МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
технологий обработки и защиты информации
А.А. Сирота

_____
01.07.2021г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.39 Основы информационной безопасности

1. Код и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация: анализ безопасности компьютерных систем, математические методы защиты информации

3. Квалификация выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: технологий обработки и защиты информации

6. Составители программы: Нестеровский Олег Игоревич, к.т.н., доцент

7. Рекомендована: протокол НМС ФКН № 5 от 10.03.2021 г.

8. Учебный год: 2022-2023 **Семестр(ы)/Триместр(ы):** 3

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

изучение основ и принципов организации и информационной безопасности в рамках комплексного обеспечения безопасности; получение профессиональных компетенций в области информационной безопасности.

Задачи дисциплины:

- обучение студентов базовым основам обеспечения информационной безопасности государства;
- обучение студентов базовым методологиям создания систем защиты информации;
- обучение студентов базовым основам процесса сбора, передачи, накопления и обработки информации;
- обучение студентов основам методов и средств ведения информационных противоборств;
- обучение студентов базовым способам оценки защищенности и обеспечения информационной;
- обучение студентов базовым принципам обеспечения безопасности объектов информатизации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относиться к обязательной части Блок 1. Дисциплины (модули).

Входные знания в области нормативной и законодательной базы в области информационной безопасности, физики, распространения сигналов, теории веро-ятностей и математической статистики, информатики.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1	Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	Знать: понятия в области информационного управления, информационного воздействия, их роль в информационном обществе, основные типы и содержание технологий информационного воздействия, информационные операции в сети Интернет, основные положения государственной политики Российской Федерации в области информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире; Уметь: определять и классифицировать субъекты, объекты и источники угроз информационно безопасности, информационные воздействия в различных коммуникативных ситуациях; использовать технологии скрытого управления личностью и обществом с помощью информационных воздействий, применять способы психологической самозащиты; Владеть: навыками информационного управления информационной безопасностью, способами манипулирования в массовых информационных процессах; навыками применения моделей, ресурсов, технологий защиты от информационных воз-
		ОПК-1.2	Знает классификацию защищаемой информации по видам тайны и степеням конфиденциальности;	
		ОПК-1.3	Знает классификацию и основные угрозы информационной безопасности для объекта информатизации;	

				действий.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1	знает источники и классификацию угроз информационной безопасности	Знать: источники и классификацию угроз информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России Уметь: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; Владеть: навыками информационного управления информационной безопасностью, способами манипулирования в массовых информационных процессах; навыками применения моделей, ресурсов, технологий защиты от информационных воздействий.
		ОПК-5.2	знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной	
		ОПК-5.3	умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	
		ОПК-5.4	умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	

12. Объем дисциплины в зачетных единицах/час. — 4/144.

Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра - 3	№ семестра	итого
Аудиторные занятия		72	72		27
в том числе:	лекции	36	36		36
	практические	36	36		36
	лабораторные				
Самостоятельная работа		36	36		36
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – 36 час.)*		36	36		36
Итого:		144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Общие проблемы безопасности. Роль и место информационном безопасности	1. Предметная область информационной безопасности. Исторические сведения и этапы развития проблем и технологий обеспечения информационной безопасности. 2. Математические основы обеспечения информационной безопасности.	
1.2	Методы и средства защиты информации	3. Функции непосредственной защиты информации. Механизмы защиты, управление механизмами защиты. 4. Методы защиты информации от преднамеренного доступа, методы защиты информации в вы-	

		числительных системах. 5. Методы идентификации и установления подлинности субъектов и различных объектов. 6. Технические, программные и организационно-правовые средства защиты информации. 7. Современные средства и способы обеспечения информационной безопасности.	
1.3	Перспективы развития информационной безопасности	8. Методы и средства развития информационной безопасности и методов и средств ведения информационных противоборств	
2. Практические занятия			
2.1	Методы и средства защиты информации	1. Функции непосредственной защиты информации. Механизмы защиты, управление механизмами защиты. 2. Методы защиты информации от преднамеренного доступа, методы защиты информации в вычислительных системах. 3. Методы идентификации и установления подлинности субъектов и различных объектов. 4. Технические, программные и организационно-правовые средства защиты информации. 5. Современные средства и способы обеспечения информационной безопасности.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Общие проблемы безопасности. Роль и место информационном безопасности	10	4		10	24
2	Методы и средства защиты информации	16	28		16	60
3	Перспективы развития информационной безопасности	10	4		10	24
	Итого:	36	36		36	108

14. Методические указания для обучающихся по освоению дисциплины:

1) При изучении дисциплины рекомендуется использовать следующие средства: рекомендуемую основную и дополнительную литературу; методические указания и пособия; контрольные задания для закрепления теоретического материала; электронные версии учебников и методических указаний для выполнения практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка знаний основ информационной безопасности.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Основы информационной безопасности : учебное пособие / С.А. Нестеров .— Изд. 4-е, стер. — Санкт-Петербург ; Москва ; Краснодар : Лань, 2018 .— 321 с. : ил., табл. — (Учебники для вузов. Специальная литература) (Библиотека высшей школы) .— Библиогр.: с. 319-321.*
2	Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.

б) дополнительная литература:

№ п/п	Источник
1	Организационно-правовое обеспечение информационной безопасности : учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов и др.; под ред. А. А. Стрельцова. – М.: Издательский центр «Академия», 2008. — 256 с.
2	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типо-графия, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
3	Тарасов А.М. Электронное правительство и информационная безопасность: учеб. пособие М.: ГАЛАРТ, 2011
4	Ярочкин Владимир Иванович. Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин .– М. : Академический Проект, 2003.– 638,[1] с. : ил. – (Gaudeamus.Учебник для вузов).– Библиогр.: с.633-637.– ISBN 5-8291-0292-7.– ISBN 5-902357-02-0.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет) *:

№ п/п	Ресурс
1	«Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020
2	«Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020
3	ЭБС «Лань» - Контракт №3010-06/03-21 от 10.03.2021
4	«РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2021
5	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
6	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
7	http://organizacionnaya-zashhita/ - Информационная безопасность
8	http://www. inform11_97/aiti1.htm - Правовое обеспечение системы защиты информации на предприятии
9	http://content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html - Организационные основы защиты информации на предприятии
10	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	*Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.*
2	*Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2) ОС Windows v.7, 8, 10; LibreOffice v.5-7; Foxit PDF Reader; MATLAB “Total Academic Headcount – 25”; Windows Server v. 2008-2019

3) LibreOffice v.5-7.

4) Foxit PDF Reader.

5) При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 381), ПК-Intel-i3, рабочее место преподавателя: проектор, видео коммутатор, специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Общие проблемы безопасности. Роль и место информационном безопасности	ОПК-1, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос
2.	Методы и средства защиты информации	ОПК-1, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос Тест № 1 Практическое задание
3.	Перспективы развития информационной безопасности	ОПК-1, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос
Промежуточная аттестация форма контроля – экзамен				Комплект КИМ

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными;

3) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Тест	Теоретические вопросы по темам/разделам дисциплины	Содержит 4 тестовых вопроса, за правильный ответ на каждый из которых дается 1 балл
3	Практическое задание	Практические задачи	Оценка «отлично» выставляется студенту, если он исчерпывающе и свободно справляется с практическими заданиями, дает правильное обоснование принятого решения; Оценка «хорошо» выставляется студенту, если он правильно, но недостаточно полно выполняет задания, не допускает существенных неточностей; Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить; Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и

			неправильно выполняет практические задания

Примерный перечень вопросов для устного опроса

1. Виды национальной безопасности и их краткая характеристика.
2. Средства обеспечения информационной безопасности.
3. Системные связи информационной безопасности с другими видами национальной безопасности.
4. Аппаратные средства обеспечения информационной безопасности.
5. Информационные уязвимости объектов.
6. Программные средства обеспечения информационной безопасности.
7. Антропогенные информационные уязвимости.
8. Криптографические средства обеспечения информационной безопасности.
9. Техногенные информационные уязвимости.
10. Стеганографические средства обеспечения информационной безопасности.
11. Организационно-правовые информационные уязвимости.
12. Организационно-правовые средства обеспечения информационной безопасности.
13. Комбинированные информационные уязвимости.
14. Государственная политика в области информационной безопасности.
15. Угрозы информационной безопасности и их источники.
16. Государственные органы обеспечения информационной безопасности.
17. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
18. Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.
19. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
20. Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.
21. Антропогенные и техногенные угрозы информационной безопасности, их классификация.
22. Технические каналы утечки конфиденциальной информации. Основные методы защиты.
23. Системная классификация угроз информационной безопасности.
24. Пассивные средства противодействия техническим разведкам.
25. Угрозы конфиденциальности, целостности и доступности информации.
26. Активные средства противодействия техническим разведкам.
27. Информационная война как высшая форма угрозы информационной безопасности.
28. Базовые стратегии организации защиты информации.
29. Категорирование информации.

Примерные тесовые задания

1. Что такое «национальная безопасность»?

а) совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер;

б) система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу;

в) состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

2. Информационная безопасность Российской Федерации – это:

а) состояние защищенности информации, циркулирующей в обществе;

б) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

г) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

3. В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

а) искать и распространять информацию любым способом;

б) искать, получать, передавать, производить и распространять информацию любым законным способом;

в) искать, получать, передавать, производить и распространять информацию любым способом;

г) получать и распространять информацию любым способом.

Примерные практические задания

1) Определите методы защиты информации для выделенного помещения.

2) Определите методы защиты информации для защищаемой автоматизированной системы.

3) Определите средства защиты информации для объекта информатизации.

20.2. Промежуточная аттестация

Примерный перечень вопросов к экзамену

№	Содержание
1	Виды национальной безопасности и их краткая характеристика
2	Средства обеспечения информационной безопасности
3	Системные связи информационной безопасности с другими видами национальной безопасности
4	Аппаратные средства обеспечения информационной безопасности
5	Информационные уязвимости объектов
6	Программные средства обеспечения информационной безопасности
7	Антропогенные информационные уязвимости
8	Криптографические средства обеспечения информационной безопасности
9	Техногенные информационные уязвимости
10	Стеганографические средства обеспечения информационной безопасности
11	Организационно-правовые информационные уязвимости
12	Организационно-правовые средства обеспечения информационной безопасности
13	Комбинированные информационные уязвимости
14	Государственная политика в области информационной безопасности
15	Угрозы информационной безопасности и их источники
16	Государственные органы обеспечения информационной безопасности
17	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация
18	Приоритетные направления обеспечения информационной безопасности в условиях информационного общества
19	Эндогенные и экзогенные, угрозы информационной безопасности, их классификация
20	Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества
21	Антропогенные и техногенные угрозы информационной безопасности, их классификация

22	Технические каналы утечки конфиденциальной информации. Основные методы защиты
23	Системная классификация угроз информационной безопасности
24	Пассивные средства противодействия техническим разведкам
25	Угрозы конфиденциальности, целостности и доступности информации
26	Активные средства противодействия техническим разведкам
27	Информационная война как высшая форма угрозы информационной безопасности
28	Базовые стратегии организации защиты информации
29	Категорирование информации
30	Полное множество функций защиты информации

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой
технологий обработки и защиты информации

_____ А.А. Сирота

«____»_____ 2021

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.39 Основы информационной безопасности

Форма обучения Очное

Вид контроля экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Виды национальной безопасности и их краткая характеристика
2. Средства обеспечения информационной безопасности

Преподаватель _____ О.И. Нестеровский

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше.