



Программа учебной практики по специальности разработана на основании федерального государственного образовательного стандарта (далее ФГОС) для специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 (Зарегистрировано в Минюсте России 26 декабря 2016 г. N 44938)

Организация-разработчик:

Частное профессиональное образовательное учреждение Тюменского областного союза потребительских обществ «Тюменский колледж экономики, управления и права» (ЧПОУ ТОСПО «ТюмКЭУП»)

## **СОДЕРЖАНИЕ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	33
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	30
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	69
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	70

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 1.1. Область применения программы

Программа учебной практики по специальности (далее - программа) - является частью основной образовательной программы в соответствии с ФГОС в части освоения видов деятельности (далее - ВД):

ВД.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ВД.2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ВД.3 Защита информации техническими средствами

ВД.4 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных

## 1.2. Цель, задачи и планируемые результаты освоения учебной практики

Учебная практика направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках профессиональных модулей по видам деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Задачами учебной практики являются:

- закрепление и совершенствование приобретенного в процессе обучения опыта практической деятельности обучающихся;
- развитие общих и профессиональных компетенций;
- ознакомление со спецификой профессиональной деятельности по избранной специальности в условиях конкретных учреждений, организаций, предприятий различных организационно-правовых форм;
- формирование у обучающегося правильного представления об общественных процессах;
- выработка умений правильно определять, толковать и применять нормы права в научных и практических целях;
- закрепление полученных теоретических знаний и формирование практических навыков в избранной сфере деятельности.

### Планируемые результаты:

#### 1) профессиональные компетенции:

Вид деятельности	Код и наименование компетенции	Требования к умениям и практическому опыту
ВД.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Практический опыт (навыки): установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем, администрирование автоматизированных систем в защищенном исполнении, эксплуатация компонентов систем защиты информации автоматизированных систем, диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	
	ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Умения: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
	ПК 1.2 Администрировать программные и программно-аппаратные компоненты	Умения: организовывать, конфигурировать, производить монтаж, осуществлять

	автоматизированной (информационной) системы в защищен-ном исполнении.	диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы.
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищен-ном исполнении в соответствии с требованиями эксплуатационной документации.	Умения: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.
	ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Умения: использовать методы для получения кода с заданной функциональностью и степенью качества.
ВД.2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Практический опыт: установка, настройка программных средств защиты информации в автоматизированной системе, обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами, тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации, решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации, применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных, учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, работа с подсистемами регистрации событий, выявление событий и инцидентов безопасности в автоматизированной системе	
	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.
	ПК.2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умения: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.
	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Умения: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.
	ПК.2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Умения: применять программные и программно-аппаратные средства для защиты информации в базах данных проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации применять математический аппарат для выполнения криптографических преобразований использовать типовые программные криптографические средства, в том числе электронную подпись.
	ПК.2.5. Уничтожать информацию и носители информации с использованием	Умения: применять средства гарантированного

	программных и программно-аппаратных средств	уничтожения информации.
	ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ВД.3 Защита информации техническими средствами	<p>Практический опыт:</p> <p>установка, монтаж и настройка технических средств защиты информации</p> <p>техническое обслуживание технических средств защиты информации</p> <p>применение основных типов технических средств защиты информации, применение основных типов технических средств защиты информации, выявление технических каналов утечки информации, участие в мониторинге эффективности технических средств защиты информации, диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации, проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации, проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации, выявление технических каналов утечки информации, установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты</p>	
	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	ПК.3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Умения: применять технические средства для криптографической защиты информации конфиденциального характера, применять технические средства для уничтожения информации и носителей информации, применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами
	ПК.3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	ПК.3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Умения: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом применять инженерно-технические средства физической защиты объектов информатизации
ВД.4 Выполнение работ по профессии Оператор электронно-вычислительных и вычислительных машин	<p>Практический опыт:</p> <p>эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;</p> <p>администрировании автоматизированных систем в защищенном исполнении;</p> <p>установке компонентов систем защиты информации автоматизированных информационных систем.</p>	
	ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в	Умения: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты

	соответствии с требованиями эксплуатационной документации.	информации автоматизированных систем
	ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Умения: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Умения: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
	ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Умения: обеспечивать работоспособность, обнаруживать и устранять неисправности
	ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Умения: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации

## 2) общие компетенции

Код	Наименование компетенции	Показатели освоения компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Выбирает способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Осуществляет поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие	Планирует и реализовывает собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Работает в коллективе и команде, эффективно взаимодействует с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Осуществляет устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	Проявляет гражданско-патриотическую позицию, демонстрирует осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Содействует сохранению окружающей среды, ресурсосбережению, эффективно действует в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использует средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддерживает необходимый уровень физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности	Использует информационные технологии в профессиональной деятельности



### **1.3. Количество часов, отводимое на освоение учебной практики:**

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении – 36 часов.

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными - 36 часов.

ПМ.03 Защита информации техническими средствами – 36 часов.

ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных – 36 часов.

Промежуточная аттестация по учебной практике:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении – дифференцированный зачет.

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными – дифференцированный зачет.

ПМ.03 Защита информации техническими средствами – дифференцированный зачет.

ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных – дифференцированный зачет.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

№ п/п	Индекс модуля, МДК	Виды работ	Номер задания по практике	Наименование лаборатории	Кол-во часов
<b>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b>					
№ п/п	Индекс модуля, МДК	Виды работ	Номер задания по практике	Наименование лаборатории	Кол-во часов
<b>1.</b>	МДК.01.01. Операционные системы	Анализ и управление процессами в ОС	Задание 1	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	<b>2</b>
		Работа с файловой системой и правами доступа	Задание 2	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
		Настройка сетевых параметров и диагностика	Задание 3	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
		Работа с системным реестром (Windows) или системными журналами (Linux)	Задание 4	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	<b>2</b>
		Управление дисками и разделами	Задание 5	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
		Написание простого скрипта автоматизации	Задание 6	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
<b>2.</b>	МДК.01.02. Базы данных	Проектирование и создание базы данных	Задание 7	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	<b>2</b>
		Наполнение базы данных и основные операции (CRUD)	Задание 8	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
		Составные запросы и агрегация данных	Задание 9	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	

				технологий, программирования и баз данных	
		Работа с представлениями (Views) и индексами	Задание 10	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Реализация бизнес-логики с помощью хранимых процедур и триггеров	Задание 11	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
		Резервное копирование и восстановление базы данных	Задание 12	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	
3.	МДК.01.03. Сети и системы передачи информации	Проектирование и настройка локальной сети с разделением на подсети (IP-планирование)	Задание 13	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Настройка VLAN (Virtual Local Area Network) на коммутаторе	Задание 14	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Анализ сетевого трафика с помощью Wireshark	Задание 15	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Настройка и диагностика DHCP и DNS	Задание 16	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Настройка статической и динамической маршрутизации (OSPF)	Задание 17	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Настройка базовой безопасности сети (ACL, NAT)	Задание 18	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
4.	МДК.01.04. Эксплуатация автоматизированных (информационн	Развертывание и ввод в эксплуатацию защищенной АИС	Задание 19	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Управление доступом в защищенной АИС на основе ролевой модели (RBAC)	Задание 20	<b>Лаборатория</b> Информационных технологий, программирования и	2

	ых) систем в защищенном исполнении			баз данных	
		Аудит и мониторинг безопасности АИС	Задание 21	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Резервное копирование и восстановление работоспособности АИС после сбоя	Задание 22	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Обеспечение криптографической защиты информации в АИС	Задание 23	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
5.	МДК.01.05 Эксплуатация компьютерных сетей	Плановое техническое обслуживание и мониторинг сетевой инфраструктуры	Задание 24	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Диагностика и устранение комплексного сетевого сбоя	Задание 25	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
		Модернизация сети: добавление новой подсети и настройка безопасности	Задание 26	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	2
	Итого по ПМ.01				36
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными					
№ п/п	Индекс модуля, МДК	Виды работ	Номер задания по практике	Наименование лаборатории	Кол-во часов
1.	МДК.02.01 Программные и программно-аппаратные средства защиты информации	Администрирование систем аутентификации и управления доступом	Задание 1	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Управление криптографическими средствами	Задание 2	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Эксплуатация систем обнаружения и предотвращения вторжений. Антивирусная защита и защита от вредоносного ПО	Задание 3	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
2.	МДК.02.02 Криптографичес	Эксплуатация аппаратных модулей доверенной загрузки	Задание 4	<b>Лаборатория</b> Информационных технологий, программирования и	6

	кие средства защиты информации			баз данных	
		Работа с аппаратными средствами криптографии	Задание 5	Лаборатория Информационных технологий, программирования и баз данных	6
		Администрирование систем контроля доступа в помещения. Эксплуатация систем защиты от утечек информации (DLP)	Задание 6	Лаборатория Информационных технологий, программирования и баз данных	6
Итого по ПМ.02					36
№ п/п	Индекс модуля, МДК	Виды работ	Номер задания по практике	Наименование лаборатории	Кол-во часов
ПМ.03 Защита информации техническими средствами					
1.	МДК.03.01. Техническая защита информации	Анализ и оценка защищенности автоматизированной системы организации	Задание 1	Лаборатория Информационных технологий, программирования и баз данных	6
		Исследование и настройка средств криптографической защиты информации (СКЗИ)	Задание 2	Лаборатория Информационных технологий, программирования и баз данных	6
		Анализ защищенности каналов связи и сегмента сети организации	Задание 3	Лаборатория Информационных технологий, программирования и баз данных	6
2.	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	Аудит и оценка эффективности системы контроля и управления доступом (СКУД) на объекте информатизации:	Задание 4	Лаборатория Информационных технологий, программирования и баз данных	6
		Исследование системы видеонаблюдения как элемента физической защиты объекта информатизации	Задание 5	Лаборатория Информационных технологий, программирования и баз данных	6
		Проектирование (или модернизация) системы инженерно-технической укреплённости и охранной сигнализации периметра и помещений	Задание 6	Лаборатория Информационных технологий, программирования и баз данных	6
Итого по ПМ.03.					36
№ п/п	Индекс модуля, МДК	Виды работ	Номер задания по практике	Наименование лаборатории	Кол-во часов
ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных					
1.	МДК.04.01	Работа с файловой системой и данными	Задание 1	Лаборатория Информационных	6

	Выполнение работ по профессии Оператор электронно-вычислительных и вычислительных машин			технологий, программирования и баз данных	
		Ввод и обработка цифровой и текстовой информации	Задание 2	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Работа с периферийным оборудованием и оргтехникой	Задание 3	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Обеспечение функционирования программного обеспечения	Задание 4	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Поддержка коммуникаций и документооборота	Задание 5	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
		Техническое обслуживание рабочих мест	Задание 6	<b>Лаборатория</b> Информационных технологий, программирования и баз данных	6
				<b>Итого по ПМ.04</b>	<b>36</b>

# ЗАДАНИЯ ПО УЧЕБНОЙ ПРАКТИКЕ

## ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

### Задание 1. Анализ и управление процессами в ОС

#### Условия выполнения задания:

Освоить методы мониторинга, управления и анализа процессов с помощью встроенных утилит операционной системы.

#### Примерный алгоритм выполнения задания:

##### 1. Мониторинг запущенных процессов:

- Windows: Откройте Диспетчер задач (Ctrl+Shift+Esc). Изучите вкладки "Процессы" и "Подробности". Обратите внимание на колонки: Имя образа (исполняемый файл), PID (Идентификатор процесса), ЦП, Память, Описание.
- Linux: Откройте терминал. Выполните команду `top` или `htop` (если установлена). Изучите вывод: PID, USER, %CPU, %MEM, COMMAND. Для вывода списка в виде таблицы используйте `ps aux`.
- Зафиксируйте в отчете: 5 процессов с наибольшим потреблением ЦП и 5 процессов с наибольшим потреблением оперативной памяти.

##### 2. Управление процессами:

- Windows: В Диспетчере задач найдите малозначительный процесс (например, "Блокнот"). Щелкните по нему правой кнопкой мыши и выберите "Снять задачу". Опишите результат.
- Linux: В терминале запустите фоновый процесс, например, `sleep 300 &`. Запишите его PID. Затем принудительно завершите его с помощью команды `kill -9 <PID>`. Проверьте его отсутствие в списке процессов (`ps aux | grep sleep`).
- Зафиксируйте в отчете: Название процесса, его PID, команду для завершения и результат.

##### 3. Анализ дерева процессов:

- Windows: Скачайте и запустите утилиту Process Explorer от Microsoft Sysinternals. Проанализируйте дерево процессов. Найдите родительский процесс (например, `explorer.exe`) и его дочерние процессы.
- Linux: В терминале выполните команду `pstree`. Проанализируйте иерархию. Определите, какой процесс является родительским для большинства других (обычно `systemd` или `init`).
- Зафиксируйте в отчете: Скриншот дерева процессов и краткое описание иерархии на примере 3-4 связанных процессов.

### Задание 2. Работа с файловой системой и правами доступа

#### Условия выполнения задания:

Научиться управлять файлами, каталогами и правами доступа к ним из командной строки.

#### Примерный алгоритм выполнения задания:

##### 1. Создание структуры каталогов и файлов:

- Windows (CMD): Создайте каталог `C:\Practice\_OS`. Внутри него создайте две папки: `Reports` и `Sources`. В папке `Reports` создайте пустой файл `report.txt`.
- Linux (Terminal): Создайте каталог `~/practice\_os`. Внутри него создайте две папки: `reports` и `sources`. В папке `reports` создайте пустой файл `report.txt` с помощью команды `touch`.
- Зафиксируйте в отчете: Полный путь к созданной структуре и команды, которые использовались.

##### 2. Управление правами доступа (Linux) / Атрибутами (Windows):

- Linux: Для папки `reports` установите права `755` (владелец: чтение-запись-выполнение, группа и остальные: чтение-выполнение). Для файла `report.txt` установите права `644`. Используйте команду `chmod`. Проверьте права с помощью `ls -l`.

- Windows: Для папки 'Reports' щелкните правой кнопкой -> "Свойства" -> "Безопасность". Проанализируйте список групп/пользователей и их разрешения. Попробуйте изменить разрешения для группы "Пользователи".

- Зафиксируйте в отчете: Команды (Linux) или действия (Windows) для изменения прав/разрешений и скриншоты, подтверждающие изменения.

### 3. Поиск файлов:

- Windows: С помощью командной строки выполните поиск всех текстовых файлов (.txt) в созданном каталоге 'C:\Practice\_OS': `dir C:\Practice_OS\*.txt /s`.

- Linux: С помощью терминала выполните поиск всех файлов с расширением '.txt' в домашнем каталоге: `find ~/ -name "*.txt"`.

- Зафиксируйте в отчете: Команду поиска и ее вывод.

## **Задание 3. Настройка сетевых параметров и диагностика**

### Условия выполнения задания:

Получить практические навыки по настройке и проверке сетевых подключений.

### Примерный алгоритм выполнения задания:

#### 1. Определение сетевых параметров:

- Windows: Откройте командную строку. Выполните `ipconfig /all`. Определите: IPv4-адрес, MAC-адрес, адрес шлюза по умолчанию и DNS-сервера для вашего основного сетевого адаптера.

- Linux: Откройте терминал. Выполните `ip addr` или `ifconfig`. Определите те же параметры.

- Зафиксируйте в отчете: Таблицу с найденными сетевыми параметрами.

#### 2. Диагностика сетевого соединения:

- Проверьте связь с шлюзом по умолчанию с помощью `ping` (например, `ping 192.168.1.1`).

- Проверьте связь с внешним ресурсом, например, с `google.com` (`ping google.com`).

- Выполните трассировку маршрута до `google.com` с помощью `tracert` (Windows) или `traceroute` (Linux).

- Зафиксируйте в отчете: Результаты команд, включая среднее время отклика и количество хопов до целевого узла.

#### 3. Анализ сетевых статистических данных:

- Windows: Выполните команду `netstat -an`. Проанализируйте список открытых портов. Найдите порты в состоянии "LISTENING" (ожидают подключения) и "ESTABLISHED" (установленные соединения).

- Linux: Выполните команду `ss -tuln` (более современный аналог `netstat`). Проанализируйте, какие сервисы слушают какие порты.

- Зафиксируйте в отчете: Список 3-5 наиболее интересных портов в состоянии "LISTENING" и предположите, каким службам они могут принадлежать.

.

## **Задание 4. Работа с системным реестром (Windows) или системными журналами (Linux)**

### Условия выполнения задания:

Понять принципы хранения конфигурации системы и научиться анализировать ее логи.

### Примерный алгоритм выполнения задания:

#### 1. Поиск и анализ информации:

- Windows: Откройте Редактор реестра (`regedit`). Перейдите к ветке `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`. Найдите и запишите значения параметров: `ProductName`, `RegisteredOwner`, `SystemRoot`.



- Linux: Откройте терминал. Просмотрите системный журнал с помощью команды `journalctl -xe` или файл `/var/log/syslog`. Найдите записи (логи) за последний час, относящиеся к демону `cron` или `systemd`.

- Зафиксируйте в отчете: Найденные значения (Windows) или несколько последних записей из лога (Linux).

2. Создание резервной копии и внесение безопасного изменения:

- Windows: В реестре создайте новую ветку в `HKEY\_CURRENT\_USER\Software` с названием `TestPractice`. Внутри создайте строковый параметр `University` со значением вашего учебного заведения. Перед этим экспортируйте эту ветку (правой кнопкой -> "Экспорт") в файл `backup.reg`.

- Linux: Создайте простую задачу для планировщика `cron`. Выполните `crontab -e` и добавьте строку `----- echo "Практика по ОС" >> ~/practice\_log.txt`. Эта команда будет каждую минуту дописывать строку в файл. Подождите 2-3 минуты и проверьте содержимое файла `~/practice\_log.txt`.

- Зафиксируйте в отчете: Действия по созданию резервной копии, команды/действия по внесению изменения и результат.

3. Откат изменений:

- Windows: Удалите созданную ветку `TestPractice`. Либо выполните двойной щелчок по файлу `backup.reg`, чтобы восстановить исходное состояние (если бы вы вносили изменения в существующие ключи).

- Linux: Удалите строку из crontab (`crontab -e`) и удалите файл `~/practice\_log.txt`.

- Зафиксируйте в отчете: Действия, выполненные для отката системы к исходному состоянию..

## **Задание 5. Написание простого скрипта автоматизации**

### Условия выполнения задания:

Закрепить навыки работы с командной строкой, объединив их в сценарий автоматизации.

### Примерный алгоритм выполнения задания:

1. Постановка задачи для скрипта:

- Скрипт должен создавать папку для резервных копий (если ее нет).
- Копировать в нее все текстовые файлы из указанной директории.
- Архивировать содержимое этой папки в файл с текущей датой в имени.
- Выводить сообщение об успешном завершении.

2. Написание скрипта:

- Windows (Пакетный файл .bat):

```
``bat
```

```
@echo off
```

```
set backup_dir=%USERPROFILE%\MyBackups
```

```
set source_dir=%USERPROFILE%\Documents
```

```
set date=%date:~-10,2%-date:~-7,2%-date:~-4,4%
```

```
if not exist "%backup_dir%" mkdir "%backup_dir%"
```

```
xcopy "%source_dir%\*.txt" "%backup_dir%" /Y
```

```
"%ProgramFiles%\7-Zip\7z.exe" a "%backup_dir%\backup_%date%.zip"
```

```
"%backup_dir%\*.txt"
```

```
echo Резервное копирование текстовых файлов завершено!
```

```
pause
```

```
``
```

- Linux (Bash-скрипт .sh):

```
``bash
```

```
#!/bin/bash
```

```

backup_dir="$HOME/my_backups"
source_dir="$HOME"
current_date=$(date +%d-%m-%Y)
    mkdir -p "$backup_dir"
find "$source_dir" -name "-.txt" -exec cp {} "$backup_dir" \;
tar -czf "$backup_dir/backup_${current_date}.tar.gz" "$backup_dir"/-.txt
echo "Резервное копирование текстовых файлов завершено!"
`

```

### 3. Запуск и тестирование:

- Сохраните код в файл с соответствующим расширением (`.bat` или `.sh`).
- Linux: Дайте права на выполнение: `chmod +x script.sh`.
- Запустите скрипт.
- Проверьте, создалась ли папка, скопировались ли файлы и создался ли архив.
- Зафиксируйте в отчете: Исходный код скрипта, скриншоты процесса запуска и результата (содержимое папки с архивом)..

## Задание 6. Работы в системе контроля версий

### Условия выполнения задания:

Освоить базовые принципы работы с дисковыми пространствами.

### Примерный алгоритм выполнения задания:

#### 1. Анализ текущей структуры дисков:

- Windows: Откройте "Управление дисками" (diskmgmt.msc). Проанализируйте список дисков, разделов, их файловые системы, размер и свободное место.
- Linux: Выполните в терминале команды `lsblk` и `df -h`. Проанализируйте вывод, определите корневой раздел, его размер, занятое и свободное пространство.
- Зафиксируйте в отчете: Скриншот или текстовый вывод, демонстрирующий структуру дисков.

#### 2. Работа с виртуальным диском (VHD/Wirtual Disk):

- Windows: В "Управлении дисками" создайте новый виртуальный жесткий диск (VHD) размером 1 ГБ. Инициализируйте его (MBR) и создайте простой том с файловой системой NTFS. Назначьте букву диска.
- Linux: Создайте файл-образ диска: `dd if=/dev/zero of=~/.disk\_image.img bs=1M count=100`. Создайте на нем файловую систему: `mkfs.ext4 ~/.disk\_image.img`. Смонтируйте его: `sudo mount ~/.disk\_image.img /mnt`.
- Зафиксируйте в отчете: Последовательность действий и команды. Скриншот, подтверждающий, что новый диск/образ смонтирован и доступен.

#### 3. Демонтаж и удаление:

- Windows: В "Управлении дисками" отключите созданный VHD.
- Linux: Размонтируйте образ: `sudo umount /mnt`. Удалите файл `~/.disk\_image.img`.
- Зафиксируйте в отчете: Действия по корректному удалению виртуального носителя.

## Задание 7. Проектирование и создание базы данных

### Условия выполнения задания:

Освоить этапы концептуального и логического проектирования БД, создать физическую модель и реализовать её в СУБД.

### Примерный алгоритм выполнения задания:

#### 1. Концептуальное проектирование (ER-диаграмма):

- Выберите предметную область (например, "Библиотека", "Интернет-магазин", "Больница").
- Определите сущности (например, для "Библиотека": Книга, Читатель, Автор, Издательство).

- Определите атрибуты для каждой сущности (например, Книга: `book\_id`, `title`, `isbn`, `year`).
  - Определите связи между сущностями (например, "Книга" связана с "Автором" связью "многие-ко-многим", так как одна книга может иметь несколько авторов, и один автор может написать несколько книг).
  - Нарисуйте ER-диаграмму (можно использовать draw.io, Lucidchart или встроенные средства СУБД).
2. Логическое проектирование (Нормализация до НФБК):
- Преобразуйте ER-модель в реляционную схему. Создайте таблицы для каждой сущности.
  - Для связи "многие-ко-многим" создайте промежуточную таблицу (например, `BookAuthor` с полями `book\_id` и `author\_id`).
  - Определите первичные ключи (ПК) для каждой таблицы.
  - Определите внешние ключи (FK) для обеспечения связей между таблицами.
  - Убедитесь, что схема соответствует минимум 3-й нормальной форме (3NF): все неключевые атрибуты зависят только от первичного ключа и не зависят друг от друга.
3. Физическое создание БД в СУБД:
- Откройте клиент для работы с СУБД (например, pgAdmin для PostgreSQL, MySQL Workbench, SSMS для SQL Server).
  - Напишите и выполните SQL-скрипт для создания базы данных: `CREATE DATABASE library_db;`
  - Напишите и выполните SQL-скрипты для создания таблиц в соответствии со спроектированной схемой, используя `CREATE TABLE`, указав типы данных, первичные и внешние ключи.

### **Задание 8. Наполнение базы данных и основные операции (CRUD)**

#### Условия выполнения задания:

Научиться выполнять базовые операции по манипуляции данными: создание, чтение, обновление, удаление (CRUD).

#### Примерный алгоритм выполнения задания:

##### 1. Вставка данных (Create):

- Напишите серию SQL-команд `INSERT INTO` для заполнения всех созданных таблиц тестовыми данными.
- Вставьте не менее 5 записей в каждую основную таблицу и не менее 10 записей в промежуточные таблицы (например, `BookAuthor`).
- Используйте различные способы вставки: по одному кортежу и множественная вставка (например, `INSERT INTO ... VALUES (...), (...), ...;`).

##### 2. Выборка и фильтрация данных (Read):

- Напишите SELECT-запросы для вывода всех данных из каждой таблицы.
- Реализуйте выборки с фильтрацией:
  - Вывести книги, изданные после 2010 года (`WHERE year > 2010`).
  - Вывести читателей с фамилией, начинающейся на "Ивано" (`WHERE last_name LIKE 'Ивано%'`).
  - Вывести книги, которые находятся "на руках" у читателей (предположим, есть поле `status` или таблица выдачи).

##### 3. Обновление и удаление данных (Update, Delete):

- Обновление: Напишите запрос `UPDATE`, который изменит значение одного из атрибутов для конкретной записи (например, изменить год издания для определенной книги).
- Удаление: Напишите запрос `DELETE`, который удалит одну из записей, не нарушающую целостность данных (например, удалить автора, который не связан ни с

одной книгой в промежуточной таблице). Продемонстрируйте каскадное удаление или его отсутствие.

### **Задание 9. Составные запросы и агрегация данных**

#### Условия выполнения задания:

Освоить работу с многотабличными запросами, соединениями (JOIN) и агрегирующими функциями.

#### Примерный алгоритм выполнения задания:

##### 1. Использование соединений (JOIN):

- Напишите запрос с 'INNER JOIN' для вывода данных из нескольких связанных таблиц. Например: "Вывести названия всех книг и их авторов".
- Напишите запрос с 'LEFT JOIN'. Например: "Вывести всех читателей и названия книг, которые у них на руках (если есть)".
- Напишите запрос с двумя и более соединениями. Например: "Вывести название книги, ее авторов и издательство".

##### 2. Группировка и агрегирующие функции:

- Используйте функции 'COUNT(), SUM(), AVG(), MAX(), MIN()'.  
- Напишите запрос, который подсчитывает количество книг у каждого автора ('GROUP BY author\_id').
- Напишите запрос, который выводит издательства и средний год издания книг для каждого из них.
- Напишите запрос, который находит читателя, взявшего наибольшее количество книг.

##### 3. Фильтрация групп (HAVING):

- Используйте конструкцию 'HAVING' для фильтрации результатов группировки.
- Напишите запрос: "Вывести авторов, у которых количество книг в библиотеке больше 2".
- Напишите запрос: "Вывести издательства, средний год издания книг которых позже 2005 года".

### **Задание 10. Работа с представлениями (Views) и индексами**

#### Условия выполнения задания:

Научиться создавать виртуальные таблицы (представления) для упрощения сложных запросов и оптимизировать производительность с помощью индексов.

#### Примерный алгоритм выполнения задания:

##### 1. Создание представлений:

- Создайте представление ('CREATE VIEW') для частого сложного запроса. Например, представление 'ActiveLoans', которое показывает ФИО читателя, название книги и дату выдачи для всех книг на руках.
- Создайте представление, которое объединяет данные о книге, ее авторах и издательстве в одну удобную для отчета виртуальную таблицу.
- Выполните простой 'SELECT - FROM your\_view;', чтобы продемонстрировать работу представления.

##### 2. Создание индексов:

- Проанализируйте, по каким полям чаще всего происходит поиск ('WHERE') и соединение ('JOIN').
- Создайте индексы ('CREATE INDEX') для этих полей. Например, создайте индекс по полю 'last\_name' в таблице 'Readers' и по полю 'title' в таблице 'Books'.
- Создайте составной индекс для полей, которые часто используются вместе в условиях 'WHERE'.

### 3. Анализ производительности запросов:

- Напишите запрос, который будет явно использовать созданные индексы (например, поиск читателя по фамилии).
- Используйте команду объяснения плана запроса ('EXPLAIN' или 'EXPLAIN ANALYZE' в PostgreSQL, 'EXPLAIN' в MySQL) для этого запроса до и после создания индекса.
- Зафиксируйте в отчете: Сравните планы выполнения и сделайте вывод об эффективности индексов.

## **Задание 11. Реализация бизнес-логики с помощью хранимых процедур и триггеров**

### Условия выполнения задания:

Научиться инкапсулировать логику работы с данными на стороне.

### Примерный алгоритм выполнения задания:

#### 1. Создание хранимой процедуры:

- Напишите хранимую процедуру, которая реализует сложную бизнес-операцию. Например: процедура 'BorrowBook(reader\_id, book\_id)', которая:
  - Проверяет, доступна ли книга.
  - Добавляет запись в таблицу выдачи ('Loans').
  - Изменяет статус книги на "выдана".
- Вызовите процедуру, передав ей необходимые параметры, и проверьте корректность ее работы.

#### 2. Создание триггера на добавление (BEFORE/AFTER INSERT):

- Создайте триггер, который срабатывает перед добавлением новой книги ('BEFORE INSERT ON Books').
  - Логика триггера: проверять корректность года издания (он не может быть больше текущего года). Если проверка не пройдена, генерировать ошибку и отменять операцию вставки.
- Протестируйте триггер, попытавшись добавить книгу с некорректным годом.

#### 3. Создание триггера на обновление (AFTER UPDATE):

- Создайте триггер, который срабатывает после обновления статуса книги в таблице 'Loans' на "возвращена".
  - Логика триггера: автоматически увеличивать значение счетчика прочитанных книг ('books\_read') у соответствующего читателя в таблице 'Readers'.
- Протестируйте триггер, обновив запись о выдаче и проверив изменение данных о читателе.

## **Задание 12. Резервное копирование и восстановление базы данных**

### Условия выполнения задания:

Освоить основные методы создания резервных копий базы данных и их восстановления.

### Примерный алгоритм выполнения задания:

#### 1. Создание полной резервной копии:

- Средствами СУБД: Используйте встроенные утилиты (например, 'pg\_dump' для PostgreSQL, 'mysqldump' для MySQL, "Backup Database" в SSMS).
- Командная строка: Выполните команду для создания дампа (dump) базы данных в файл (например, 'pg\_dump -U username library\_db > backup.sql').
- Зафиксируйте в отчете: Команду или последовательность действий, а также размер и местоположение полученного файла резервной копии.

#### 2. Восстановление базы данных из резервной копии:

- Метод 1 (Удаление и создание заново): Удалите исходную базу данных (`'DROP DATABASE library_db;'`) и восстановите ее из дампа (например, `'psql -U username -d postgres -f backup.sql'`).

- Метод 2 (Восстановление поверх существующей): Воспользуйтесь утилитой восстановления в графическом клиенте СУБД.

- Убедитесь, что после восстановления все данные и объекты (таблицы, представления, процедуры) находятся на своем месте, выполнив несколько проверочных `SELECT`-запросов.

### 3. Создание транзакции для обеспечения целостности данных:

- Смоделируйте ситуацию, требующую атомарности (все или ничего). Например, перевод книги из одного статуса в другой должен сопровождаться записью в таблицу истории.

- Напишите скрипт, который использует `'BEGIN TRANSACTION'`, несколько операций `'UPDATE/INSERT'`, и `'COMMIT'`.

- Смоделируйте ошибку (например, вставьте неверные данные) и используйте `'ROLLBACK'` для отката всех изменений в рамках транзакции. Продемонстрируйте, что данные не изменились.

## Задание 13. Проектирование и настройка локальной сети с разделением на подсети (IP-планирование)

### Условия выполнения задания:

Освоить принципы проектирования IP-сетей, расчета масок подсетей и базовой настройки сетевых интерфейсов.

### Примерный алгоритм выполнения задания:

#### 1. Разработка схемы сети и планирование IP-адресации:

- Разработка схемы: Нарисуйте логическую схему сети, включающую 3 подсети:
  - Подсеть для отдела бухгалтерии (требуется 10 рабочих мест).
  - Подсеть для отдела разработки (требуется 20 рабочих мест).
  - Подсеть для серверов (требуется 5 адресов).
- Выбор адреса: Исходная сеть: `'192.168.50.0/24'`.
- Расчет подсетей: Рассчитайте маски подсетей и диапазоны IP-адресов для каждого отдела, чтобы обеспечить необходимое количество хостов. Результаты оформите в таблицу:

Отдел	Требуется хостов	Маска подсети	Диапазон адресов	Шлюз по умолчанию
Бухгалтерия	10	<code>'/28'</code> ( <code>'255.255.255.240'</code> )	<code>'192.168.50.1' - '192.168.50.14'</code>	<code>'192.168.50.1'</code>
Разработка	20	<code>'/27'</code> ( <code>'255.255.255.224'</code> )	<code>'192.168.50.33' - '192.168.50.62'</code>	<code>'192.168.50.33'</code>
Серверы	5	<code>'/29'</code> ( <code>'255.255.255.248'</code> )	<code>'192.168.50.65' - '192.168.50.70'</code>	<code>'192.168.50.65'</code>

#### 2. Настройка сетевых интерфейсов на маршрутизаторе (эмулятор, например, Cisco Packet Tracer):

- Добавьте на схему маршрутизатор (например, Cisco 2911).
- Настройте интерфейсы маршрутизатора в соответствии с рассчитанными шлюзами:
  - `'interface g0/0.10'` (VLAN для бухгалтерии): `'ip address 192.168.50.1 255.255.255.240'`
  - `'interface g0/0.20'` (VLAN для разработки): `'ip address 192.168.50.33 255.255.255.224'`
  - `'interface g0/0.30'` (VLAN для серверов): `'ip address 192.168.50.65 255.255.255.248'`
- Включите интерфейсы командой `'no shutdown'`.

### 3. Проверка связности:

- Добавьте на схему компьютеры в каждой подсети и настройте им статические IP-адреса из соответствующих диапазонов, указав в качестве шлюза адрес маршрутизатора.
- С помощью утилиты `ping` проверьте связность:
  - С компьютера в подсети бухгалтерии до шлюза (`ping 192.168.50.1`).
  - С компьютера в подсети бухгалтерии до компьютера в подсети серверов (`ping 192.168.50.66`).
- Проанализируйте результаты.

2.4 Заказчик хочет убедиться, что ПО держит нагрузку в 2000 пользователей.

## **Задание 14: Настройка VLAN (Virtual Local Area Network) на коммутаторе**

### Условия выполнения задания:

Научиться сегментировать сеть на логическом уровне для повышения безопасности и производительности.

### Примерный алгоритм выполнения задания:

#### 1. Создание VLAN и назначение имен:

- Подключитесь к коммутатору (в эмуляторе или через консоль).
- Перейдите в режим глобальной конфигурации (`configure terminal`).
- Создайте VLAN для отделов:
  - `vlan 10` → `name Accounting`
  - `vlan 20` → `name Developers`
  - `vlan 30` → `name Servers`

#### 2. Настройка портов доступа (Access Ports):

- Настройте интерфейсы, к которым подключены конечные пользователи, в режиме доступа и назначьте им соответствующие VLAN:
  - `interface fastEthernet 0/1` → `switchport mode access` → `switchport access vlan 10`
  - `interface fastEthernet 0/2` → `switchport mode access` → `switchport access vlan 20`
- Аналогично для других портов.

#### 3. Настройка магистрального порта (Trunk Port):

- Настройте порт, соединяющий коммутатор с маршрутизатором, в режиме транка. Это позволит передавать трафик нескольких VLAN по одному физическому каналу.
  - `interface gigabitEthernet 0/1` → `switchport mode trunk` → `switchport trunk allowed vlan 10,20,30`
- Проверьте конфигурацию VLAN командой `show vlan brief` и конфигурацию транка командой `show interfaces trunk`.

## **Задание 15: Анализ сетевого трафика с помощью Wireshark**

### Условия выполнения задания:

Освоить базовые навыки захвата, фильтрации и анализа сетевых пакетов для диагностики проблем и понимания протоколов.

### Примерный алгоритм выполнения задания:

#### 1. Захват трафика:

- Установите Wireshark.
- Запустите захват пакетов на основном сетевом интерфейсе.
- Сгенерируйте различный трафик: откройте веб-страницу в браузере, выполните `ping` до удаленного узла (например, `google.com`).

## 2. Применение фильтров:

- Остановите захват.
- Используйте фильтры для анализа конкретного трафика:
  - `icmp` – чтобы увидеть только ICMP-пакеты (пинги).
  - `dns` – чтобы увидеть только DNS-запросы и ответы.
  - `http` – чтобы увидеть HTTP-трафик (нешифрованный).
  - `ip.addr == <ваш IP>` – чтобы увидеть весь трафик, связанный с вашим компьютером.

## 3. Анализ пакетов и составление отчета:

- Выберите любой TCP-пакет. Разверните его и опишите в отчете структуру: Ethernet-кадр, IP-пакет, TCP-сегмент.
- Найдите DNS-пакет. Определите, это запрос или ответ? Какое имя запрашивалось и какой IP-адрес был получен?
- Найдите трехстороннее рукопожатие TCP (SYN, SYN-ACK, ACK) при установке соединения с веб-сервером. Зафиксируйте номера портов клиента и сервера.

## **Задание 16: Настройка и диагностика DHCP и DNS**

### Условия выполнения задания:

#### **Требования к рабочему месту:**

Компьютер с ОС Windows Server 2019/2022 или Linux

Установленная роль DHCP-сервера и DNS-сервера

Доступ к оснасткам управления серверами

Сетевой интерфейс с статическим IP-адресом

Права администратора на сервере

#### **Исходные данные:**

Диапазон IP-адресов для DHCP: 192.168.1.100-192.168.1.200

Маска подсети: 255.255.255.0

Шлюз по умолчанию: 192.168.1.1

DNS-серверы: 192.168.1.10 и 8.8.8.8

Домен: company.local.

### Примерный алгоритм выполнения задания:

#### 1: Настройка DHCP-сервера

##### 1.1. Установка и настройка роли DHCP-сервера

powershell

Установка роли DHCP-сервера в Windows Server

Install-WindowsFeature DHCP -IncludeManagementTools

Добавление сервера в авторизованные DHCP-серверы

Add-DhcpServerInDC -DnsName "dhcp1.company.local" -IPAddress 192.168.1.10

##### 1.2. Создание и настройка области (scope) DHCP

powershell

Создание области DHCP

Add-DhcpServerV4Scope -Name "MainOffice" `

-StartRange 192.168.1.100 `

-EndRange 192.168.1.200 `

-SubnetMask 255.255.255.0 `

-State Active



Настройка параметров области

```
Set-DhcpServerV4OptionValue -ScopeId 192.168.1.0 `
    -DnsDomain "company.local" `
    -DnsServer 192.168.1.10, 8.8.8.8 `
    -Router 192.168.1.1
```

Настройка времени аренды

```
Set-DhcpServerV4Scope -ScopeId 192.168.1.0 `
    -LeaseDuration 8.00:00:00
```

### 1.3. Резервирование адресов и настройка исключений

powershell

Добавление исключений (адреса, не выдаваемые по DHCP)

```
Add-DhcpServerV4ExclusionRange -ScopeId 192.168.1.0 `
    -StartRange 192.168.1.1 `
    -EndRange 192.168.1.50
```

Резервирование IP-адреса для конкретного устройства

```
Add-DhcpServerV4Reservation -ScopeId 192.168.1.0 `
    -IPAddress 192.168.1.150 `
    -ClientId "AA-BB-CC-DD-EE-FF" `
    -Description "Network Printer"
```

## 2: Настройка DNS-сервера

### 2.1. Установка и базовая настройка DNS-сервера

powershell

Установка роли DNS-сервера

```
Install-WindowsFeature DNS -IncludeManagementTools
```

Проверка состояния DNS-сервера

```
Get-Service -Name DNS
```

Настройка корневых подсказок (root hints)

```
Get-DnsServerRootHint
```

### 2.2. Создание зон и записей DNS

powershell

Создание прямой зоны поиска

```
Add-DnsServerPrimaryZone -Name "company.local" `
    -ZoneFile "company.local.dns" `
    -DynamicUpdate Secure
```

Создание обратной зоны поиска

```
Add-DnsServerPrimaryZone -NetworkId "192.168.1.0/24" `
    -ZoneFile "1.168.192.in-addr.arpa.dns" `
    -DynamicUpdate Secure
```

Добавление A-записей

```
Add-DnsServerResourceRecordA -Name "webserver" `
    -ZoneName "company.local" `
    -IPv4Address "192.168.1.20" `
```

-TimeToLive 01:00:00

Добавление CNAME-записи

```
Add-DnsServerResourceRecordCName -Name "www" `
    -HostNameAlias "webserver.company.local" `
    -ZoneName "company.local"
```

### 2.3. Настройка условных перенаправлений и безопасности

powershell

Добавление условного перенаправления

```
Add-DnsServerConditionalForwarderZone -Name "branch.company.com" `
    -MasterServers 192.168.2.10
```

Настройка передачи зон (если есть вторичные DNS-серверы)

```
Add-DnsServerZoneTransfer -Name "company.local" `
    -SecondaryServer "192.168.1.11"
```

Включение защиты от кэширования отравления

```
Set-DnsServerResponseRateLimiting -LogOnly $false `
    -Mode Enable
```

### 3: Диагностика и устранение неисправностей

#### 3.1. Диагностика работы DHCP-сервера

powershell

Проверка статистики DHCP-сервера

```
Get-DhcpServerv4ScopeStatistics
```

Просмотр арендованных адресов

```
Get-DhcpServerv4Lease -ScopeId 192.168.1.0
```

Проверка доступности DHCP-сервера

```
Test-NetConnection -ComputerName 192.168.1.10 -Port 67
```

Аудит событий DHCP

```
Get-EventLog -LogName "System" -Source "DHCP Server" -Newest 50
```

#### 3.2. Диагностика работы DNS-сервера

powershell

Проверка разрешения имен

```
Resolve-DnsName "webserver.company.local" -Server 192.168.1.10
```

Тестирование рекурсивных запросов

```
Resolve-DnsName "google.com" -Server 192.168.1.10
```

Проверка состояния зон DNS

```
Get-DnsServerZone | Format-Table ZoneName, ZoneType, State
```

Диагностика с помощью nslookup

```
nslookup webserver.company.local 192.168.1.10
```

```
nslookup 192.168.1.20 192.168.1.10
```

#### 3.3. Мониторинг и решение типовых проблем

powershell

Проверка связанных служб

```
Get-Service -Name "DHCPServer", "DNS"
```

Анализ журналов событий

```
Get-EventLog -LogName "System" -EntryType Error,Warning -Newest 20
```

Проверка конфигурации сети на клиенте

```
ipconfig /all
```

```
ipconfig /release
```

```
ipconfig /renew
```

Очистка DNS-кэша на клиенте

```
ipconfig /flushdns
```

Диагностика с помощью утилиты dnscmd

```
dnscmd /info
```

4: Интеграция и тестирование

4.1. Интеграция DHCP и DNS

powershell

Настройка динамического обновления DNS от DHCP

```
Set-DhcpServerv4DnsSetting -DynamicUpdates "Always" `
    -DeleteDnsRROnLeaseExpiry $true
```

Проверка интеграции

```
Get-DhcpServerv4DnsSetting
```

4.2. Комплексное тестирование работы

powershell

Тест получения IP-адреса по DHCP

```
$lease = Get-DhcpServerv4Lease -ScopeId 192.168.1.0 | Select-Object -First 1
Write-Host "Арендованный адрес: $($lease.IPAddress)"
```

Тест разрешения имен

```
$dnsTest = Resolve-DnsName "webserver.company.local" -ErrorAction SilentlyContinue
if ($dnsTest) {
    Write-Host "DNS разрешение работает: $($dnsTest.IPAddress)"
} else {
    Write-Host "Ошибка DNS разрешения"
}
```

Проверка обратного DNS-запроса

```
$reverseTest = Resolve-DnsName "192.168.1.20" -ErrorAction SilentlyContinue
if ($reverseTest) {
    Write-Host "Обратное разрешение работает: $($reverseTest.NameHost)"
}
```

4.3. Документирование результатов

powershell

Экспорт конфигурации DHCP

```
Get-DhcpServerv4Scope | Export-Clixml "C:\DHCP_Configuration.xml"
```

Экспорт зон DNS

```
Get-DhcpServerv4Scope | Export-Clixml "C:\DNS_Zones.xml"
```

Создание отчета о состоянии

```
$report = @{  
    DHCP_Scopes = (Get-DhcpServerv4Scope).Count  
    DNS_Zones = (Get-DnsServerZone).Count  
    DHCP_Leases = (Get-DhcpServerv4Lease -ScopeId 192.168.1.0).Count  
    Test_Date = Get-Date  
}  
$report | ConvertTo-Json | Out-File "C:\Network_Services_Report.json"
```

### Критерии успешного выполнения

DHCP-сервер:

- Клиенты получают IP-адреса из заданного диапазона
- Резервированные адреса корректно назначаются
- Параметры (шлюз, DNS) правильно передаются клиентам

DNS-сервер:

- Прямое и обратное разрешение имен работает корректно
- Динамические обновления от DHCP обрабатываются
- Рекурсивные запросы к внешним доменам выполняются

Диагностика:

- Выявляются и устраняются типовые неисправности
- Журналы событий анализируются корректно
- Производительность служб соответствует норме

Все этапы должны быть задокументированы, а результаты проверены практическим тестированием.

## Задание 17: Настройка статической и динамической маршрутизации (OSPF)

Условия выполнения задания:

Требования к оборудованию и ПО:

3 маршрутизатора Cisco (или эмулятор GNS3/EVE-NG/Packet Tracer)

4 компьютера для тестирования

Консольный доступ к оборудованию

Базовые знания протокола OSPF и статической маршрутизации.

Исходная топология сети:

text

```
[PC1]--[R1]---[R2]---[R3]--[PC2]  
|   |   |   |   |  
[PC3] [PC4] [PC5] [PC6] [PC7]
```

Сети:

- R1: 192.168.1.0/24, 10.1.12.0/30

- R2: 10.1.12.0/30, 10.1.23.0/30, 192.168.2.0/24

- R3: 10.1.23.0/30, 192.168.3.0/24

Примерный алгоритм выполнения задания:

1: Базовая настройка сети и статической маршрутизации

1.1. Настройка интерфейсов маршрутизаторов

*Маршрутизатор R1*

enable

```
configure terminal
hostname R1
! Настройка интерфейсов
interface gigabitethernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface gigabitethernet0/1
ip address 10.1.12.1 255.255.255.252
no shutdown
exit
```

*Маршрутизатор R2*

```
enable
configure terminal
hostname R2
! Настройка интерфейсов
interface gigabitethernet0/0
ip address 10.1.12.2 255.255.255.252
no shutdown
exit
interface gigabitethernet0/1
ip address 10.1.23.1 255.255.255.252
no shutdown
exit
interface gigabitethernet0/2
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
```

*Маршрутизатор R3*

```
enable
configure terminal
hostname R3
! Настройка интерфейсов
interface gigabitethernet0/0
ip address 10.1.23.2 255.255.255.252
no shutdown
exit
interface gigabitethernet0/1
```

```
ip address 192.168.3.1 255.255.255.0
no shutdown
exit
```

## 1.2. Настройка статических маршрутов

*На R1 - маршруты к сетям за R2 и R3*

```
ip route 192.168.2.0 255.255.255.0 10.1.12.2
ip route 192.168.3.0 255.255.255.0 10.1.12.2
```

*На R2 - маршруты к сетям за R1 и R3*

```
ip route 192.168.1.0 255.255.255.0 10.1.12.1
ip route 192.168.3.0 255.255.255.0 10.1.23.2
```

*На R3 - маршруты к сетям за R1 и R2*

```
ip route 192.168.1.0 255.255.255.0 10.1.23.1
ip route 192.168.2.0 255.255.255.0 10.1.23.1
```

## 1.3. Проверка статической маршрутизации

*Проверка таблицы маршрутизации на R1*

```
show ip route
```

! Должны отображаться маршруты:

! S 192.168.2.0/24 [1/0] via 10.1.12.2

! S 192.168.3.0/24 [1/0] via 10.1.12.2

*Проверка связности*

```
ping 192.168.2.1 source 192.168.1.1
```

```
ping 192.168.3.1 source 192.168.1.1
```

*Проверка трассировки*

```
tracert 192.168.3.1
```

## 2: Настройка динамической маршрутизации OSPF

### 2.1. Базовая настройка OSPF на всех маршрутизаторах

*На R1 - настройка OSPF*

```
router ospf 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255 area 0
network 10.1.12.0 0.0.0.3 area 0
passive-interface gigabitethernet0/0
exit
```

*На R2 - настройка OSPF*

```
router ospf 1
router-id 2.2.2.2
network 10.1.12.0 0.0.0.3 area 0
network 10.1.23.0 0.0.0.3 area 0
```

```
network 192.168.2.0 0.0.0.255 area 0
passive-interface gigabitethernet0/2
exit
```

*На R3 - настройка OSPF*

```
router ospf 1
router-id 3.3.3.3
network 10.1.23.0 0.0.0.3 area 0
network 192.168.3.0 0.0.0.255 area 0
passive-interface gigabitethernet0/1
exit
```

## 2.2. Удаление статических маршрутов и проверка OSPF

*На всех маршрутизаторах удаляем статические маршруты*

```
no ip route 192.168.2.0 255.255.255.0 10.1.12.2
no ip route 192.168.3.0 255.255.255.0 10.1.12.2
```

*Проверка соседства OSPF*

```
show ip ospf neighbor
```

! Должны видеть:

! Neighbor ID	Pri	State	Dead Time	Address	Interface
! 2.2.2.2	1	FULL/DR	00:00:37	10.1.12.2	GigabitEthernet0/1

*Проверка таблицы маршрутизации*

```
show ip route ospf
```

! Должны отображаться маршруты OSPF:

```
! O 192.168.2.0/24 [110/20] via 10.1.12.2, 00:05:43, GigabitEthernet0/1
! O 192.168.3.0/24 [110/30] via 10.1.12.2, 00:05:43, GigabitEthernet0/1
```

## Пункт 3: Диагностика и мониторинг OSPF

### 3.1. Комплексная диагностика OSPF

Проверка общей информации OSPF

```
show ip ospf
```

! Проверяем:

! - Router ID

! - Количество областей

! - Время работы протокола

Детальная информация о соседях

```
show ip ospf neighbor detail
```

! Проверяем:

! - Состояние соседей (FULL, 2WAY, etc.)

! - Приоритет DR/BDR

! - Время до сброса соседа

Проверка базы данных OSPF

```
show ip ospf database
```

! Анализируем LSA:  
! - Router LSA (Type 1)  
! - Network LSA (Type 2)  
! - Summary LSA (Type 3)

### 3.2. Мониторинг и логирование OSPF

Включение логирования OSPF событий  
logging buffered 32000  
debug ip ospf events  
debug ip ospf adj  
! После диагностики отключаем debug:  
undebug all

Настройка SNMP для мониторинга OSPF  
snmp-server community public RO  
snmp-server enable traps ospf

Проверка статистики OSPF  
show ip ospf interface  
! Анализируем:  
! - Количество отправленных/полученных пакетов  
! - Ошибки  
! - Состояние интерфейсов

### 3.3. Тестирование отказоустойчивости и восстановления

Тестирование восстановления связи  
! 1. Отключаем интерфейс на R2  
interface gigabitethernet0/1  
! 2. Наблюдаем за изменением таблицы маршрутизации на R1  
show ip route ospf  
! 3. Включаем интерфейс обратно  
interface gigabitethernet0/1  
no shutdown  
! 4. Замеряем время восстановления

Проверка альтернативных маршрутов  
show ip ospf database router  
! Анализируем альтернативные пути

Тестирование нагрузки на каналы  
ping 192.168.3.1 source 192.168.1.1 size 1500 repeat 100  
! Мониторим загрузку каналов

### Пункт 4: Сравнение и документирование результатов

#### 4.1. Сравнение статической и динамической маршрутизации

Сбор статистики для сравнения  
show ip route summary  
show ip ospf traffic  
show ip protocol

Тестирование времени конвергенции  
! Для статической маршрутизации:



! - Время восстановления: ручная настройка  
! Для OSPF:  
! - Время восстановления: автоматическое  
4.2. Документирование конфигурации

Сохранение текущей конфигурации  
copy running-config startup-config  
show running-config

Экспорт важной информации  
show ip ospf neighbor > ospf\_neighbors.txt  
show ip route > routing\_table.txt  
show ip ospf interface > ospf\_interfaces.txt  
4.3. Финальное тестирование и отчет

Комплексное тестирование сети  
! С PC1 (192.168.1.10)  
ping 192.168.2.10  
ping 192.168.3.10  
tracert 192.168.3.10

Проверка балансировки нагрузки (если настроено)  
show ip ospf border-routers  
show ip ospf virtual-links

Финальная проверка стабильности  
show ip ospf | include uptime  
show logging | include OSPF  
Критерии успешного выполнения

#### **Статическая маршрутизация:**

Все сети доступны с любого маршрутизатора  
Таблицы маршрутизации содержат правильные статические маршруты  
Ping и tracert работают корректно  
Динамическая маршрутизация OSPF:  
Соседние отношения установлены (состояние FULL)  
Таблицы маршрутизации заполнены маршрутами OSPF  
Автоматическое восстановление при обрывах связей  
Оптимальные маршруты выбраны правильно

#### **Диагностика:**

Выявление и устранение проблем конфигурации  
Мониторинг состояния OSPF соседей  
Анализ базы данных OSPF  
Документация:  
Конфигурации сохранены и задокументированы  
Результаты тестирования записаны  
Сравнительный анализ выполнен  
Все этапы должны быть подтверждены практическими тестами связности и соответствующими командами проверки.

### **Задание 18: Настройка базовой безопасности сети (ACL, NAT)**

Условия выполнения задания:

- Маршрутизатор Cisco с IOS
- 2 сети: внутренняя (192.168.1.0/24) и внешняя (203.0.113.0/24)
- Интернет-шлюз: 203.0.113.1

Примерный алгоритм выполнения задания:

1.1: Настройка NAT для выхода в интернет

Настройка интерфейсов

```
interface gigabitethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
no shutdown
interface gigabitethernet0/1
ip address 203.0.113.2 255.255.255.0
ip nat outside
no shutdown
```

! Настройка NAT

```
ip access-list standard NAT_ACL
permit 192.168.1.0 0.0.0.255
ip nat inside source list NAT_ACL interface gigabitethernet0/1 overload
```

1.2: Создание ACL для фильтрации трафика\*\*

! Создание расширенного ACL

```
ip access-list extended INBOUND_FILTER
deny ip any 192.168.1.0 0.0.0.255
permit tcp any host 203.0.113.2 eq 80
permit tcp any host 203.0.113.2 eq 443
deny ip any any log
```

Применение ACL к интерфейсам

```
interface gigabitethernet0/1
ip access-group INBOUND_FILTER in
```

1.3: Настройка безопасности управляющего доступа\*\*

Ограничение доступа по SSH

```
ip access-list extended MGMT_ACL
permit tcp 192.168.1.0 0.0.0.255 any eq 22
deny tcp any any eq 22 log
line vty 0 4
access-class MGMT_ACL in
transport input ssh
login local
```

## **Задание 19: Развертывание и ввод в эксплуатацию защищенной АИС**

Условия выполнения задания:

- Сервер с ОС Windows Server 2022
- База данных PostgreSQL
- Веб-приложение ASP.NET

Примерный алгоритм выполнения задания:

2.1: Подготовка защищенной ОС\*\*

powershell

Отключение неиспользуемых служб

```
Get-Service | Where-Object {$_.Name -like "*Telnet*" -or $_.Name -like "*FTP*"} | Stop-Service -Force
```

```
Set-Service -Name "Telnet" -StartupType Disabled
```

Настройка брандмауэра

```
New-NetFirewallRule -DisplayName "Block Inbound SMB" -Direction Inbound -Protocol TCP -
LocalPort 445 -Action Block
```

Настройка политики паролей

```
secedit /export /cfg C:\sec_policy.cfg
```

В файле: MinimumPasswordAge = 1, MinimumPasswordLength = 8

```
secedit /configure /db C:\Windows\security\local.sdb /cfg C:\sec_policy.cfg
```

## 2.2: Установка и настройка АИС\*\*

-- Создание БД с ограничениями доступа

```
CREATE DATABASE AIS_DB;
```

```
CREATE USER ais_user WITH PASSWORD 'SecurePass123!';
```

```
GRANT CONNECT ON DATABASE AIS_DB TO ais_user;
```

Настройка SSL для PostgreSQL

```
ALTER SYSTEM SET ssl = on;
```

```
ALTER SYSTEM SET ssl_cert_file = 'C:\PostgreSQL\ssl\server.crt';
```

```
ALTER SYSTEM SET ssl_key_file = 'C:\PostgreSQL\ssl\server.key';
```

```
SELECT pg_reload_conf();
```

## 2.3: Настройка веб-сервера и приложения\*\*

xml

```
<!-- web.config - настройка безопасности -->
```

```
<system.web>
```

```
  <httpRuntime requestValidationMode="2.0" />
```

```
  <compilation debug="false" />
```

```
</system.web>
```

```
<system.webServer>
```

```
  <httpProtocol>
```

```
    <customHeaders>
```

```
      <add name="X-Content-Type-Options" value="nosniff" />
```

```
    </customHeaders>
```

```
  </httpProtocol>
```

```
</system.webServer>
```

## **Задание 20: Управление доступом в защищенной АИС на основе ролевой модели (RBAC)**

### Условия выполнения задания:

- АИС с веб-интерфейсом

- 3 группы пользователей: Администраторы, Редакторы, Читатели

### Примерный алгоритм выполнения задания:

#### 3.1: Проектирование ролевой матрицы

Создание ролей в БД

```
CREATE ROLE admin_role;
```

```
CREATE ROLE editor_role;
```

```
CREATE ROLE reader_role;
```

Назначение прав на таблицы

```
GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO
admin_role;
```

```
GRANT SELECT, INSERT, UPDATE ON documents TO editor_role;
```

```
GRANT SELECT ON documents TO reader_role;
```

#### 3.2: Реализация RBAC в приложении\*\*

csharp

Контроллер управления доступом

```
[Authorize(Roles = "Admin")]
```

```
public class AdminController : Controller
```

```

{
    public IActionResult ManageUsers()
    {
        return View();
    }
}

[Authorize(Roles = "Editor,Admin")]
public class DocumentController : Controller
{
    public IActionResult EditDocument(int id)
    {
        return View();
    }
}

```

### 3.3: Создание пользователей и тестирование прав\*\*

sql

Создание тестовых пользователей

```

CREATE USER user_admin WITH PASSWORD 'admin123';
CREATE USER user_editor WITH PASSWORD 'editor123';
CREATE USER user_reader WITH PASSWORD 'reader123';
GRANT admin_role TO user_admin;
GRANT editor_role TO user_editor;
GRANT reader_role TO user_reader;

```

## **Задание 21: Аудит и мониторинг безопасности АИС**

### Условия выполнения задания:

- Сервер с ОС Windows
- АИС с веб-интерфейсом
- SIEM система

### Примерный алгоритм выполнения задания:

#### 1.1: Настройка аудита в ОС

powershell

Включение аудита безопасности

```

auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
auditpol /set /category:"Object Access" /success:enable /failure:enable

```

Настройка аудита для файлов АИС

```

icacls "C:\AIS\Data\" /grant:r "SYSTEM:(OI)(CI)(F)" /inheritance:r
icacls "C:\AIS\Data\" /grant "Администраторы:(OI)(CI)(F)"
icacls "C:\AIS\Data\" /audit:r "Все:(OI)(CI)(W,DE,DC)"

```

#### 1.2: Настройка журналирования в АИС\*\*

csharp

// Конфигурация логирования

```

public void ConfigureLogging()
{
    var loggerFactory = LoggerFactory.Create(builder =>
    {
        builder.AddFile("Logs/ais-{Date}.txt",
            minimumLevel: LogLevel.Warning,
            fileSizeLimitBytes: 10485760);
    });
}

```

### 1.3: Мониторинг и оповещения\*\*

powershell

# Создание задачи для мониторинга аномалий

\$Trigger = New-ScheduledTaskTrigger -AtStartup

\$Action = New-ScheduledTaskAction -Execute "Powershell.exe" -Argument "C:\Scripts\SecurityMonitor.ps1"

Register-ScheduledTask -TaskName "SecurityMonitor" `
-Trigger \$Trigger -Action \$Action `
-RunLevel Highest -User "SYSTEM"

## **Задание 22: Резервное копирование и восстановление работоспособности АИС после сбоя**

Условия выполнения задания:

- АИС с БД PostgreSQL
- Файловое хранилище документов
- Сетевой ресурс для хранения бэкапов

Примерный алгоритм выполнения задания:

### 1.1: Настройка резервного копирования БД\*\*

bash

!/bin/bash

backup\_script.sh

DATE=\$(date +%Y%m%d\_%H%M%S)

PGPASSWORD="SecurePass123!" pg\_dump -U ais\_user -h localhost -d AIS\_DB > /backups/ais\_db\_\$DATE.sql

find /backups -name "ais\_db\_\*.sql" -mtime +7 -delete

### 1.2: Резервное копирование файлов\*\*

powershell

PowerShell скрипт для бэкапа файлов

\$Source = "C:\AIS\Data\"

\$Destination = "\\backup-server\ais-backups\"

\$Date = Get-Date -Format "yyyyMMdd"

Robocopy \$Source (\$Destination + \$Date) /MIR /Z /W:5 /R:3 /LOG+:C:\Logs\backup.log

### 1.3: Процедура восстановления\*\*

-- Восстановление БД из дампа

DROP DATABASE AIS\_DB;

CREATE DATABASE AIS\_DB;

\i /backups/ais\_db\_20241201\_120000.sql

Проверка целостности данных

SELECT COUNT(\*) FROM documents;

SELECT COUNT(\*) FROM users;

## **Задание 23: Обеспечение криптографической защиты информации в АИС**

Условия выполнения задания:

- Веб-приложение с HTTPS
- Шифрование данных в БД
- Защита конфиденциальных файлов

Примерный алгоритм выполнения задания:

### 1.1: Настройка HTTPS для веб-сервера

powershell

Создание самоподписанного сертификата

```
New-SelfSignedCertificate -DnsName "ais.company.local" `
  -CertStoreLocation "cert:\LocalMachine\My" `
  -KeyLength 2048 -KeyAlgorithm RSA `
  -HashAlgorithm SHA256
```

Привязка сертификата к сайту

```
New-WebBinding -Name "Default Web Site" -Protocol https -Port 443
```

```
$Cert = Get-ChildItem "Cert:\LocalMachine\My" | Where-Object {$_.Subject -like
"*ais.company.local*"}
```

```
New-Item -Path "IIS:\SslBindings\0.0.0.0!443" -Value $Cert
```

1.2: Шифрование данных в БД\*\*

sql

-- Создание расширения для шифрования

```
CREATE EXTENSION pgcrypto;
```

-- Функция для шифрования конфиденциальных данных

```
CREATE OR REPLACE FUNCTION encrypt_data(data TEXT, key TEXT)
RETURNS BYTEA AS $$
```

```
BEGIN
```

```
    RETURN pgp_sym_encrypt(data, key);
```

```
END;
```

```
$$ LANGUAGE plpgsql;
```

-- Функция для дешифрования

```
CREATE OR REPLACE FUNCTION decrypt_data(encrypted_data BYTEA, key TEXT)
RETURNS TEXT AS $$
```

```
BEGIN
```

```
    RETURN pgp_sym_decrypt(encrypted_data, key);
```

```
END;
```

```
$$ LANGUAGE plpgsql;
```

1.3: Шифрование файлового хранилища

powershell

Включение BitLocker для диска с данными

```
Enable-BitLocker -MountPoint "D:" -EncryptionMethod Aes256 `
  -RecoveryPasswordProtector -UsedSpaceOnly
```

Настройка EFS для отдельных папок

```
$Acl = Get-Acl "C:\AIS\Confidential\"
```

```
$Acl.SetAccessRuleProtection($true, $false)
```

```
Set-Acl "C:\AIS\Confidential\" $Acl
```

## **Задание 24: Плановое техническое обслуживание и мониторинг сетевой инфраструктуры**

Условия выполнения задания:

- Сеть с 3 коммутаторами, 2 маршрутизаторами
- Система мониторинга Zabbix
- Резервный канал связи

Примерный алгоритм выполнения задания:

1.1: Ежедневный мониторинг

bash

```
!/bin/bash
```

```
daily_check.sh
```

```
DEVICES=("192.168.1.1" "192.168.1.2" "192.168.1.10" "192.168.1.11")
```

```

for device in "${DEVICES[@]}"; do
    if ping -c 3 $device &> /dev/null; then
        echo "$(date): $device - OK" >> /var/log/network_status.log
    else
        echo "$(date): $device - FAILED" >> /var/log/network_status.log
        echo "Device $device is down" | mail -s "Network Alert" admin@company.local
    fi
done
1.2: Проверка конфигураций оборудования**
bash
# Сбор конфигураций с сетевых устройств
for device in "${DEVICES[@]}"; do
    scp admin@$device:running-config /backups/configs/$device-$(date +%Y%m%d).cfg
done
Проверка целостности конфигураций
md5sum /backups/configs/*.cfg > /backups/configs/checksums.txt
1.3: Анализ производительности**
bash
# Мониторинг загрузки каналов
snmpwalk -v2c -c public 192.168.1.1 1.3.6.1.2.1.2.2.1.10 > /logs/interface_traffic_$(date +%Y%m%d).log
# Анализ использования памяти на коммутаторах
snmpget -v2c -c public 192.168.1.1 1.3.6.1.4.1.9.9.48.1.1.1.6.1

```

## **Задание 25: Диагностика и устранение комплексного сетевого сбоя**

### Условия выполнения задания:

- Многосегментная сеть предприятия
- Пользователи сообщают о потере доступа к интернету и серверам

### Примерный алгоритм выполнения задания:

```

1.1: Локализация проблемы**
bash
Проверка доступности ключевых узлов
tracert 8.8.8.8
ping -c 5 192.168.1.1
ping -c 5 192.168.2.1
Проверка таблиц маршрутизации
ssh admin@192.168.1.1 "show ip route"
ssh admin@192.168.2.1 "show ip route"
Анализ ARP таблиц
arp -a
ssh admin@192.168.1.1 "show arp"
1.2: Диагностика на уровне 2**
bash
Проверка STP на коммутаторах
ssh admin@switch1 "show spanning-tree summary"
ssh admin@switch2 "show spanning-tree detail"
Поиск петель
ssh admin@switch1 "show interface counters errors"
ssh admin@switch2 "show mac address-table count"
1.3: Устранение неисправности**
bash

```

Сброс проблемных интерфейсов  
ssh admin@switch1 "interface gigabitethernet1/0/24"  
ssh admin@switch1 "shutdown"  
ssh admin@switch1 "no shutdown"  
Очистка MAC-таблиц при необходимости  
ssh admin@switch1 "clear mac address-table dynamic"  
Проверка восстановления  
ping -c 10 8.8.8.8  
traceroute 8.8.8.8

### **Задание 25: Модернизация сети: добавление новой подсети и настройка безопасности**

#### Условия выполнения задания:

- Существующая сеть 192.168.0.0/22
- Новая подсеть для гостевого Wi-Fi
- Требуется изоляция от корпоративной сети

#### Примерный алгоритм выполнения задания:

##### 1.1: Проектирование и планирование

bash

Расчет новой подсети

Существующая: 192.168.0.0/22 (192.168.0.1 - 192.168.3.254)

Новая гостевая: 192.168.4.0/24 (192.168.4.1 - 192.168.4.254)

##### 1.2: Настройка сетевого оборудования

bash

Создание VLAN для гостевой сети

configure terminal

vlan 100

name GUEST\_WIFI

exit

interface vlan 100

ip address 192.168.4.1 255.255.255.0

exit

Настройка DHCP для гостей

ip dhcp pool GUEST\_POOL

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 8.8.8.8 8.8.4.4

lease 0 8

##### 1.3: Настройка политик безопасности

bash

Создание ACL для изоляции гостевой сети

ip access-list extended GUEST\_ISOLATION

deny ip 192.168.4.0 0.0.0.255 192.168.0.0 0.0.3.255

deny ip 192.168.4.0 0.0.0.255 10.0.0.0 0.255.255.255

permit ip 192.168.4.0 0.0.0.255 any

Применение ACL

interface vlan 100

ip access-group GUEST\_ISOLATION in



## **ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ**

### **Задание 1: Подготовительный этап и планирование ревью**

#### Условия выполнения задания:

- Место проведения: Учебная лаборатория или виртуальный стенд (например, на базе VMware/VirtualBox).
- Допустимые средства: Разрешено использовать только лицензионное или свободно распространяемое ПО (Nmap, OpenVAS, Wireshark, специализированные дистрибутивы для тестирования безопасности, такие как Kali Linux).
- Объект тестирования: Изолированный сегмент сети, включающий виртуальные машины с преднамеренно настроенными уязвимостями (например, устаревшие версии ОС, незакрытые порты, слабые пароли).
- Безопасность: Все работы проводятся только на выделенном полигоне. Проведение аналогичных работ в реальной корпоративной сети без письменного разрешения запрещено.
- Результат: Подробный отчет установленного образца.

#### Примерный алгоритм выполнения задания:

##### **1. Подготовка и планирование**

- Изучить и согласовать с руководителем практики программу и методику испытаний.
- Развернуть виртуальный стенд или получить доступ к учебному полигону.
- Установить и настроить необходимое программное обеспечение для тестирования.
- Определить IP-адреса целевых систем и границы тестирования.

##### **2. Активное сканирование и сбор данных**

- Провести сканирование сети (Nmap) для обнаружения активных хостов, открытых портов и служб.
- Выполнить сканирование уязвимостей (OpenVAS) для выявления известных проблем безопасности на обнаруженных службах.
- Проанализировать полученные отчеты от сканеров, идентифицировать и классифицировать уязвимости по степени критичности (высокая, средняя, низкая).

##### **3. Анализ конфигураций и политик**

- Проверить (на основе данных сканирования) соблюдение парольной политики (если есть доступ к хэшам паролей).
- Проанализировать конфигурации сетевых экранов (межсетевых экранов) на тестовых машинах (например, с помощью iptables -L в Linux или Get-NetFirewallRule в PowerShell Windows).
- Исследовать сетевой трафик (Wireshark) на предмет передачи данных в открытом виде.

##### **4. Формирование отчета и рекомендаций**

- Систематизировать все обнаруженные уязвимости в сводную таблицу.
- Для каждой уязвимости предложить конкретные меры по ее устранению (например, установить обновление, закрыть порт, изменить политику).
- Оформить отчет, включающий введение, описание методик, результаты, выводы и рекомендации.

### **Задание 2: Исследование и настройка средств криптографической защиты информации (СКЗИ)**

#### Условия выполнения задания:

- Программное обеспечение: Использовать российские СКЗИ, допущенные к использованию ФСБ России (например, КриптоПро CSP, ViPNet CSP).
- Лицензии: Работать с пробными или учебными лицензиями.
- Инфраструктура: Самостоятельно развернуть тестовую инфраструктуру открытых ключей (PKI) или использовать предоставленную.

- Объекты защиты: Тестовые файлы (документы, архивные файлы) и виртуальные каналы связи.
- Результат: Настроенная среда и регламент по использованию СКЗИ.

Примерный алгоритм выполнения задания:

### **1. Изучение нормативной базы и установка ПО**

Изучить основы работы с электронной подписью и шифрованием по российским стандартам (ГОСТ).

Установить и настроить криптопровайдер (КриптоПро CSP).

Установить корневой сертификат Удостоверяющего Центра (УЦ) и сертификат сервера.

### **2. Работа с ключевой информацией и сертификатами**

Сгенерировать ключевую пару (закрытый и открытый ключ) и создать запрос на сертификат.

Обратиться к тестовому УЦ для выпуска сертификата (или выпустить самоподписанный сертификат для учебных целей).

Установить полученный сертификат в личное хранилище.

### **3. Практическое применение СКЗИ**

Подписать тестовый электронный документ с помощью усиленной квалифицированной электронной подписи (УКЭП). Проверить созданную подпись.

Зашифровать файл для условного получателя, используя его открытый ключ.

Расшифровать файл, используя свой закрытый ключ.

Создать и настроить зашифрованное соединение (например, с использованием VipNet Client) между двумя виртуальными машинами.

### **4. Документирование результатов**

Составить пошаговую инструкцию для пользователя: "Как установить сертификат", "Как подписать документ", "Как зашифровать файл".

Оформить отчет, описывающий проделанную работу, и предложить фрагмент регламента по использованию СКЗИ в организации.

.

## **Задание 3: Аудит системы защиты от вредоносного программного обеспечения**

Условия выполнения задания:

- Объект аудита: Парк виртуальных машин, имитирующих рабочие станции и серверы организации.
- Имитация угрозы: Использование тестовых (неопасных) файлов-индикаторов (например, файлов EICAR) и образцов вредоносных программ в изолированной среде.
- Средства защиты: Централизованная система управления антивирусной защитой (например, Kaspersky Security Center, Dr.Web Security Space).
- Критерий успеха: Своевременное обнаружение и нейтрализация тестовых угроз, соответствие настроек политикам безопасности.
- Результат: Отчет о аудите с оценкой эффективности системы..

Примерный алгоритм выполнения задания:

### **1. Анализ архитектуры и политик системы защиты**

Изучить консоль управления антивирусной защитой. Определить, какие компьютеры входят в группу, и проверить их актуальный статус (защита включена, базы актуальны).

Проанализировать настройки политик защиты: режимы сканирования (по требованию, по расписанию, в реальном времени), настройки проактивной защиты (HIPS, контроль поведения).

Проверить актуальность антивирусных баз и версий программного обеспечения на клиентских станциях.

### **2. Моделирование угроз и тестирование реакции системы**

Разместить тестовые файлы EICAR на виртуальных машинах для проверки срабатывания сканирования в реальном времени и по требованию.

Имитировать атаку с использованием USB-накопителя с тестовым вредоносным кодом для проверки работы устройства контроля.

Проанализировать отчеты на сервере управления: зафиксированы ли события, каковы были действия системы (лечение, удаление, карантин).

### **3. Проверка резервных механизмов защиты**

Проверить наличие и настройки дополнительных средств защиты (например, AppLocker в Windows для ограничения запуска нежелательных приложений).

Оценить систему резервного копирования (если она доступна на стенде) как последний рубеж защиты от ransomware (шифровальщиков).

### **4. Разработка предложений по повышению эффективности**

Выявить недостатки в текущей конфигурации (например, не все компьютеры защищены, устаревшие базы, неоптимальные настройки).

Предложить конкретные меры: настройка более строгих политик, изменение расписания сканирований, внедрение дополнительных средств защиты.

Оформить отчет, включающий описание текущего состояния, результаты тестирования и план мероприятий по повышению уровня защищенности.

## **Задание 4: Аудит системы контроля и управления доступом (СКУД) на объекте информатизации**

### Условия выполнения задания:

- Объект работы: Учебный полигон, имитирующий защищаемый объект (например, здание университета с серверной комнатой), либо реальный объект с разрешения и под надзором ответственного сотрудника.
- Доступ: Наличие разрешающего документа (допуска) для проведения обследования. Все работы согласовываются со службой безопасности объекта.
- Документация: Возможность изучения проектной и эксплуатационной документации на СКУД (технические паспорта, схемы, регламенты).
- Результат: Отчет установленного образца с перечнем замечаний и рекомендаций.

### Примерный алгоритм выполнения задания:

#### **1. Подготовительный этап и изучение документации**

Получить и изучить технический паспорт системы, схемы подключения, инструкции по эксплуатации СКУД.

Изучить регламенты обслуживания системы и журналы учета работ.

Составить и согласовать с руководителем программу и методику аудита.

Ознакомиться с планировкой объекта и зонированием (периметр, зоны ограниченного доступа).

#### **2. Визуальное обследование и проверка аппаратной части**

Обследовать физическое состояние и правильность установки всех элементов СКУД: считывателей, контроллеров, исполнительных устройств (турникеты, электромеханические замки), пультов управления.

Проверить надежность крепления, целостность корпусов, наличие пломб.

Составить актуальную схему размещения точек доступа.

Проверить работоспособность системы резервного питания (при наличии доступа).

#### **3. Анализ программного обеспечения и баз данных**

Изучить базу данных системы (списки пользователей, права доступа, историю проходов).

Проверить актуальность списков, своевременность отключения пропусков у уволенных сотрудников.

Проанализировать соответствие прав доступа сотрудников их должностным инструкциям и принципу минимальных привилегий.

Провести выборочную проверку реакции системы на события "КЗ" (принудительное открытие), "Недопуск" и др.

#### **4. Формирование отчета**

Систематизировать все выявленные недостатки (физический износ, неактуальные права доступа, "слепые" зоны).

Разработать конкретные рекомендации по устранению каждого замечания.

Оформить отчет, включающий введение, описание методики, результаты обследования, выводы и рекомендации.

#### **Задание 5: Обследование и оценка эффективности системы охранной сигнализации и видеонаблюдения**

Условия выполнения задания:

- Объект работы: Учебный полигон или реальный объект (с разрешения). Критически важные зоны (серверная, архив).
- Безопасность: Работы по тестированию датчиков проводятся только в присутствии и с разрешения сотрудника службы безопасности для предотвращения ложных срабатываний.
- Оборудование: Наличие тестового оборудования для проверки линий связи (при возможности).
- Результат: Карта зон контроля и отчет с оценкой соответствия системы современным требованиям.

Примерный алгоритм выполнения задания:

##### **1. Анализ проектной документации и зонирования**

Изучить проект системы охранной сигнализации (ОС) и видеонаблюдения (CCTV).

Определить зоны ответственности каждого датчика и камеры.

Составить список всего установленного оборудования с указанием моделей и местоположения.

##### **2. Обследование аппаратных средств**

**Для ОС:** Проверить физическое состояние и правильность установки датчиков (объемных, акустических, магнитоcontactных). Выявить наличие "мертвых" (слепых) зон.

**Для видеонаблюдения:** Обследовать углы обзора камер, отсутствие помех обзору, качество изображения днем/ночью. Проверить фиксацию и сохранение записей.

Проверить исправность и время работы системы резервного питания.

##### **3. Функциональное тестирование систем**

Провести (со службой безопасности) контрольное тестирование датчиков ОС на срабатывание.

Проверить скорость и надежность передачи тревожного извещения на пульт охраны.

Протестировать работу детектора движения и качество записи в ночное время для камер.

Проверить синхронизацию систем: например, срабатывает ли запись по детектору движения и поворачивается ли PTZ-камера в зону сработки датчика ОС.

##### **4. Анализ и разработка предложений**

Составить карту-схему с указанием зон контроля и выявленных недостатков.

Оценить соответствие разрешения камер задачам идентификации/детекции.

Подготовить предложения по оптимизации системы: изменение углов обзора, установка дополнительных датчиков/камер, замена устаревшего оборудования.

Оформить отчет с выводами и рекомендациями.

#### **Задание 6: Разработка проекта модернизации инженерных укреплений и контроля периметра**

Условия выполнения задания:

- Объект работы: Условный объект информатизации (например, учебный корпус с серверной комнатой). Работа выполняется на основе плана БТИ или поэтажного плана.

– Исходные данные: План объекта, технические каталоги средств физической защиты, нормативные документы (например, СП 118.13330).

– Формат результата: Пояснительная записка и комплект чертежей/схем.

Примерный алгоритм выполнения задания:

#### **Шаг 1. Обследование и анализ уязвимостей объекта**

Изучить планировку объекта, выделить критические зоны (серверные, архивы, комнаты с коммутацией).

Провести визуальное обследование (или анализ плана) строительных конструкций: материал и толщина стен, конструкция дверей и окон, наличие решеток.

Выявить слабые места для возможного проникновения (окна первого этажа, вентиляционные шахты, слабые двери).

#### **Шаг 2. Анализ существующих инженерных средств защиты**

Оценить прочность и надежность существующих дверей, замков, оконных решеток.

Оценить организацию контроля периметра (забор, освещение, возможность скрытого подхода).

Определить, соответствуют ли существующие средства современным требованиям и тактике нарушителей.

#### **Шаг 3. Разработка предложений по модернизации**

**Для помещений:** Предложить замену обычных дверей на усиленные противопожарные/противоударные, установку сейфовых комнат, укрепление дверных коробок.

**Для окон:** Предложить установку антивандальных стекол, защитных пленок, роллет или усиление решеток.

**Для периметра:** Разработать предложения по организации зоны технических средств охраны (например, установку рубежа охранной сигнализации по периметру забора, улучшение освещения).

#### **Шаг 4. Формирование проектной документации**

Составить план-схему объекта с нанесением всех предлагаемых к установке или модернизации средств защиты.

Подготовить спецификацию на оборудование и материалы.

Написать пояснительную записку, содержащую обоснование выбранных решений, описание предлагаемых систем и ожидаемый эффект от модернизации.

Представить результаты руководителю практики в виде защитного слова.

## **ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ**

### **Задание 1. Работа с файловой системой и данными**

Условия выполнения задания:

Прием и регистрация входящих электронных документов и данных от сотрудников или из внешних источников.

Систематизация, копирование, перемещение и переименование файлов и папок в соответствии с установленным в организации регламентом.

Запись данных на различные типы носителей информации (USB-флеш-накопители, внешние жесткие диски, оптические диски) и их подготовка к передаче.

Примерный алгоритм выполнения задания:

#### **Этап 1: Прием и первичная обработка**

1. **Ежедневная проверка каналов поступления.** В начале рабочего дня осуществите проверку всех входящих каналов: корпоративная электронная почта, сетевые папки, файлообменники, чаты (например, Telegram, корпоративный мессенджер) на наличие новых поступлений.

2. **Фиксация поступления.** Для каждого поступившего файла или пакета файлов зафиксируйте дату и время его получения, а также источник (например, e-mail от Иванова И.И., файл в сетевой папке "Входящие\_Отдел\_Сбыта").
3. **Входной контроль целостности и безопасности.** Проверьте файлы с помощью антивирусного программного обеспечения. Убедитесь, что архивные файлы не повреждены (не выводятся ошибки при попытке их открыть).
4. **Ведение журнала поступления (регистрация).** Внесите запись в электронный журнал регистрации (например, таблица Excel или Google Sheets). Присвойте входящему документу уникальный регистрационный номер, укажите его краткое название, источник, дату поступления и присвоенный номер.
5. **Создание папки для входящего задания.** Создайте на рабочем или сетевом диске в папке «Входящие» отдельную папку с именем, соответствующим регистрационному номеру (например, «BX-051124-001»).

#### **Этап 2: Систематизация и обработка**

6. **Копирование файлов в рабочую папку.** Скопируйте все полученные файлы в созданную папку с регистрационным номером. **Важно:** работайте всегда с копиями, оставляя оригиналы входящих данных неизменными.
7. **Анализ содержимого и переименование.** Откройте и ознакомьтесь с содержимым файлов. Приведите их названия в соответствие с регламентом организации. Стандартный формат: «[Рег. номер]/[Краткое название]/[Дата документа].расширение» (например, «BX-051124-001\_Акт\_выполненных\_работ\_10.11.2024.pdf»).
8. **Сортировка по типам заданий.** Проанализируйте содержание документов и определите их тематику или тип (например, «Договоры», «Акты», «Внутренние отчеты», «Коммерческие предложения»).
9. **Создание структуры подпапок.** Внутри папки с регистрационным номером создайте подпапки для упорядочивания, например, «Исходные\_документы», «Обработанные\_файлы», «Для\_архива».
10. **Перемещение файлов по папкам.** Разместите переименованные файлы по созданным подпапкам в соответствии с их текущим статусом и назначением.

#### **Этап 3: Подготовка к передаче и архивация**

11. **Определение необходимости записи на носитель.** На основании внутренних инструкций или указаний руководителя определите, для каких документов требуется создание физических копий на внешних носителях.
12. **Подготовка носителя.** Возьмите чистый USB-накопитель (или иной носитель). Проверьте его на наличие вирусов и достаточный объем свободного места. При необходимости отформатируйте его (убедившись, что на нем нет нужной информации).
13. **Создание целевой папки на носителе.** На носителе создайте папку с понятным названием, например, «Документы\_для\_бухгалтерии\_10.11.2024».
14. **Копирование и верификация.** Скопируйте необходимые файлы из рабочей папки на компьютере в целевую папку на носителе. После завершения копирования убедитесь, что файлы скопированы корректно, открыв один-два из них прямо с носителя.
15. **Физическая маркировка и передача.** Подпишите носитель (если это возможно), указав регистрационный номер, дату и содержимое. Передайте носитель ответственному лицу или в соответствующий отдел под подпись в журнале передачи, либо составьте сопроводительную записку. Исходную рабочую папку на сетевом диске переместите в архив.

### **Задание 2 Ввод и обработка цифровой и текстовой информации**

Условия выполнения задания:

Ввод текстовой информации с соблюдением правил орфографии и пунктуации, а также требований к оформлению (шрифты, межстрочные интервалы, выравнивание).

Обработка цифровых данных: составление, форматирование и проведение простых вычислений в таблицах с использованием базовых формул и функций (сумма, среднее значение, сортировка, фильтрация).

Проверка и устранение ошибок ввода в текстовых и табличных документах.

Примерный алгоритм выполнения задания:

#### **Этап 1: Подготовка и первичный ввод**

1. **Подготовка рабочего места и ПО.** Откройте необходимую программу (текстовый редактор, например, MS Word, или табличный процессор, например, MS Excel). Убедитесь, что выбран чистый документ или нужный лист книги.
2. **Изучение технического задания (ТЗ) и требований к оформлению.** Внимательно прочтите исходный документ (если он есть в виде изображения или рукописи) и внутренний регламент. Зафиксируйте требования к шрифту (тип, размер), межстрочному интервалу, полям, выравниванию и другим параметрам форматирования.
3. **Предварительная настройка документа.** Задайте в документе все необходимые параметры форматирования *до начала ввода* (например, установите шрифт Times New Roman, размер 14, интервал 1.5). Это сэкономит время на последующее редактирование.
4. **Ввод текстовой информации.** Осуществите перенос текста из источника в электронный документ, сосредоточившись на точности и соблюдении орфографии. Для таблиц — заполните все ячейки исходными данными.
5. **Сохранение файла.** Впервые сохраните файл под понятным названием, отражающим его суть и дату (например, «Отчет\_о\_продажах\_ноябрь\_черновик»). Регулярно сохраняйтесь в процессе работы (сочетание клавиш Ctrl+S).

#### **Этап 2: Форматирование и обработка данных**

6. **Применение структурного форматирования.** Разметьте документ: расставьте заголовки разного уровня, применив к ним соответствующие стили («Заголовок 1», «Заголовок 2»). Настройте нумерацию списков (маркированных и нумерованных).
7. **Детальное форматирование текста.** Выводите текст по ширине (или как того требует ТЗ), установите абзацные отступы, проверьте межстрочные интервалы и расставьте переносы слов (если необходимо).
8. **Обработка табличных данных (для Excel).** Выделите диапазон ячеек с числами и примените к ним необходимое форматирование: «Числовой», «Денежный», «Дата» и т.д. Это обеспечит корректность последующих вычислений.
9. **Применение формул и функций.** Проведите необходимые вычисления. Используйте функцию СУММ() для итогов, СРЗНАЧ() для средних значений, простые арифметические формулы (сложение, вычитание, деление) для других расчетов.
10. **Сортировка и фильтрация данных.** Выделите диапазон данных (включая заголовки столбцов) и примените сортировку по нужному столбцу (например, по дате или по убыванию суммы). Используйте инструмент «Фильтр» для отображения только тех строк, которые соответствуют определенным критериям (например, продажи конкретного менеджера).

#### **Этап 3: Контроль качества и финализация**

11. **Проверка орфографии и пунктуации.** Запустите встроенную проверку правописания (F7 в Word). Внимательно просмотрите все подчеркнутые ошибки и исправьте их. Помните, что автоматическая проверка не идеальна, поэтому проведите визуальную вычитку текста.
12. **Верификация данных и формул.** В табличном документе проверьте несколько ключевых формул, убедившись, что они ссылаются на правильные ячейки.

Сравните итоговые цифры с исходными данными, если это возможно (например, «пересчитав» сумму на калькуляторе для выборочной проверки).

13. **Сравнение с исходником и ТЗ.** Проведите итоговое сравнение готового электронного документа с исходным материалом и техническим заданием. Убедитесь, что все данные перенесены верно, а оформление полностью соответствует требованиям.
14. **Сохранение финальной версии.** Сохраните итоговый вариант документа под новым, чистым именем, убрав из названия слово «черновик» (например, «Отчет\_о\_продажах\_ноябрь\_финал»). Для Excel это может быть также сохранение в формате PDF для защиты от случайных изменений.
15. **Передача результата и архивация.** Отправьте готовый файл ответственному лицу (руководителю, сотруднику) через установленный канал связи (электронная почта, сетевой диск) и переместите рабочие черновики в архивную папку.

### **Задание 3. Работа с периферийным оборудованием и оргтехникой**

#### Условия выполнения задания:

Подключение, настройка и проверка работоспособности периферийных устройств (монитор, клавиатура, мышь, принтер, сканер).

Выполнение операций по сканированию документов с последующим сохранением в заданном формате и разрешении.

Печать документов, настройка параметров печати (ориентация, качество, количество копий), оперативное устранение мелких неисправностей (замятие бумаги, замена картриджа с тонером/чернил).

#### Примерный алгоритм выполнения задания:

##### **Этап 1: Подключение и настройка оборудования**

1. **Подготовка и безопасность.** Отключите питание системного блока и всех подключаемых устройств. Осмотрите кабели и разъемы на предмет видимых повреждений.

2. **Физическое подключение.** Подсоедините кабели периферийных устройств (монитор, клавиатура, мышь) к соответствующим портам системного блока (USB, HDMI/VGA). Принтер/сканер подключите к сети и компьютеру, убедитесь в подаче питания.

3. **Установка драйверов.** Включите компьютер и все устройства. При первом подключении операционная система попытается автоматически найти и установить драйверы. Если этого не произошло, установите их вручную с предоставленного установочного диска или официального сайта производителя.

4. **Проверка работоспособности в ОС.** Убедитесь, что устройства распознаны системой. Проверьте мышь и клавиатуру, введя текст и переместив курсор. Проверьте монитор, убедившись в корректном разрешении и отсутствии артефактов.

5. **Проверка функций принтера/сканера.** Запустите пробную печать страницы (функция «Настройка печати» -> «Печать пробной страницы»). Для сканера запустите программу сканирования и выполните предварительный просмотр.

##### **Этап 2: Сканирование документов**

7. **Подготовка документа к сканированию.** Уберите со документа скрепки, стикеры и посторонние предметы. Очистите стекло сканера от пыли и отпечатков. Правильно разместите документ лицевой стороной вниз по ориентиру (меткам на стекле).

8. **Выбор параметров сканирования.** В программном обеспечении сканера или через меню «Устройства и принтеры» задайте требуемые параметры:

9. **Тип документа:** Черно-белый, Оттенки серого, Цветной.

10. **Разрешение (DPI):** 150-300 dpi для текста, 300-600 dpi для изображений (согласно регламенту).

11. **Формат файла:** PDF (для документов), JPEG (для фото).



12. **Предварительный просмотр и коррекция.** Выполните предварительный просмотр. Обрежьте ненужные поля, если это требуется, и убедитесь в качестве изображения (резкость, отсутствие затемнений).

13. **Запуск сканирования и сохранение.** Нажмите кнопку «Сканировать». Укажите путь для сохранения файла, дайте ему понятное имя в соответствии с правилами документооборота организации.

14. **Этап 3: Печать документов и устранение неисправностей**

15. **Подготовка к печати.** Убедитесь, что принтер включен, в лотке достаточно бумаги нужного формата (А4, А5), а уровни тонера/чернил удовлетворительны.

16. **Настройка параметров печати.** В диалоговом окне «Печать» выберите целевой принтер, укажите:

17. **Диапазон страниц** (все, текущая, номера).

18. **Количество копий.**

19. **Ориентация:** Книжная или Альбомная.

20. **Качество печати:** Черновое (Draft) или Высокое (High).

21. **Запуск задания на печать и контроль.** Нажмите «Печать». Проследите за выходом первой страницы, чтобы убедиться в отсутствии дефектов (полос, пятен, блеклого текста). При печати многостраничного документа проверьте порядок страниц.

22. **Устранение замятия бумаги.** При сигнале об ошибке отключите принтер от сети. Откройте соответствующие крышки согласно инструкции. Аккуратно, без рывков, извлеките смятые листы бумаги по направлению вращения валов. Убедитесь, что в механизме не осталось обрывков.

23. **Замена картриджа.** При появлении сообщения о низком уровне тонера/чернил или значительном ухудшении качества печати:

24. Откройте крышку доступа к картриджам.

25. Извлеките старый картридж, взявшись за него за специальные ручки.

26. Извлеките новый картридж из упаковки, удалите защитную ленту.

27. Вставьте новый картридж на место до щелчка.

28. **Финализация и отчетность.** После завершения печати убедитесь, что все страницы напечатаны корректно. Соберите документы в соответствии с заданием. При замене картриджа или устранении серьезной неисправности сделайте запись в журнале учета технического состояния оборудования.

#### **Задание 4. Обеспечение функционирования программного обеспечения**

##### Условия выполнения задания:

Установка, обновление и удаление стандартного прикладного программного обеспечения (офисные пакеты, архиваторы, средства просмотра) под руководством системного администратора.

Ежедневная проверка компьютеров на вирусы с помощью антивирусного программного обеспечения, инициирование сканирования и лечение/помещение в карантин обнаруженных угроз.

Создание резервных копий пользовательских данных и системных настроек с использованием штатных средств ОС и специализированного ПО.

##### Примерный алгоритм выполнения задания:

#### **Этап 1: Установка, обновление и удаление ПО**

1. **Получение задания и согласование.** Получите от руководителя или системного администратора четкий перечень программ для установки, обновления или удаления. **Важно:** Не производите никаких действий с ПО без санкции администратора.

2. **Проверка системных требований.** Убедитесь, что компьютер пользователя соответствует системным требованиям программного обеспечения (версия ОС, объем оперативной памяти, свободное место на диске).

3. **Подготовка установочных файлов.** Скачайте дистрибутивы программ с официальных сайтов производителей или скопируйте их с утвержденного сетевого ресурса компании. Проверьте файлы с помощью антивируса.

4. **Создание точки восстановления системы.** Перед установкой/удалением ПО создайте точку восстановления Windows (Панель управления -> Восстановление -> Создание точки восстановления). Это позволит откатить систему в случае возникновения конфликтов.

5. **Выполнение установки/обновления.** Запустите установщик от имени администратора. Следуйте шагам мастера установки, выбирая настроенные администратором параметры (путь установки, отсутствие дополнительного ПО). Для обновления используйте функцию «Проверить наличие обновлений» внутри самой программы.

6. **Удаление программ.** Для корректного удаления используйте раздел «Программы и компоненты» в Панели управления или «Параметры» -> «Приложения» в Windows. Не удаляйте программы путем стирания их папок.

7. **Верификация результата.** После установки, обновления или удаления перезагрузите компьютер и убедитесь, что программа запускается и работает стабильно, а ненужное ПО полностью удалено.

#### 8. **Этап 2: Антивирусная защита**

9. **Ежедневная проверка статуса антивируса.** В начале рабочего дня визуально проверьте значок антивирусной программы в системном трее. Убедитесь, что защита активна (нет красных или желтых значков), и базы сигнатур актуальны.

10. **Инициирование быстрого сканирования.** Запустите быстрое (экспресс) сканирование критических областей системы (загрузочные сектора, память, системные папки). Эта операция обычно занимает 15-20 минут.

11. **Анализ отчета и реагирование на угрозы.** После завершения сканирования откройте отчет антивируса. Если обнаружены угрозы, действуйте в соответствии с политикой безопасности компании: как правило, для известных вирусов применяйте лечение/удаление, для подозрительных или новых объектов — помещайте в карантин.

12. **Запуск полного сканирования.** По графику (например, раз в неделю) или по указанию администратора запустите полное сканирование всех дисков. Запланируйте его на время, когда компьютер не будет активно использоваться.

#### 13. **Этап 3: Резервное копирование**

14. **Подготовка к резервированию.** Определите, какие пользовательские данные подлежат копированию (папки «Документы», «Рабочий стол», «Изображения», ключи настроек специфичных программ). Подключите внешний жесткий диск или убедитесь в доступности сетевой папки для резервных копий.

#### 15. **Настройка и запуск копирования.**

16. **Через штатные средства:** Используйте «Историю файлов» в Windows или «Мастер архивации» для создания копии данных.

17. **Через специализированное ПО:** Запустите программу для бэкапа (например, Acronis True Image, Veeam Agent), выберите источник (файлы и папки) и цель (внешний носитель), запустите задание.

18. **Проверка целостности резервной копии.** После завершения процесса убедитесь, что архив создан, откройте его и проверьте наличие ключевых файлов, убедившись, что копия не повреждена.

19. **Документирование и отчет.** Сделайте запись в журнале резервного копирования: дата, время, объем данных, использованный носитель, результат проверки. Сообщите системному администратору о завершении плановых работ.

## **Задание 5 Поддержка коммуникаций и документооборота**

### Условия выполнения задания:

Работа с электронной почтой: прием, отправка, сортировка входящей и исходящей корреспонденции, работа с вложениями, ведение адресной книги.

Участие в подготовке и оформлении электронных документов (приказов, служебных записок, отчетов) в соответствии с действующими в организации стандартами делопроизводства.

Использование средств оперативного обмена сообщениями (корпоративные мессенджеры) для служебных коммуникаций.

### Примерный алгоритм выполнения задания:

#### **Этап 1: Работа с электронной почтой**

1. **Ежедневная первичная проверка почты.** В начале рабочего дня откройте клиент электронной почты (например, Outlook) или веб-интерфейс. Проверьте папку «Входящие» и «Отправленные» на наличие новых сообщений.

2. **Сортировка входящей корреспонденции.** Быстро отсортируйте письма по приоритету:

3. **Срочные/Важные:** От руководства, ключевых клиентов, с пометкой «Важно».

4. **Обычные:** Информационные рассылки, внутренние уведомления.

5. **Спам:** Рекламные и нерелевантные письма (переместите в папку «Спам»).

6. **Обработка вложений.** Откройте вложения из проверенных источников. Сохраните их в заранее подготовленную папку «Входящие\_документы» на рабочем столе или сетевом диске, присвоив понятные имена.

7. **Ведение адресной книги.** При получении писем от новых корреспондентов добавляйте их контакты в корпоративную адресную книгу, указав ФИО, должность, компанию и примечание (например, «Поставщик, отдел закупок»).

8. **Подготовка к отправке исходящей почты.** Перед созданием нового письма подготовьте все необходимые файлы-вложения, убедившись в их корректности и окончательных версиях.

9. **Форматирование и отправка письма.** Заполните поля:

10. **«Кому»:** Основные адресаты.

11. **«Копия»:** Лица, которых ставят в известность.

12. **Тема:** Четко и кратко отражающая суть письма.

13. **Текст письма:** Составьте лаконичный и структурированный текст с корректным обращением и подписью (должность, ФИО, контакты).

14. **Сортировка исходящей корреспонденции.** Отправленные письма переместите в тематические папки (например, «Отправленные\_Отчеты», «Отправленные\_Договоры»).

#### **Этап 2: Подготовка и оформление электронных документов**

16. **Получение задачи и шаблона.** Получите от руководителя задачу на создание документа (приказ, служебная записка, отчет) и запросите утвержденный шаблон или инструкцию по оформлению.

17. **Сбор и ввод информации.** Соберите необходимые данные для заполнения документа (цифры, факты, списки). Внесите информацию в шаблон, соблюдая структуру.

18. **Применение стандартов оформления.** Установите предписанные параметры форматирования: шрифт (например, Times New Roman, 14), межстрочный интервал (1.5), выравнивание (по ширине), поля документа.

19. **Проверка и согласование черновика.** Проверьте документ на орфографические ошибки (F7) и фактологическую точность. Отправьте черновик на согласование инициатору задачи или руководителю по электронной почте.

20. **Финальное сохранение и регистрация.** Внесите полученные правки. Сохраните финальную версию документа в установленную сетевую папку с именем по

регламенту (например, «Служебная\_записка\_О\_закупке\_канцтоваров\_от\_15112024»). При необходимости внесите запись в электронный журнал документов.

**21. Этап 3: Работа в корпоративных мессенджерах**

**22. Настройка статуса и проверка активности.** После включения компьютера запустите корпоративный мессенджер (Teams, Telegram, Viber). Установите статус «Доступен» или «Активен». Проверьте непрочитанные сообщения в общих чатах и личных беседах.

**23. Корректное ведение коммуникации.** Отвечайте на сообщения своевременно. Используйте четкие и лаконичные формулировки. Для сложных вопросов, требующих обсуждения, предлагайте перейти к общению по телефону или электронной почте.

**24. Работа с уведомлениями и файлами.** Настройте уведомления для важных чатов, отключив их для второстепенных. Полученные через мессенджер файлы сохраняйте в предназначенные папки на рабочем диске, а не работайте с ними прямо из чата. Перед завершением рабочего дня убедитесь, что на все срочные сообщения получены ответы.

### **Задание 6. Техническое обслуживание рабочих мест**

Условия выполнения задания:

Проведение визуального контроля и внешнего профилактического обслуживания аппаратной части рабочих станций (очистка от пыли, проверка кабельных соединений).

Подготовка компьютеров к началу рабочего дня (включение, проверка работоспособности ОС и критичного ПО) и корректное завершение работы в конце дня.

Ведение журналов учета технического состояния оборудования и отчетности о выполненных операциях.

Примерный алгоритм выполнения задания:

**Этап 1: Ежедневное обслуживание (начало рабочего дня)**

**1. Визуальный осмотр перед включением.** Осмотрите системный блок, монитор, клавиатуру, мышь и периферийные устройства на предмет видимых повреждений, следов жидкости или посторонних предметов.

**2. Включение оборудования и диагностика.** Включите питание системного блока и монитора. В процессе загрузки обратите внимание на любые нестандартные звуки (щелчки, гудение) и сообщения на экране (ошибки BIOS/Hardware).

**3. Проверка входа в операционную систему.** Убедитесь, что ОС загружается без сбоев, пользователь может успешно авторизоваться.

**4. Проверка работоспособности критичного ПО.** Запустите основные приложения, необходимые для работы (офисный пакет, 1С, корпоративный мессенджер, почтовый клиент). Убедитесь, что они открываются и функционируют стабильно.

**5. Проверка сетевого подключения и доступа к ресурсам.** Убедитесь в наличии подключения к локальной сети и интернету. Проверьте доступ к сетевым папкам и общим ресурсам.

**Этап 2: Ежедневное обслуживание (окончание рабочего дня)**

**6. Закрытие приложений и сохранение данных.** Убедитесь, что пользователь сохранил все рабочие документы и закрыл приложения.

**7. Корректное завершение работы ОС.** Через меню «Пуск» выберите «Завершение работы» для операционной системы. Дождитесь полного выключения компьютера. **Запрещено** выключать компьютер кнопкой питания или выдергивать кабель из розетки.

**8. Отключение питания.** Выключите монитор и другое периферийное оборудование (принтер, сканер, ИБП), если это предусмотрено правилами.

**9. Уборка рабочего места.** Протрите поверхности монитора, клавиатуры, мыши и стола специальными салфетками для оргтехники. Приведите рабочее место в порядок.

**10. Этап 3: Периодическое профилактическое обслуживание (по графику)**

**11. Отключение оборудования от сети.** Полностью обесточьте все устройства перед проведением чистки.

**12. Очистка от пыли.** Аккуратно пропылесосьте вентиляционные решетки системного блока и блоков питания с помощью узкой насадки. Сжатым воздухом из баллончика удалите пыль из клавиатуры. Корпус монитора и системного блока протрите от пыли.

**13. Проверка кабельных соединений.** Визуально и тактильно проверьте надежность подключения всех кабелей (силовых, видео, USB, сетевых) к системному блоку, монитору и розеткам. Устраните перегибы и уберите кабели в предназначенные для этого каналы.

**14. Контроль состояния оборудования.** Во время чистки визуально оцените состояние оборудования на предмет явных дефектов: вздувшиеся конденсаторы на материнской плате, сильный перегрев компонентов, физические повреждения.

**15. Этап 4: Ведение документации**

**16. Ежедневное заполнение журнала учета.** Внесите запись в журнал технического состояния (электронный или бумажный) о результатах ежедневного осмотра и проверки. Отметьте отсутствие или наличие замечаний. Пример записи: «[Дата] - РМ-15: Запуск ОС штатный, сетевое подключение стабильное, ПО работает. Замечаний нет».

**17. Фиксация инцидентов и проведенных работ.** При обнаружении неисправности или проведении профилактических работ (чистка, замена) подробно зафиксируйте в журнале: дату, описание проблемы/работы, предпринятые действия, результат. Пример: «[Дата] - РМ-07: Обнаружено ослабление кабеля монитора. Разъем поправлен, соединение восстановлено. Оборудование работает стабильно».

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

**Для реализации программы учебной практики предусмотрены следующие специальные помещения:**

**Лаборатория** Информационных технологий, программирования и баз данных.

**1)Основное оборудование:**

Автоматизированные рабочие места на 15 обучающихся с конфигурацией: процессор Core i5, оперативная память объемом 8 Гб; дискретная видеокарта 8GB ОЗУ, два монитора 23", мышь, клавиатура.

Автоматизированное рабочее место преподавателя с конфигурацией: процессор Core i5, оперативная память объемом 8 Гб, дискретная видеокарта 8GB ОЗУ, два монитора 23", мышь, клавиатура.

Проектор и экран; Многофункциональное устройство (МФУ) формата А4;

Специализированная эргономичная мебель для работы за компьютером; Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения.

Программное обеспечение общего и профессионального назначения: EclipseIDEforJavaEEDevelopers, NETFrameworkJDK 8, MicrosoftSQLServerExpressEdition, MicrosoftVisioProfessional, MicrosoftVisualStudio, MySQLInstallerforWindows, NetBeans, SQLServerManagementStudio, MicrosoftSQLServerJavaConnector, AndroidStudio, IntelliJIDEA. Интернет.

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

### 4.1. Комплект оценочной документации

Контроль и оценка результатов практики осуществляется в ходе текущего контроля и промежуточной аттестации. Формой промежуточной аттестации по учебной практике является дифференцированный зачет.

Для получения оценки по практике студент обязан представить следующий комплект отчетных документов:

- 1) Дневник (Приложение 4.1.);
- 2) Аттестационный лист (Приложение 4.2.);
- 3) Характеристику (Приложение 4.3).

В случае прохождения учебной практики на базе предприятия вышеуказанные документы заверяются печатью соответствующего предприятия.

### 4.2. Процедура оценки результатов освоения общих и профессиональных компетенций

Процедура оценки результатов освоения общих и профессиональных компетенций осуществляется по итогам выполненных видов работ.

Руководитель практики определяет студенту задание на каждый день практики, контролирует его выполнение и отражение в дневнике практики и выставляет текущую оценку за каждый день практики, за выполнение задания в целом или за каждый вид выполненной работы.

Руководитель осуществляет оценивание умений и первоначального практического опыта.

Оценивание по практике осуществляется в виде дифференцированного зачета.

Вывод о достаточном или недостаточном уровне сформированности ОК и ПК руководитель практики делает на основе оценок текущего контроля и отчетных документов по практике.

Код и наименование компетенции	Требования к умениям и практическому опыту	Формы контроля
<b>ВД.1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b>	<b>Практический опыт (навыки):</b> установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем, администрирование автоматизированных систем в защищенном исполнении, эксплуатация компонентов систем защиты информации автоматизированных систем, диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Умения: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем	Текущий контроль в форме проверки результатов выполнения заданий практики. Демонстрация сформированных умений. Промежуточная аттестация в форме дифференцированного зачета, на котором оценивается отчет, дневник и ответы на вопросы
ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной)	Умения: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации	

системы в защищен-ном исполнении.	автоматизированных систем производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы.	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищен-ном исполнении в соответствии с требованиями эксплуатационной документации.	Умения: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Умения: использовать методы для получения кода с заданной функциональностью и степенью качества.	
<b>ВД.2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</b>	Практический опыт: установка, настройка программных средств защиты информации в автоматизированной системе, обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами, тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации, решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации, применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных, учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, работа с подсистемами регистрации событий, выявление событий и инцидентов безопасности в автоматизированной системе	
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.	Текущий контроль в форме проверки результатов выполнения заданий практики. Демонстрация сформированных умений. Промежуточная аттестация в форме дифференцированного зачета, на котором оценивается отчет, дневник и ответы на вопросы
ПК.2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умения: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации.	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Умения: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.	
ПК.2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Умения: применять программные и программно-аппаратные средства для защиты информации в базах данных проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации применять математический аппарат для выполнения криптографических преобразований использовать типовые программные	



	криптографические средства, в том числе электронную подпись.	
ПК.2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Умения: применять средства гарантированного уничтожения информации.	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
<b>ВД.3 Защита информации техническими средствами</b>	Практический опыт: установка, монтаж и настройка технических средств защиты информации техническое обслуживание технических средств защиты информации применение основных типов технических средств защиты информации, применение основных типов технических средств защиты информации, выявление технических каналов утечки информации, участие в мониторинге эффективности технических средств защиты информации, диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации, проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации, проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации, выявление технических каналов утечки информации, установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты	
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	Текущий контроль в форме проверки результатов выполнения заданий практики. Демонстрация сформированных умений. Промежуточная аттестация в форме дифференцированного зачета, на котором оценивается отчет, дневник и ответы на вопросы
ПК.3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Умения: применять технические средства для криптографической защиты информации конфиденциального характера, применять технические средства для уничтожения информации и носителей информации, применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами	
ПК.3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	
ПК.3.4. Осуществлять	Умения: применять технические средства для	

измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	защиты информации в условиях применения мобильных устройств обработки и передачи данных	
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Умения: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом применять инженерно-технические средства физической защиты объектов информатизации	
<b>ВД.4 Выполнение работ по профессии Оператор электронно-вычислительных и вычислительных машин</b>	<b>Практический опыт:</b> эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности; администрировании автоматизированных систем в защищенном исполнении; установке компонентов систем защиты информации автоматизированных информационных систем..	
ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Умения: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем	Текущий контроль в форме проверки результатов выполнения заданий практики. Демонстрация сформированных умений. Промежуточная аттестация в форме дифференцированного зачета, на котором оценивается отчет, дневник и ответы на вопросы
ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Умения: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	
ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Умения: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Умения: обеспечивать работоспособность, обнаруживать и устранять неисправности	
ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	
ПК 2.3 Осуществлять	Умения: диагностировать, устранять отказы,	

тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	
---	--	--

Частное профессиональное образовательное учреждение Тюменского  
областного союза потребительских обществ «Тюменский колледж  
экономики, управления и права»  
(ЧПОУ ТОСПО «ТюмКЭУП»)

## ДНЕВНИК УЧЕБНОЙ ПРАКТИКИ

---

---

наименование профессионального модуля

Специальность \_\_\_\_\_  
Код и наименование специальности

Студента(ки) \_\_\_\_\_ курса \_\_\_\_\_ группы  
форма обучения \_\_\_\_\_  
(очная, заочная)

---

(фамилия, имя, отчество)

Место практики

---

—  
(наименование организации)

Срок практики с «\_\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_\_» \_\_\_\_\_ 20\_\_ г.



Частное профессиональное образовательное учреждение  
Тюменского областного союза потребительских обществ  
«Тюменский колледж экономики, управления и права»  
(ЧПОУ ТОСПО «ТюмКЭУП»)

**Аттестационный лист**

Студент(ка) \_\_\_\_\_, \_\_\_\_\_

ФИО

обучающийся(ая) на \_\_\_\_\_ курсе по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

прошел(ла) учебную практику по **ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**

в объеме 36 часов с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_ г.

в организации \_\_\_\_\_

полное наименование организации

Оценка сформированности профессиональных компетенций через виды  
и качество выполнения работ

Профессиональные компетенции	Виды и объем работ, выполненных обучающимся во время практики, согласно программе производственной практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика	Оценка сформированности профессиональных компетенций*	
			«ДА»	«НЕТ»
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Развертывание защищенной программно-аппаратной платформы: Установка и базовая настройка операционной системы Astra Linux Special Edition на виртуальную машину. Проведение первоначального закрепления (hardening) ОС в соответствии с руководством по безопасной настройке: отключение неиспользуемых сетевых служб, настройка политики паролей и блокировки учетных записей, активация и базовая настройка подсистемы РАМ. Установка и настройка СУБД PostgreSQL с включением шифрования соединений по протоколу SSL.			
	Установка и конфигурирование защищенной АИС: Поэтапная установка системы электронного документооборота в соответствии с техническим паспортом и руководством администратора. Настройка защищенного сетевого взаимодействия между веб-сервером (nginx) и сервером приложений по выделенному порту с использованием TLS. Интеграция АИС с ранее настроенной СУБД PostgreSQL, создание учетных записей администратора системы с минимально необходимыми привилегиями.			
ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной	Управление доступом и ролями: Разработана и внедрена ролевая матрица доступа для сотрудников бухгалтерии и отдела кадров. В административном интерфейсе АИС созданы роли «Редактор», «Утверждающий», «Читатель» и			

(информационной) системы в защищенном исполнении.	настроены соответствующие права доступа к документам и функциям системы. Осуществлена привязка учетных записей пользователей (созданных в централизованной каталоговой службе) к созданным ролям.			
	Мониторинг и аудит: Настроен сбор и консолидация журналов событий (log-файлов) АИС и СУБД на выделенном сервере. Реализованы правила фильтрации для отслеживания критичных событий безопасности (неудачные попытки входа, попытки доступа к запрещенным разделам). Проведен еженедельный анализ журналов на предмет аномальной активности.			
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Организация резервного копирования: Разработан и реализован регламент резервного копирования, включающий: Ежедневное дифференциальное копирование базы данных АИС с помощью утилиты `pg_dump`. Еженедельное полное копирование файлового хранилища документов и конфигурационных файлов с помощью утилиты `rsync`. Настроено автоматическое выполнение заданий резервного копирования через `cron`.			
	Проактивный мониторинг производительности: Настроено отслеживание ключевых метрик системы: загрузка ЦП и ОП сервера, свободное место на дисках, доступность сетевых служб АИС. Внедрена система оповещений на электронную почту администратора при достижении пороговых значений.			
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Плановое техническое обслуживание: Еженедельно проводилась проверка целостности системного программного обеспечения и обновление вирусных баз. Выполнялась проверка и очистка дискового пространства от временных файлов. Проводился аудит установленных обновлений безопасности для ОС и прикладного ПО.			
	Устранение сбоев и восстановление работоспособности: Выявлена и устранена причина сбоя в работе веб-интерфейса АИС, связанная с исчерпанием памяти сервером приложений. Путем настройки параметров JVM и создания скрипта автоматической перезагрузки службы при критической ошибке. Локализована и устранена проблема с подключением к СУБД, вызванная некорректными настройками пула соединений в конфигурационном файле АИС.			
	Восстановление системы после инцидента: Смоделирован инцидент потери			

	критичного конфигурационного файла. Выполнено восстановление файла из резервной копии в течение установленного регламентом времени. Проведено полное функциональное тестирование АИС для подтверждения ее работоспособности после восстановления.			
--	---	--	--	--

\*(ДА): 91-100% - «5» 76-90% - «4» 51-75% - «3» (НЕТ): до 50% - «2»

**Характеристика деятельности обучающегося во время практики  
через оценку сформированности общих компетенций**

Общие компетенций	Основные показатели оценивания результата ОК	Уровни оценки ОК		
		Низкий	Средний	Высокий
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознают задачу в профессиональном контексте; анализируют задачу выделять её составные части; определяют этапы решения задачи; эффективно находят информацию, необходимую для решения задачи; владеют актуальными методами работы в профессиональной и смежных сферах; реализовывают составленный план; оценивают результат и последствия своих действий			
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Определяют задачи для поиска информации; определяют необходимые источники информации; планируют процесс поиска; структурируют получаемую информацию; выделяют наиболее значимое в перечне информации; оценивают практическую значимость результатов поиска; оформляют результаты поиска			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Определяют актуальность нормативно-правовой документации в профессиональной деятельности; применяют современную научную профессиональную терминологию; определяют и выстраивают траектории профессионального развития и самообразования			
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	Организовывают работу коллектива и команды; взаимодействуют с коллегами, руководством, клиентами в ходе профессиональной деятельности			
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотно излагают свои мысли и оформляют документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе			
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Описывают значимость своей специальности			
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Соблюдать нормы экологической безопасности; определяют направления ресурсосбережения в рамках профессиональной деятельности по специальности			
ОК 08. Использовать	Используют физкультурно-оздоровительную			



средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применяют рациональные приемы двигательных функций в профессиональной деятельности; пользуются средствами профилактики перенапряжения характерными для данной специальности			
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Применяют средства информационных технологий для решения профессиональных задач; используют современное программное обеспечение			

+ Низкий ;+ Средний; + Высокий.

Итоговая оценка по практике \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Руководитель практики от колледжа \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

Руководитель практики от организации \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

С результатами прохождения учебной практики  
ознакомлен \_\_\_\_\_ / \_\_\_\_\_  
подпись
расшифровка подписи

М.П.

Частное профессиональное образовательное учреждение  
Тюменского областного союза потребительских обществ  
«Тюменский колледж экономики, управления и права»  
(ЧПОУ ТОСПО «ТюмКЭУП»)

**Аттестационный лист**

Студент(ка) \_\_\_\_\_, \_\_\_\_\_,  
ФИО

обучающийся(ая) на \_\_\_\_\_ курсе по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

прошел(ла) учебную практику по **ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами**

в объеме 36 часов с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_ г.

в организации \_\_\_\_\_

полное наименование организации

Оценка сформированности профессиональных компетенций через виды и качество выполнения работ

Профессиональные компетенции	Виды и объем работ, выполненных обучающимся во время практики, согласно программе производственной практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика	Оценка сформированности профессиональных компетенций*	
			«ДА»	«НЕТ»
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Развертывание и базовая настройка средств защиты информации: Установка, настройка и проверка работоспособности антивирусного ПО, межсетевого экрана, средств криптографической защиты информации (СКЗИ) на рабочих станциях и серверах.			
ПК.2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами ПК.2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Обеспечение защиты информации в АС и работа с данными ограниченного доступа: Реализация мер по защите информации в процессе ее обработки, включая разграничение доступа, шифрование и контроль целостности.			

<p>ПК.2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств</p> <p>ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p>	<p>Уничтожение информации и реагирование на инциденты безопасности:</p> <p>Применение средств уничтожения данных и участие в мониторинге и регистрации событий безопасности</p>			
--	---	--	--	--

\*(ДА): 91-100% - «5» 76-90% - «4» 51-75% - «3» (НЕТ): до 50% - «2»

#### Характеристика деятельности обучающегося во время практики через оценку сформированности общих компетенций

Общие компетенций	Основные показатели оценивания результата ОК	Уровни оценки ОК		
		Низкий	Средний	Высокий
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознают задачу в профессиональном контексте; анализируют задачу выделять её составные части; определяют этапы решения задачи; эффективно находят информацию, необходимую для решения задачи; владеют актуальными методами работы в профессиональной и смежных сферах; реализовывают составленный план; оценивают результат и последствия своих действий			
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Определяют задачи для поиска информации; определяют необходимые источники информации; планируют процесс поиска; структурируют получаемую информацию; выделяют наиболее значимое в перечне информации; оценивают практическую значимость результатов поиска; оформляют результаты поиска			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Определяют актуальность нормативно-правовой документации в профессиональной деятельности; применяют современную научную профессиональную терминологию; определяют и выстраивают траектории профессионального развития и самообразования			
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	Организовывают работу коллектива и команды; взаимодействуют с коллегами, руководством, клиентами в ходе профессиональной деятельности			
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотно излагают свои мысли и оформляют документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе			
ОК 06. Проявлять гражданско-патриотическую	Описывают значимость своей специальности			

позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.				
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Соблюдать нормы экологической безопасности; определяют направления ресурсосбережения в рамках профессиональной деятельности по специальности			
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Используют физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применяют рациональные приемы двигательных функций в профессиональной деятельности; пользуются средствами профилактики перенапряжения характерными для данной специальности			
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Применяют средства информационных технологий для решения профессиональных задач; используют современное программное обеспечение			

+ Низкий ;+ Средний; + Высокий.

Итоговая оценка по практике \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Руководитель практики от колледжа \_\_\_\_\_ / \_\_\_\_\_  
 должность подпись расшифровка подписи

Руководитель практики от организации \_\_\_\_\_ / \_\_\_\_\_  
 должность подпись расшифровка подписи

С результатами прохождения учебной практики  
 ознакомлен \_\_\_\_\_ / \_\_\_\_\_  
 подпись расшифровка подписи

М.П.

Частное профессиональное образовательное учреждение  
Тюменского областного союза потребительских обществ  
«Тюменский колледж экономики, управления и права»  
(ЧПОУ ТОСПО «ТюмКЭУП»)

**Аттестационный лист**

Студент(ка) \_\_\_\_\_, \_\_\_\_\_  
ФИО

обучающийся(ая) на \_\_\_\_\_ курсе по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

прошел(ла) учебную практику по **ПМ.03 Защита информации техническими средствами** в объеме 36 часов с «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_ г.

в организации \_\_\_\_\_

полное наименование организации

Оценка сформированности профессиональных компетенций через виды и качество выполнения работ

Профессиональные компетенций	Виды и объем работ, выполненных обучающимся во время практики, согласно программе производственной практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика	Оценка сформированности профессиональных компетенций*	
			«ДА»	«НЕТ»
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации ПК.3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Монтаж, ввод в эксплуатацию и сервисное обслуживание ТСЗИ: Установка, настройка, плановое техническое обслуживание и текущая эксплуатация аппаратных средств защиты			
ПК.3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Проведение инструментальных измерений побочных электромагнитных излучений (ПЭМИН) и наводок: Организация и проведение измерений параметров ПЭМИН от технических средств (рабочих станций, серверов, средств связи) в контролируемой зоне.			
ПК.3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Измерение уровней фоновых шумов и физических полей от ТСЗИ: Оценка эффективности работы технических средств защиты информации (например, средств виброакустической защиты, генераторов шума) путем измерения создаваемых ими полей и шумов			
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Организация работ по физической защите объекта информатизации: Участие в планировании и выполнении мероприятий по усилению физической защиты помещений, содержащих критическую информационную инфраструктуру.			

\*(ДА): 91-100% - «5» 76-90% - «4» 51-75% - «3» (НЕТ): до 50% - «2»

Характеристика деятельности обучающегося во время практики через оценку  
сформированности общих компетенций

Общие компетенций	Основные показатели оценивания результата ОК	Уровни оценки ОК		
		Низкий	Средний	Высокий
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознают задачу в профессиональном контексте; анализируют задачу выделять её составные части; определяют этапы решения задачи; эффективно находят информацию, необходимую для решения задачи; владеют актуальными методами работы в профессиональной и смежных сферах; реализовывают составленный план; оценивают результат и последствия своих действий			
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Определяют задачи для поиска информации; определяют необходимые источники информации; планируют процесс поиска; структурируют получаемую информацию; выделяют наиболее значимое в перечне информации; оценивают практическую значимость результатов поиска; оформляют результаты поиска			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Определяют актуальность нормативно-правовой документации в профессиональной деятельности; применяют современную научную профессиональную терминологию; определяют и выстраивают траектории профессионального развития и самообразования			
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	Организовывают работу коллектива и команды; взаимодействуют с коллегами, руководством, клиентами в ходе профессиональной деятельности			
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотно излагают свои мысли и оформляют документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе			
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Описывают значимость своей специальности			
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Соблюдать нормы экологической безопасности; определяют направления ресурсосбережения в рамках профессиональной деятельности по специальности			
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Используют физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применяют рациональные приемы двигательных функций в профессиональной деятельности; пользуются средствами профилактики перенапряжения характерными для данной специальности			
ОК 09. Пользоваться профессиональной	Применяют средства информационных технологий для решения профессиональных			

документацией на государственном и иностранном языках.	задач; используют современное программное обеспечение			
--	--	--	--	--

+ Низкий ;+ Средний; + Высокий.

Итоговая оценка по практике \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Руководитель практики от колледжа \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

Руководитель практики от организации \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

С результатами прохождения учебной практики  
ознакомлен \_\_\_\_\_ / \_\_\_\_\_  
подпись
расшифровка подписи

М.П.



Частное профессиональное образовательное учреждение  
Тюменского областного союза потребительских обществ  
«Тюменский колледж экономики, управления и права»  
(ЧПОУ ТОСПО «ТюмКЭУП»)

**Аттестационный лист**

Студент(ка) \_\_\_\_\_, \_\_\_\_\_

ФИО

обучающийся(аяся) на первом курсе по специальности 10.02.05 Обеспечение  
информационной безопасности автоматизированных систем  
прошел(ла) учебную практику по **ПМ.04 Выполнение работ по профессии Оператор  
электронно-вычислительных и вычислительных машин**

в объеме 36 часов с « » 202 г. по « » 202 г.

в организации \_\_\_\_\_

полное наименование организации

Оценка сформированности профессиональных компетенций через виды и качество  
выполнения работ

Профессиональные компетенций	Виды и объем работ, выполненных обучающимся во время практики, согласно программе производственной практики	Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика	Оценка сформированности профессиональных компетенций*	
			«ДА»	«НЕТ»
ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Под руководством специалиста принял участие в развертывании рабочей станции защищенного исполнения (на базе ОС Astra Linux или Alt Linux). Самостоятельно установил и настроил сертифицированное офисное программное обеспечение (Р7-Офис, LibreOffice) в соответствии с инструкцией по установке. Выполнил подключение и настройку сертифицированного аппаратного средства криптографической защиты информации (СЗИ) «КриптоПро CSP» для работы с электронной подписью, включая установку личных сертификатов. Участвовал в подключении и первичной настройке защищенного сетевого оборудования (маршрутизатор Cisco) согласно руководству по эксплуатации: настройка базовых параметров, правил фильтрации MAC-адресов.			
ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Ежедневно осуществлял мониторинг работоспособности ключевых сервисов защищенной АС с помощью встроенных средств ОС и систем мониторинга (Zabbix). Выполнял учет и управление учетными записями пользователей: создание, блокировка, сброс паролей в соответствии с заявками в системе HelpDesk. Проводил аудит системных журналов (журналов событий Windows / Linux) на предмет выявления аномальных событий и ошибок. Участвовал в обновлении (патчинге) операционных систем и			

	прикладного программного обеспечения на рабочих станциях защищенного контура.			
ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	<p>Участвовал в проведении плановых профилактических работ по резервному копированию данных защищенной АС с использованием штатных средств (rsync, Bacula) и специализированного ПО.</p> <p>Выполнял проверку целостности резервных копий путем их тестового восстановления в изолированную среду.</p> <p>Осуществлял контроль за использованием дискового пространства на серверах и рабочих станциях, производил его очистку в соответствии с регламентом.</p> <p>Составлял и актуализировал простейшую эксплуатационную документацию (инструкции по запуску/остановке сервисов, чек-листы ежедневного контроля).</p>			
ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	<p>Проводил диагностику и устранил отказ жесткого диска на рабочей станции пользователя: выявил аппаратную неисправность по SMART-атрибутам, заменил диск и восстановил ОС и данные из резервной копии.</p> <p>Выполнил восстановление работоспособности сертифицированного СЗИ после сбоя в работе драйверов: переустановил ПО, настроил корректное взаимодействие с криптопровайдером.</p> <p>Участвовал в поиске и устранении неисправности в сети (проблема с кабелем), используя кабельный тестер.</p> <p>Проводил еженедельный визуальный осмотр и очистку серверного и коммутационного оборудования от пыли.</p>			
ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	<p>Самостоятельно установил и настроил межсетевой экран уровня ОС (iptables на Linux-сервере) согласно правилам, предоставленным администратором безопасности.</p> <p>Участвовал в развертывании и первичной настройке сертифицированного средства защиты от вредоносного ПО (Kaspersky Endpoint Security для Linux) на серверах защищенного контура.</p> <p>Выполнил установку и настройку системы обнаружения вторжений (IDS) Snort на демонстрационном стенде, настроил правила для отслеживания подозрительной сетевой активности.</p>			

ПК 2.3 Осуществлять тестирование функций отдельных программных и аппаратных средств защиты информации.	Провел тестирование работоспособности системы резервного копирования: инициировал создание копии, проверил ее целостность и выполнил процедуру тестового восстановления файлов. Участвовал в плановых тестах антивирусной защиты, запуская на изолированной виртуальной машине эталонные вирусные тестовые файлы (EICAR) и фиксируя реакцию СЗИ. Проверил корректность работы правил межсетевого экрана с помощью утилит сетевого сканирования (nmap, telnet) на разрешенные и запрещенные порты. Составил отчеты по результатам тестирования с выводами и рекомендациями.			
--	--	--	--	--

\*(ДА): 91-100% - «5» 76-90% - «4» 51-75% - «3» (НЕТ): до 50% - «2»

### Характеристика деятельности обучающегося во время практики через оценку сформированности общих компетенций

Общие компетенций	Основные показатели оценивания результата ОК	Уровни оценки ОК		
		Низкий	Средний	Высокий
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Распознают задачу в профессиональном контексте; анализируют задачу выделять её составные части; определяют этапы решения задачи; эффективно находят информацию, необходимую для решения задачи; владеют актуальными методами работы в профессиональной и смежных сферах; реализовывают составленный план; оценивают результат и последствия своих действий			
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Определяют задачи для поиска информации; определяют необходимые источники информации; планируют процесс поиска; структурируют получаемую информацию; выделяют наиболее значимое в перечне информации; оценивают практическую значимость результатов поиска; оформляют результаты поиска			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Определяют актуальность нормативно-правовой документации в профессиональной деятельности; применяют современную научную профессиональную терминологию; определяют и выстраивают траектории профессионального развития и самообразования			
ОК 04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Организовывают работу коллектива и команды; взаимодействуют с коллегами, руководством, клиентами в ходе профессиональной деятельности			
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотно излагают свои мысли и оформляют документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе			

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	Описывают значимость своей специальности, применять стандарты антикоррупционного поведения			
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Соблюдают нормы экологической безопасности; определяют направления ресурсосбережения в рамках профессиональной деятельности по специальности			
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Используют физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применяют рациональные приемы двигательных функций в профессиональной деятельности; пользуются средствами профилактики перенапряжения характерными для данной специальности			
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Применяют средства информационных технологий для решения профессиональных задач; используют современное программное обеспечение			

+ Низкий ;+ Средний; + Высокий.

Итоговая оценка по практике \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Руководитель практики от колледжа \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

Руководитель практики от организации \_\_\_\_\_ / \_\_\_\_\_  
должность
подпись
расшифровка подписи

С результатами прохождения учебной практики  
ознакомлен \_\_\_\_\_ / \_\_\_\_\_  
подпись
расшифровка подписи

М.П.

Выполняется на фирменном бланке организации – базы учебной практики  
**ХАРАКТЕРИСТИКА**

на обучающегося (щейся) ЧПОУ ТОСПО «ТюмКЭУП»

\_\_\_\_\_  
(ФИО)  
группы \_\_\_\_\_  
специальность \_\_\_\_\_  
(код и наименование специальности)

проходившего(шей) учебную практику по профессиональному модулю

\_\_\_\_\_  
(название профессионального модуля)  
с «\_\_» \_\_\_\_\_ 202\_\_ г. по «\_\_» \_\_\_\_\_ 202\_\_ г.  
на базе: \_\_\_\_\_  
(название организации)

За время прохождения учебной практики (по профессиональному модулю)  
зарекомендовал (а) себя

(производственная дисциплина, прилежание, внешний вид, проявление интереса к специальности, регулярность ведения дневника, индивидуальные особенности, морально - волевые качества, честность, инициатива, уравновешенность, выдержка, другое)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Приобрел (а) умения и практический опыт:

\_\_\_\_\_  
\_\_\_\_\_

Освоил (а) вид профессиональной деятельности:

\_\_\_\_\_  
\_\_\_\_\_

Сформировал (а) профессиональные компетенции:

\_\_\_\_\_  
\_\_\_\_\_

Сформировал (а) общие компетенции: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

Выводы, рекомендации: \_\_\_\_\_

**Учебную практику прошел (прошла) с оценкой**

«\_\_» \_\_\_\_\_ 20\_\_ г.  
Руководитель практики  
от организации

\_\_\_\_\_  
должность / подпись / расшифровка подписи

М.П.