МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Димитровградский инженерно-технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(ДИТИ НИЯУ МИФИ)

СОГЛАСОВАНО
От работодателя:
Зам. директора ООО "АИС Город"
должность, название предприятия
_____ Р.Н. Насальник
«15» апреля 2022 г.
М.П.

УТВЕРЖДАЮ
Руководитель ДИТИ НИЯУ МИФИ
должность и название образовательного учреждения
_____ И.И. Бегинина
«12» мая 2022 г.
М.П.

РАБОЧАЯ ПРОГРАММА

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
Шифр, название дисциплины

программы подготовки специалистов среднего звена по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
Код, наименование специальности

Форма обучения очная

Учебный цикл ПМ

Составитель: И.А. Стрельников, преподаватель техникума ДИТИ НИЯУ МИФИ
ФИО, должность

Димитровград

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ МДК
МДК.01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1.1. Область применения программы

Программа МДК является частью программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасностиавтоматизированных систем.

Место МДК в структуре ППССЗ

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по специальности 10.02.05 Обеспечение информационной безопасностиавтоматизированных систем относится к обязательной части ППССЗ и принадлежит к профессиональному модулю ПМ.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Междисциплинарные связи: содержание дисциплины связано с изучением материалов следующих дисциплин: «Операционные системы», «Технические средства информатизации».

1.2. Цели и задачи МДК – требования к результатам освоения МДК:

В результате изучения МДК студент должен освоить основной вид деятельности ВД 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:

И личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций квалифицированных рабочих, служащих/специалистов среднего звена на практике.

1.2.1. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.2.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для

	выполнения задач профессиональной деятельности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.

1.1.3. Общие компетенции воспитания в рамках основных направлений воспитательной работы.

Код	Наименование общих компетенций воспитания
В17	Формирование чувства личной ответственности за научно-технологическое развитие России, за результаты исследований и их последствия
В18	Формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения
В19	Формирование научного мировоззрения, культуры поиска нестандартных научно-технических решений, критического отношения к исследованиям лженаучного толка
В25	Формирование творческого инженерного мышления, навыков организации коллективной проектной деятельности
В 26	Формирование культуры информационной безопасности
В 27	Формирование профессиональной ответственности в области эксплуатации автоматизированных (информационных) систем в защищённом исполнении

1.3. Рекомендуемое количество часов на освоение программы дисциплины:
обязательной аудиторной учебной нагрузки обучающегося **90 часа**, из них :

- лекции 44 ч.;
- практические занятия 46 часов;
- консультаций 4 час;
- самостоятельная работа – 4 ч.;
- промежуточная аттестация – дифференцированный зачет.

2. СТРУКТУРА И СОДЕРЖАНИЕ МДК

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Количество часов*
Максимальная нагрузка	**98**
Обязательная аудиторная учебная нагрузка (всего)	**90**
в том числе:	
теоретические занятия	**44**
практические занятия	**46**
контрольные работы	**-**
консультации	**4**
Самостоятельная работа	**4**
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения	компетенции
1	*2*	*3*	*4*	
Раздел 3. Разработка защищенных автоматизированных (информационных) систем				
Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание учебного материала**	**4**		
	1. Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	2. Основные особенности современных проектов АИС. Электронный документооборот.	2		
	Лабораторные работы не предусмотрены		2,3	
	Практические работы	**4**		
	1. Практическая работа № 1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2		
	2. Практическая работа № 1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2		
	Контрольные работы не предусмотрены			
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание учебного материала**	**6**	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09 В17-19,
	1. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные,	2		

		организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.			В25-27
	2.	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2		
	3.	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	2		
	Лабораторные работы не предусмотрены				
	Практические работы		**2**		
	Практическая работа № 2. Разработка технического задания на проектирование автоматизированной системы		2	2,3	
	Контрольные работы не предусмотрены				
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	**Содержаниеучебногоматериала**		**4**		ПК 1.2-1.4 ОК 01, 02, ОК 09 В17-19, В25-27
	1	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	2	1,2	
	2	Понятие уязвимости угрозы. Классификация уязвимостей.	2		
	Лабораторные работы не предусмотрены				
	Практические работы		**10**		
	Практическая работа № 3 Категорирование информационных ресурсов		2	2,3	
	Практическая работа № 4 Анализ угроз безопасности информации		2		
	Практическая работа № 4 Анализ угроз безопасности информации		2		

	Практическая работа № 5 Построение модели угроз		2		
	Практическая работа № 5 Построение модели угроз		2		
	Контрольные работы не предусмотрены				
Тема 1.4. Основные меры защиты информации в автоматизированных системах.	**Содержаниеучебногоматериала**		**4**		ПК 1.2-1.4 ОК 01, 02, ОК 09 В17-19, В25-27
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		2	2,3	
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		2		
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание учебного материала**		**4**		ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	1	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	2	1,2	
	2	Ограничение программной среды. Защита машинных носителей информации	2		
	3	Регистрация событий безопасности			
	4	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.			
	5	Обнаружение (предотвращение) вторжений			
	6	Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации			
	7	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.			
	8	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных			

	9	Резервное копирование и восстановление данных.			
	10	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.			
	Лабораторные работы не предусмотрены			2,3	
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 1.6. Защита информации в распределенных автоматизированных системах	**Содержание учебного материала**		**4**		ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	1	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.	2	1,2	
	2	Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2		
	Лабораторные работы не предусмотрены			2,3	
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание учебного материала**		**4**		ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	1	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.	2	1,2	
	2	Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2		
	Лабораторные работы не предусмотрены			2,3	
	Практические работы		4		
	Практическая работа № 6 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.		2		
	Практическая работа № 6 Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.		2		
	Контрольные работы не предусмотрены				
Раздел 2.Эксплуатация защищенных автоматизированных систем.					

Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание учебного материала**		4		
	1	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	2	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	2		
	Лабораторные работы не предусмотрены			2,3	
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 2.2. Администрирование автоматизированных систем	**Содержание учебного материала**		**4**		
	1	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем.	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 0 9, В17-19, В25-27
	2	Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2		
	Лабораторные работы не предусмотрены				
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание учебного материала**		**2**		
	1	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 0 9, В17-19, В25-27
	Лабораторные работы не предусмотрены				
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				

Тема 2.4. **Защита от несанкционированного доступа к информации**	**Содержание**		**2**		
	1	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД. Классификация автоматизированных систем. Требования по защите информации от НСД для АС Требования защищенности СВТ от НСД к информации Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	Лабораторные работы не предусмотрены				
	Практические работы не предусмотрены				
	Контрольные работы не предусмотрены				
Тема 2.5. **СЗИ от НСД**	**Содержание**		**2**		
	1	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности. Обеспечение целостности информационной системы и информации Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	Лабораторные работы не предусмотрены				

	Практические работы	16		
	Практическая работа № 7 Установка и настройка СЗИ от НСД	2	2,3	
	Практическая работа № 7Установка и настройка СЗИ от НСД	2		
	Практическая работа № 8 Защита входа в систему (идентификация и аутентификация пользователей)	2		
	Практическая работа № 8 Защита входа в систему (идентификация и аутентификация пользователей)	2		
	Практическая работа № 9 Разграничение доступа к устройствам	2		
	Практическая работа № 9 Разграничение доступа к устройствам	2		
	Практическая работа № 10 Управление доступом	2		
	Практическая работа № 10 Управление доступом	2		
	Контрольные работы не предусмотрены			
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	**2**		
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	Лабораторные работы не предусмотрены			
	Практические работы	**4**		
	Практическая работа № 11 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2	2,3	
	Практическая работа № 12 Оформление основных эксплуатационных документов на автоматизированную систему.	2		
	Контрольные работы не предусмотрены			
Тема 2.7.	**Содержание**	**2**		

Документация на защищаемую автоматизированную систему	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	2	1,2	ПК 1.2-1.4 ОК 01, 02, ОК 09, В17-19, В25-27
	Лабораторные работы не предусмотрены			
	Практические работы	**2**		
	Зачетное занятие	2	2,3	
	Самостоятельная работа подготовка презентации	4		
	ВСЕГО	**90**		
	экзамен			
	консультации	**4**		
	Самостоятельная работа	**4**		
	ИТОГО	**98**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МДК

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).
- Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:
- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- дистрибутив устанавливаемой операционной системы;
- виртуальная машина для работы с операционной системой (гипервизор);
- СУБД;
- CASE-средства для проектирования базы данных;
- инструментальная среда программирования;
- пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

3.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Периодические издания:

Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

Журналы Защита информации. Инсайд: Информационно-методический журнал

Информационная безопасность регионов: Научно-практический журнал

Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.3. Применяемые образовательные технологии

При организации и проведении учебных занятий по дисциплине применяются элементы активного метода обучения - **компьютерное моделирование.**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике