МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

13.02.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2024 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2024, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
13.02.2024 г. протокол № 4

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ИиИБ_____ Д.Н. Мазнин

Рецензент:
Начальник отдела информационной безопасности «КУБ» (АО)
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Научиться разрабатывать проектные решения по защите информации (ЗИ) в автоматизированных системах (АС):

1. Разрабатывать организационно-распорядительную и техническую документацию по защите информации в АС;

2. Определять направления информационных технологий, для которых необходимо производить работы по защите информации в рамках защищаемой АС;

3. Определять требуемый состав СЗИ и СКЗИ, необходимых для нейтрализации угроз, и разрабатывать сценарии их применения;

4. Разрабатывать и реализовывать сценарии подготовки и тренировки ИБ-персонала посредством киберучений.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Технологии обеспечения информационной безопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Безопасность сетей ЭВМ

Безопасность систем баз данных

Моделирование угроз информационной безопасности

Безопасность Интернета вещей

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Теория информации

Сети и системы передачи информации

Информационные технологии. Базы данных

Организация ЭВМ и вычислительных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Анализ рисков информационной безопасности

Методы и стандарты оценки защищенности компьютерных систем

Разработка Siem систем

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Управление информационной безопасностью

Аттестация АИС

Защита программного обеспечения

Защита электронного документооборота

Методы выявления нарушений информационной безопасности

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Технологии обеспечения информационной безопасности» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 69,8 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 74,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. 1. Угрозы безопасности в информационных системах								
1.1 Понятие "угрозы безопасности" в информационных системах. Виды угроз, классификация угроз. Определение предмета угрозы безопасности в информационных системах и вычислительных сетях. Понятие "нарушитель" в информационной системе. Модели нарушителей в информационных системах. Классификация нарушителей. Внешний и внутренний нарушитель.	7	4		4	8,2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
1.2 Планирование работ по обеспечению безопасности в информационных системах. Этапы, объем и содержание работ. Организационно-распорядительная и техническая документация для выполнения работ по защите автоматизированной системы. Техническое задание на разработку системы защиты информации и технический проект системы защиты информации.						Выполнение самостоятельного задания "Разработка технического задания на разработку системы защиты информации"	Защита самостоятельного задания "Разработка технического задания на разработку системы защиты информации"	
Итого по разделу		4		4	8,2			

2. 2. Виды информационной безопасности								
2.1 Виды информационной безопасности: 1. Сетевая безопасность. 2. Безопасность веб-приложений. 3. Безопасность данных. 4. Безопасность конечных устройств. 5. Облачная безопасность. 6. Безопасность интернета вещей. 7. Устойчивость к целевым кибератакам APT-группировок	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) по каждому из видов информационной безопасности с примерами реализации	Устный опрос по теме "Примеры реализации информационной безопасности"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		4		4	8			
3. 3. Безопасность конечных устройств								
3.1 Безопасность конечных устройств (рабочих мест). Угрозы безопасности рабочих мест - недоверенная загрузка, несанкционированный доступ и т.д. Модели нарушителя информационной безопасности при защите конечных устройств. Требования к комплексной защите конечных устройств.	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
3.2 Средства защиты информации для конечных устройств.		4			8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическая работа "Развертывание средства защиты информации от несанкционированного доступа"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		8		4	16			
4. 4. Сетевая безопасность								

4.1 Безопасность вычислительных сетей	7	4		4	4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическая работа "Развертывание средства межсетевого экранирования"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
4.2 Безопасность Web-приложений						Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическая работа "Использование Web Application Firewall (WAF)"	
4.3 Безопасность интернета вещей						Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)		
Итого по разделу		4		4	4			
5. 5. Безопасность данных								
5.1 Безопасность систем управления базами данных	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическое занятие "Безопасность данных в СУБД - защита и разграничение доступа"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4

5.2 Безопасность облачных данных						Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	
Итого по разделу		4		4	8			
6. 6. Применение средств криптографической защиты информации (СКЗИ)								
6.1 Нормативно-правовые и методические документы, регламентирующие применение СКЗИ для защиты информации в автоматизированных системах. Состав применяемых СКЗИ и сценарии их возможного применения.	7	4		4	8	Изучение методических рекомендаций и приказов организаций-регуляторов в области криптографическ ой защиты информации	Устный опрос	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
6.2 Использование СКЗИ для обеспечения защиты информации в автоматизированных системах						Изучение учебных пособий и технической документации по использованию СКЗИ ViPNet	Выполнение практической работы "Использование СКЗИ ViPNet Office"	
Итого по разделу		4		4	8			
7. 7. Устойчивость к целевым кибератакам APT-группировок								
7.1 Целевая кибератака как самый сложный вариант компьютерной атаки. Киберпреступность, цели киберпреступности. Наиболее распространенные сценарии и инструментарий целевых кибератак. Киберучения - командная игра по моделированию целевой кибератаки и ее отражению.	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическое задание "Командная игра "Киберучения". Разработка сценария целевой кибератаки и методов противодействия ей"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		4		4	8			
8. 8. Организационно-правовое обеспечение информационной безопасности								

8.1 Определение необходимого набора организационно-правовых документов и мер защиты, состава и видов средств защиты информации в соответствии с требованиями модели угроз и нормативно-правовой базы для обеспечения информационной безопасности автоматизированной системы	7	2		6	14	Выполнение индивидуального задания "Разработка перечня организационно-распорядительной документации" с решением задачи определения набора компенсирующих мер защиты информации и необходимых средств защиты информации	Защита индивидуального задания	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		2		6	14			
Итого за семестр		34		34	74,		зао	
Итого по дисциплине		34		34	74,		зачет с оценкой	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Технологии обеспечения информационной безопасности» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Доступ из справочно-правовой системы Консультант-Плюс.

2. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Доступ из справочно-правовой системы Консультант-Плюс.

3. Методический документ "Методика оценки угроз информации". Утвержден ФСТЭК России 5 февраля 2021 г. // URL https://docs.cntd.ru/document/607699443#7D80K5 (Дата обращения 31.01.2024 г.)

4. Банк данных угроз безопасности информации ФСТЭК России. // URL https://bdu.fstec.ru/threat (Дата обращения 31.01.2024 г.)

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утв. руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432

6. Модель угроз безопасности персональных данных - что это такое и как составлять. Блог компании "Selectel" // URL https://selectel.ru/blog/personal-data-security-threat-model/ (дата обращения 31.01.2024 г.)

б) Дополнительная литература:

Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.01.2024)

МАКРООБЪЕКТЫ:

Баранкова, И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон.

опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858 (дата обращения: 31.01.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

в) Методические указания:

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007	№ 135 от 17.09.2007	бессрочно
7Zip	свободно	бессрочно
Kaspersky Endpoint Security для бизнеса-Станд	Д-165-23 от 27.03.2023	27.03.2025
Ред ОС	Сертификат №01-04\22	06.05.2025
Linux	свободно	бессрочно
Браузер	свободно	бессрочно
Браузер Mozilla	свободно распростран	бессрочно
Calculate Linux Desktop	свободно распростран	бессрочно
Электронные плакаты по дисциплине "Сети ЭВМ"	Д-903-13 от 14.06.2013	бессрочно
LibreOffice	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий	https://dlib.eastview.com/
Поисковая система Академия Google (Google	URL: https://scholar.google.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И.	https://host.megaprolib.net/MP0109/Web
Российская Государственная	https://www.rsl.ru/ru/4readers/catalogues/
Информационная система - Нормативные правовые акты, организационно-распоряди тельные документы,	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053

Информационная система - Банк данных угроз безопасности	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

Компьютерный класс - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Технологии обеспечения информационной безопасности» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

1. Угрозы информационной безопасности в автоматизированных системах.
2. Инцидент безопасности – что это такое. Цели и задачи обработки и анализа инцидентов безопасности в автоматизированных системах.
3. Нарушитель информационной безопасности – виды и способы противодействия.
4. Организация работ по защите информации в автоматизированных системах. Этапы работ и необходимые документы.
5. Техническое задание на разработку системы защиты информации. Основные элементы.
6. Технический проект системы защиты информации.
7. Основные направления работ по защите информации в автоматизированных системах.
8. Основные угрозы для конечных устройств.
9. СЗИ для защиты конечных устройств и сценарии их применения.
10. Угрозы информационной безопасности в современных вычислительных сетях и способы их нейтрализации.
11. СЗИ для защиты вычислительной сети и сценарии их применения.
12. Безопасность Web-приложений – основные угрозы, способы и технологии организации защиты.
13. СЗИ для защиты Web-приложений и сценарии их применения.

14. Безопасность интернета вещей – основные угрозы и способы защиты от них.
15. Организация безопасной работы при использовании СУБД. Защита доступа к СУБД. Разграничение доступа к СУБД.
16. Использование и сценарии применения средств криптографической защиты информации (СКЗИ) в автоматизированных системах.
17. Применение СКЗИ для построения защищенной сети передачи данных на примере технологии ViPNet.
18. Безопасность данных при использовании облачных технологий – средства защиты информации и сценарии их применения.
19. Целевая APT-атака как самый сложный сценарий компьютерной атаки.
20. Противодействие APT-атаке. Киберучения и их формат.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах		
ПК-7.1 Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах		
1. Способность к самостоятельному анализу тенденций развития информационных технологий с точки зрения специалиста по информационной безопасности; 2. Способность прогнозировать потребности организации в технологиях защиты информации исходя из характера хозяйственной деятельности организации и обрабатываемой ею информации; 3. Знание состава организационно-распорядительной и технической документации, необходимой для организации работ по защите информации в автоматизированных системах; 4. Навыки разработки организационно-распорядительной документации в области ИБ; 5. Знание базовых нормативно-правовых документов, необходимых для организации работ по информационной безопасности в организации.		
ПК-7.2 Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы		
1. Анализ структуры АС с определением необходимых работ по направлению информационной безопасности; 2. Определение необходимых мероприятий по ИБ исходя из разработанной модели угроз; 3. Определение состава организационно-распорядительных и технических мер по реализации плана мероприятий; 4. Разработка и реализация политики безопасности на основе разработанной организационно-распорядительной и технической документации по защите информации в АС; 5. Организация и проведение контрольных мероприятий.		
ПК-7.3 Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации		
1. Знание основных рабочих характеристик современных средств защиты информации (СЗИ), способность к самостоятельному выбору необходимых СЗИ при разработке проекта защиты информационной инфраструктуры;		

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
2. Понимание принципов функционирования средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ); 3. Знание номенклатуры средств защиты информации отечественного и мирового производства; 4. Разработка сценариев применения СЗИ и СКЗИ при использовании их в автоматизированных системах.		
ПК-7.4 Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем		
1. Знание современной нормативно-правовой базы в области информационной безопасности; 2. Разработка проектной документации на систему защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области ИБ; 3. Способность сделать заключение о соответствии разработанной политики информационной безопасности при настройке и конфигурировании СЗИ в автоматизированной системе требованиям нормативно-правовых документов.		

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Показатели и критерии оценивания зачета с оценкой:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе

знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.