых процедур.

Структура руководства.

Основные разделы:

- Общие сведения о системе.
- Подготовка к работе.
- Описание интерфейса.
- Основные операции.
- Устранение типичных неисправностей.
- Приложения.

Особенности разработки для Windows.

Специфические разделы:

- Работа с Проводником Windows.
- Использование меню “Пуск”.
- Настройка параметров системы.
- Работа с учетными записями.
- Интеграция с Active Directory.

Особенности разработки для Linux.

Ключевые разделы:

- Основы работы с терминалом.
- Управление файлами и папками.
- Настройка прав доступа.
- Работа с пакетным менеджером.
- Конфигурация окружения.

Рекомендации по структуре.

Обязательные компоненты:

- **Введение:**
  - Назначение руководства.
  - Область применения.
  - Термины и определения.

- **Основная часть:**
  - Подготовка к работе.
  - Описание интерфейса.
  - Порядок выполнения операций.
  - Обработка ошибок.
  - Техническое обслуживание.
- **Приложения:**
  - Справочные материалы.
  - Глоссарий.
  - Схемы и диаграммы.

Требования к содержанию.

Основные принципы:

- Понятность изложения.
- Структурированность информации.
- Актуальность данных.
- Полнота описания.
- Практическая применимость.

Оформление документации.

Правила оформления:

- Единый стиль.
- Использование иллюстраций.
- Четкая структура.
- Нумерация разделов
- Система ссылок

Практические рекомендации.

Для Windows-систем:

- Использовать стандартные элементы Windows.
- Описывать работу с Проводником.
- Учитывать интеграцию с Office.
- Описывать работу с сетевыми ресурсами.

Для Linux-систем:

- Включать команды терминала.

- Описывать работу с файловой системой.
- Учитывать различные дистрибутивы.
- Описывать настройку окружения.

Методы представления информации.

Форматы материалов:

- Текстовые инструкции.
- Скриншоты интерфейса.
- Видеоуроки.
- Интерактивные руководства.
- Схемы процессов.

Контроль качества.

Методы проверки:

- Тестирование на целевой аудитории.
- Проверка актуальности.
- Оценка понятности.
- Анализ полноты.
- Проверка соответствия стандартам.

Обновление документации.

Механизмы актуализации:

- Регулярный аудит.
- Внесение изменений.
- Обновление примеров.
- Добавление новых разделов.
- Удаление устаревшей информации.

Обучение пользователей.

Формы обучения:

- Офлайн-тренинги.
- Онлайн-курсы.
- Вебинары.
- Самостоятельное обучение.
- Практические семинары.

Оценка эффективности.

Критерии оценки:

- Время освоения материала.
- Количество обращений в поддержку.
- Успешность выполнения задач.
- Удовлетворенность пользователей.
- Частота использования документации.

Качественно разработанное руководство оператора должно обеспечивать:

- Быстрое освоение системы.
- Эффективное выполнение задач.
- Снижение количества ошибок.
- Повышение производительности труда.
- Уменьшение нагрузки на техническую поддержку.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Перлова О. Н. Соадминистрирование баз данных и серверов: учебное издание / Перлова О. Н., Ляпина О. П. - Москва : Академия, 2023. - 304 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный.

2. Федорова, Г. Н. Разработка, внедрение и адаптация программного обеспечения отраслевой направленности : Учебное пособие / Г. Н. Федорова. – Москва : КУРС : ИНФРА-М, 2022. – 336 с. (Среднее профессиональное образование). – ISBN 9785906818416. – Текст : непосредственный.

Дополнительная литература

1. Компьютерные сети : учебник для среднего профессионального образования по специальностям 09.02.06 "Сетевое и системное администрирование", 09.02.07 "Информационные системы и программирование" / В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин ; В. В. Баринов [и др.]. – 4-е изд., испр. и доп.. - Москва : Академия, 2021. – 192 с. – ISBN 9785446899258. – URL: https://academia-moscow.ru/catalogue/4831/551458/. – Текст : электронный.

2. Гохберг Г.С. Информационные технологии: ЭУМК: учебное издание / Гохберг Г.С., Зафиевский А.В., Короткин А.А. - Москва : Академия, 2024. - 0 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный.

3. Казанский, А. А. Программирование на C# : учебное пособие для среднего профессионального образования / А. А. Казанский. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 181 с. — (Профессиональное образование). — ISBN 978-5-534-21380-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569863.

4. Семакин И.Г. Основы алгоритмизации и программирования: ЭУМК: учебное издание / Семакин И.Г., Шестаков А. П. - Москва : Академия, 2025. - 0 с. (Специальности среднего профессионального образования). - URL: https://academia-

moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный

5. Куприянов, Д. В. Информационное обеспечение профессиональной деятельности : учебник и практикум для среднего профессионального образования / Д. В. Куприянов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 236 с. — (Профессиональное образование). — ISBN 978-5-534-20826-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/558828.

6. Грекул, В. И. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 404 с. — (Профессиональное образование). — ISBN 978-5-534-19506-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566739.

7. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 273 с. — (Профессиональное образование). — ISBN 978-5-534-20362-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562355.

Приложение А. Бланк титульного листа

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение \

высшего образования

«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ ИМЕНИ Т.Ф.ГОРБАЧЕВА»

Филиал КузГТУ в г.Белово

ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

ПМ.06 «Сопровождение информационных систем»

Выполнил:

Студент группы _____

/_____/_____

подпись

Руководитель:

/_____/_____

подпись

Оценка_____

«___»_____20___ г.

Белово

20__г.

ПРИЛОЖЕНИЕ Б. Бланк задания по ПП

ЗАДАНИЕ

на производственную практику

по профессионального модуля **ПМ.06 «Сопровождение информационных систем»**

студент _____

группы_____

специальности «09.02.07 Информационные системы и программирование»

Дата начала практики «___» _____ 20___г.

Дата окончания практики «___» _____ 20__г.

Дата сдачи практики «___» _____ 20__г.

Виды работ, обязательных для выполнения:

1. _____
2. _____
3. _____
4. _____

Задание выдал руководитель производственной практики от

филиала КузГТУ в г.Белово /_____/_____

подпись

ПРИЛОЖЕНИЕ В. Дневник по ПП

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф.ГОРБАЧЕВА»

Филиал КузГТУ в г.Белово

ДНЕВНИК ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

профессионального модуля ПМ.06 «Сопровождение информационных систем»

студент _____

группы_____

специальности «09.02.07 Информационные системы и программирование»

Период практики с «___» _____ 20__г. по «___» _____ 20__.

База практики_____

М.П.

Руководитель практики от

ОРГАНИЗАЦИИ /_____/_____

подпись

Закончил практику «___» _____ 20__.

Дата	Содержание работы	Оценка	Подпись

ПРИЛОЖЕНИЕ Г. Бланк аттестационного листа по ПП

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение \

высшего образования

«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ ИМЕНИ Т.Ф.ГОРБАЧЕВА»

Филиал КузГТУ в г.Белово

АТТЕСТАЦИОННЫЙ ЛИСТ

по производственной практике

по профессиональному модулю _____

(индекс и наименование профессионального модуля)

Обучающийся	
Институт/факультет	
Специальность	
(код специальности)	
Курс	Группа
Вид практики	
Способ прохождения практики	
Период прохождения практики с	по
Профильная организация	

(наименование, местонахождение)

Во время прохождения практики обучающимся были освоены следующие профессиональные и общие компетенции

Наименование компетенции	Оценка	
	Освоена	Не освоена

Руководитель учебной практики от

филиала КузГТУ в г.Белово

/_____/_____

подпись

ПРИЛОЖЕНИЕ Д. Бланк характеристики на обучающегося в период прохождения ПП

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение \ высшего образования

«КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф.ГОРБАЧЕВА»

Филиал КузГТУ в г.Белово

ХАРАКТЕРИСТИКА

на обучающегося по освоению общих и профессиональных компетенций в период прохождения производственной практики

по профессиональному модулю_____

(индекс и наименование профессионального модуля)

Обучающийся

Институт/факультет

Специальность

(код специальности)

Курс	Группа
Вид практики	
Способ прохождения практики	
Период прохождения практики с	по
Профильная организация	

(наименование, местонахождение)

Виды и качество выполненных работ:

Виды работ	Критерии выполнения работ		
	Выполнены полностью самостоятельно	Выполнены с незначительной помощью	Выполнены с помощью наставника

Руководитель учебной практики от филиала КузГТУ в г.Белово

/_____/_____

подпись

Составитель
Витвицкий Максим Николаевич

Методические указания по производственной практике УП.06.01
для студентов очной формы обучения
по направлению специальности
09.02.07 «Информационные системы и программирование»

Публикуется в авторской редакции