МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДАЮ:
Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке
_____Баранов Ю.А.
«29» мая 2026г

Рабочая программа дисциплины
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2026

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2026 г.

РАБОЧУЮ ПРОГРАММУ СОСТАВИЛ

Преподаватель отделения СПО _____Т.А. Бич
Подпись

СОГЛАСОВАНО

заведующий отделением СПО _____Т.В. Гуменникова
Подпись

СОГЛАСОВАНО

Зам. директора по УР _____Т.А. Евсина
Подпись

Рабочая программа обсуждена на заседании
учебно-методического совета
филиала КузГТУ в г. Новокузнецке
Протокол No 6 от 28.05.2026

1. Общая характеристика рабочей программы дисциплины

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».
Учебная дисциплина «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» обеспечивает формирование профессиональных и общих компетенций в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2 Цель и планируемые результаты освоения дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общих компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам;
Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;
Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
Знать: способы демонстрации принятых решений;
Уметь: обосновывать, анализировать и корректировать результаты собственной работы;

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами;
Уметь: обосновать и анализировать работу членов команды (подчиненных);

ОК 09. Использовать информационные технологии в профессиональной деятельности.
Знать: информационно-коммуникационные технологии профессиональной деятельности;
Уметь: использовать информационные технологии в профессиональной деятельности;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.
Знать: способы использования профессиональной документации;
Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;

профессиональных компетенций:

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
Знать: теоретические основы автоматизированных (информационных) систем в защищенном исполнении; Уметь: осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; Иметь практический опыт: администрирование автоматизированных систем в защищенном исполнении;

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации автоматизированных (информационных) систем в защищенном исполнении; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в автоматизированных (информационных) систем в защищенном исполнении; Иметь практический опыт: эксплуатация компонентов систем защиты информации автоматизированных систем;

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Знать: принципы основных методов организации и проведения технического обслуживания автоматизированных (информационных) систем в защищенном исполнении; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности автоматизированных (информационных) систем в защищенном исполнении; Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;

В результате освоения дисциплины обучающийся в общем по дисциплине должен
Знать:
- способы решения задач профессиональной деятельности, применительно к различным контекстам;
- источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;
- способы демонстрации принятых решений;
- принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами;
- информационно-коммуникационные технологии профессиональной деятельности;
- способы использования профессиональной документации;
- теоретические основы автоматизированных (информационных) систем в защищенном исполнении;
- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации автоматизированных (информационных) систем в защищенном исполнении;
- принципы основных методов организации и проведения технического обслуживания автоматизированных (информационных) систем в защищенном исполнении;
Уметь:
- выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;
- использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;
- обосновывать, анализировать и корректировать результаты собственной работы;
- обосновать и анализировать работу членов команды (подчиненных);
- использовать информационные технологии в профессиональной деятельности;
- использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;
- осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в автоматизированных (информационных) систем в защищенном исполнении;
- обеспечивать работоспособность, обнаруживать и устранять неисправности автоматизированных (информационных) систем в защищенном исполнении;
Иметь практический опыт:
- 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;

2. Структура и содержание дисциплины

2.1 Объем дисциплины и виды учебной работы

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 1 / Семестр 2			
Объем дисциплины	114		
в том числе:			
лекции, уроки	50		
лабораторные работы			
практические занятия	40		
Консультации			
Самостоятельная работа	24		
Промежуточная аттестация			
Индивидуальное проектирование			
Форма промежуточной аттестации			
Курс 2 / Семестр 3			
Объем дисциплины	42		
в том числе:			
лекции, уроки	14		
лабораторные работы			
практические занятия	14		
Консультации			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Самостоятельная работа	14		
Промежуточная аттестация			
Индивидуальное проектирование			
Форма промежуточной аттестации	дифференцированный зачет		

2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
2 семестр		
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		
Тема 1.1. Основы информационных систем как объекта защиты.		
Лекции		
	Лекция 1.1.1. 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
	Лекция 1.1.2. Основные особенности современных проектов АИС. Электронный документооборот.	2
Практические занятия		
	Практическое занятие 1.1.1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	4
Тема 1.2. *Жизненный цикл автоматизированных систем*		
Лекции		
	Лекция 1.2.1. 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
	Лекция 1.2.2. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2
	Лекция 1.2.3. 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
Практические занятия		
	Практическое занятие 1.2.1. Разработка технического задания на проектирование автоматизированной системы	6
Самостоятельная работа обучающихся		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	1.2.1. Разработка концепции защиты автоматизированной (информационной) системы	4
Тема 1.3. Угрозы безопасности информации в автоматизированных системах		
Лекции		
	Лекция 1.3.1. 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
	Лекция 1.3.2. Понятие уязвимости угрозы. Классификация уязвимостей.	2
Практические занятия		
	Практическое занятие 1.3.1. Категорирование информационных ресурсов	8
	Практическое занятие 1.3.2. Анализ угроз безопасности информации	8
	Практическое занятие 1.3.3. Построение модели угроз	8
Самостоятельная работа обучающихся		
	1.3.1. Анализ банка данных угроз безопасности информации	4
Тема 1.4. Основные меры защиты информации в автоматизированных системах		
Лекции		
	Лекция 1.4.1. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	2
	Лекция 1.4.2. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении		
Лекции		
	Лекция 1.5.1. Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	2
	Лекция 1.5.2. Ограничение программной среды. Защита машинных носителей информации	2
	Лекция 1.5.3. Регистрация событий безопасности	2
	Лекция 1.5.4. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	2
	Лекция 1.5.5. Обнаружение (предотвращение) вторжений	1
	Лекция 1.5.6. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.	2
	Лекция 1.5.7. Технологии виртуализации. Цель создания. Задачи, архитектура и	2

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	основные функции. Преимущества от внедрения.	
	Лекция 1.5.8. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.	2
	Лекция 1.5.9. Резервное копирование и восстановление данных.	2
	Лекция 1.5.10. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	2
Тема 1.6. Защита информации в распределенных автоматизированных системах		
Лекции		
	Лекция 1.6.1. 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.	2
Тема 1.7. Особенности разработки информационных систем персональных данных		
Лекции		
	Лекция 1.7.1. 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.	2
Практические занятия		
	Практическое занятие 1.7.1. Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	6
Раздел 2. Эксплуатация защищенных автоматизированных систем.		
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.		
Лекции		
	Лекция 2.1.1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	1
	Лекция 2.1.2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	1
	Лекция 2.1.3. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	1
Самостоятельная работа обучающихся		
	2.1.1. Анализ журнала аудита ОС на рабочем месте	4
	2.1.2. Построение сводной матрицы угроз автоматизированной (информационной) системы	4
	2.1.3. Анализ политик безопасности информационного объекта	4
Тема 2.2. Администрирование автоматизированных систем		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекции		
	Лекция 2.2.1. 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.	1
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении		
Лекции		
	Лекция 2.3.1. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	1
Тема 2.4. Защита от несанкционированного доступа к информации		
Лекции		
	Лекция 2.4.1. 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.	1
	Лекция 2.4.2. Классификация автоматизированных систем. Требования по защите информации от НСД для АС	1
	Лекция 2.4.3. Требования защищенности СВТ от НСД к информации	1
	Лекция 2.4.4. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	1
Самостоятельная работа обучающихся		
	2.4.1. Изучение аналитических обзоров в области построения систем безопасности	4
3 семестр		
Тема 2.5. СЗИ от НСД		
Лекции		
	Лекция 2.5.1. 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.	2
	Лекция 2.5.2. 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.	2
	Лекция 2.5.3. Обеспечение целостности информационной системы и информации	2

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	Лекция 2.5.4. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.	2
Практические занятия		
	Практическое занятие 2.5.1. Установка и настройка СЗИ от НСД	1
	Практическое занятие 2.5.2. Защита входа в систему (идентификация и аутентификация пользователей)	1
	Практическое занятие 2.5.3. Разграничение доступа к устройствам	1
	Практическое занятие 2.5.4. Управление доступом	1
	Практическое занятие 2.5.5. Использование принтеров для печати конфиденциальных документов. Контроль печати	1
	Практическое занятие 2.5.6. Настройка системы для задач аудита	1
	Практическое занятие 2.5.7. Настройка контроля целостности и замкнутой программной среды	1
	Практическое занятие 2.5.8. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	1
Самостоятельная работа обучающихся		
	2.4.1. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации	10
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях		
Лекции		
	Лекция 2.6.1. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	2
	Лекция 2.6.2. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	1
	Лекция 2.6.3. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	1
	Лекция 2.6.4. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	1
Практические занятия		
	Практическое занятие 2.6.1. Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	4
Тема 2.7. Документация на защищаемую автоматизированную систему		
Лекции		
	Лекция 2.7.1. Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
Практические занятия		
	Практическое занятие 2.7.1. Оформление основных эксплуатационных документов на автоматизированную систему.	4

3 Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)

3.1 Специальные помещения для реализации программы

Наличия учебного кабинета «информационной безопасности, лаборатории информационных технологий».

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий «Информационная безопасность»;
- электронное учебное пособие.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением, мультимедийный диапроектор, интерактивная доска.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО / Внуков А. А.. – 3-е изд., пер. и доп. – Москва :Юрайт, 2020. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356. – Текст : электронный.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471159 .

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475890

2. Дополнительная литература

1. Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — Москва : Издательство Юрайт, 2021. — 431 с. — (Профессиональное образование). — ISBN 978-5-534-11624-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476355 .

3 Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL: http://library.kuzstu.ru/meto.php?n=9964 – Текст : электронный

3.2.4 Интернет ресурсы

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

с) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.
2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.
3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.
4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.
5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.
6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.
7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.
9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.
10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.
11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Организация самостоятельной работы обучающихся

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля).

Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

6. Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных, так и современных интерактивных технологий. При контактной работе педагогического работника с обучающимися применяются следующие элементы интерактивных технологий:
- совместный разбор проблемных ситуаций;
- совместное выявление причинно-следственных связей вещей и событий, происходящих в повседневной жизни, и их сопоставление с учебным материалом.
2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.