

Приложение ППСЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2023-2024 уч.г.: Рабочая программа междисциплинарного курса МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Рабочая программа междисциплинарного курса

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

для специальности

**10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

г. Алексеевка
2023

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчик:

И.А. Дешина, преподаватель ОГАОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ МДК	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК	6
3. СТРУКТУРА И СОДЕРЖАНИЕ МДК	7
4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК	21
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК	30

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

МДК 01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ **(ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ** **ИСПОЛНЕНИИ**

1.1. Область применения рабочей программы

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

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. Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

- 1) способы защиты информации от утечки по техническим каналам;
- 2) основные методы управления защитой информации;
- 3) применять антивирусные средства защиты информации в операционных системах;
- 4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

- 1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;
- 2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;
- 3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;
- 4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;
- 5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;
- 6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;
- 7) знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.4. Количество часов на освоение рабочей программы МДК:

максимальной учебной нагрузки обучающегося – 96 часов, в том числе: аудиторной учебной работы обучающегося – 78 часов, из них в форме практической подготовки – 50 часов; в том числе практических занятий - 30 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК

Результатом освоения МДК является овладение обучающимися видом деятельности - Эксплуатация автоматизированных (информационных) систем в защищенном исполнении в том числе профессиональными компетенциями (ПК):

Код	Наименование результата обучения
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 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять 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
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
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.

3. СТРУКТУРА И СОДЕРЖАНИЕ МДК

3.1. Объем МДК и виды учебной работы

Вид учебной работы	Объем часов новый
Максимальная учебная нагрузка (всего)	96
Аудиторная учебная работа (обязательные учебные занятия) (всего)	78
из них в форме практической подготовки	96
в том числе:	
теоретические занятия	48
лабораторные работы	*
практические занятия	30
контрольные работы	*
Самостоятельная работа обучающегося (всего)	*
Консультации	12
Промежуточная аттестация в форме <i>экзамена</i>	6

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

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся	Объем часов	Коды личностных результатов, формированию которых способствует элемент программы
1	2	3	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем			
Тема 1.1. Основы информационных систем как объекта защиты.	Содержание	2/2	ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 1 ЛР 5
	1 Понятие автоматизированной (информационной) системы. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	4/4	
	Контрольные работы	*	
Тема 1.2. Жизненный цикл автоматизированных систем	Содержание	4/4	ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 4
	1 Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.		
	2 Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.		
	Лабораторные работы	*	

	Практические занятия, в том числе в форме практической подготовки: Разработка технического задания на проектирование автоматизированной системы	2/2	
	Контрольные работы	*	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание	4/4	ОК 05 ПК 1.1 ПК 1.4 ЛР 2 ЛР 3
	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 Понятие уязвимости угрозы. Классификация уязвимостей.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки: Категорирование информационных ресурсов Анализ угроз безопасности информации Построение модели угроз	6/6	
	Контрольные работы	*	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Содержание	4/4	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 1 ЛР 4
	1 Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		
	2 Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание	8/8	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 2 ЛР 3
	1 Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.		
	2 Обнаружение (предотвращение) вторжений		
	3 Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.		
	4 Защита технических средств.		

		Защита информационной системы, ее средств, систем связи и передачи данных		
		Лабораторные работы	*	
		Практические занятия, в том числе в форме практической подготовки:	*/*	
		Контрольные работы	*	
Тема 1.6. Защита информации в распределенных автоматизированных системах	Содержание		2/2	ОК 03 ПК 1.2 ЛР 1 ЛР 5
	1	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.		
		Лабораторные работы	*	
		Практические занятия, в том числе в форме практической подготовки:	*/*	
		Контрольные работы	*	
Тема 1.7. Особенности разработки информационных систем персональных данных	Содержание		2/2	ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 11
	1	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.		
		Лабораторные работы	*	
		Практические занятия, в том числе в форме практической подготовки: Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	2/2	
		Контрольные работы	*	
Раздел 2. Эксплуатация защищенных автоматизированных систем.				
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание		4/4	ОК 03 ПК 1.2 ЛР 3
	1	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.		
	2	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.		
		Лабораторные работы	*	

	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 2.2. Администрирование автоматизированных систем	Содержание	2/2	ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 5
	1 Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание	2/2	ОК 05 ПК 1.1 ПК 1.4 ЛР 9
	1 Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 2.4. Защита от несанкционированного доступа к информации	Содержание	4/4	ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 2 ЛР 3
	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.		
	2 Требования защищенности СВТ от НСД к информации		
	Лабораторные работы	*	
	Практические занятия, в том числе в форме практической подготовки:	*/*	
	Контрольные работы	*	
Тема 2.5. СЗИ от НСД	Содержание	4/4	ОК 01 ОК 03
	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.		ПК 1.1 ПК 1.4 ЛР 1
	2	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Установка и настройка СЗИ от НСД Защита входа в систему (идентификация и аутентификация пользователей) Разграничение доступа к устройствам Управление доступом Использование принтеров для печати конфиденциальных документов. Контроль печати Настройка системы для задач аудита Настройка контроля целостности и замкнутой программной среды Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		12/12	
	Контрольные работы		*	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	Содержание		4/4	ОК 05 ПК 1.1 ПК 1.4 ЛР 5 ЛР 2
	1	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.		
	2	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации		
	3	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		
	4	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем		2/2	

	Контрольные работы		*	
Тема 2.7. Документация на защищаемую автоматизированную систему	Содержание		2/2	ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 3
	1	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.		
	Лабораторные работы		*	
	Практические занятия, в том числе в форме практической подготовки: Оформление основных эксплуатационных документов на автоматизированную систему.		2/2	
	Контрольные работы		*	
Экзамен			6	
	Консультации		12	
	Всего:		96	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие учебного кабинета лаборатория программных и программно-аппаратных средств защиты информации

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении (1-е изд.) учебное пособие/Кравченко В.Б. М.: ИЦ Академия, 2018-304 с

Дополнительные источники:

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.

3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.

4. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.

6. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.

7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. — Саратов : Профобразование, 2019. — 136 с. — ISBN 978-5-4488-0355-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: <https://profspo.ru/books/86210> (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - <https://www.iprbookshop.ru/102192.html>

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж»
<http://moodle.alcollege.ru/>

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, экзамена

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Экзамен
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	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. экзамен
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	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения индивидуальных домашних заданий. Экзамен
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и	Экспертная оценка в рамках текущего контроля и на практических занятиях. Экспертная оценка выполнения

автоматизированных (информационных) систем в защищенном исполнении.	восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	индивидуальных домашних заданий. Экзамен
---	---	--