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.В.12 Информационная безопасность

1. Код и наименование направления подготовки/специальности:
02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: квантовая теория информации, распределенные системы и искусственный интеллект

3. Квалификация выпускника: бакалавр

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: 2024-2025 **Семестр(ы)/Триместр(ы):** 8

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

изучение теоретических основ информационной безопасности, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты исходных и байт кодов программ; овладение практическими навыками применения методов криптографии, стеганографии, получение профессиональных компетенций в области современных технологий защиты информации.

Задачи дисциплины:

- обучение студентов теоретическим и практическим аспектам обеспечения информационной безопасности;
- обучение студентов базовым принципам защиты конфиденциальной информации, методам идентификации, аутентификации пользователей информационной системы, принципам организации скрытых каналов передачи информации, принципам защиты авторских прав на объекты цифровой интеллектуальной собственности;
- овладение практическими навыками применения теоретических знаний для шифрования конфиденциальной информации, стеганографического скрытия информации, контроля за целостностью информации, решения задач идентификации и аутентификации.

10. Место учебной дисциплины в структуре ООП:

Входит в блок вариативные дисциплин Б1.В.

Входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, криптографии, 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
ПК-1	Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	ПК-1.1	Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий,	Знать: основные теоретические и практические аспекты обеспечения информационной безопасности, основные требования к обеспечению информационной безопасности, в том числе защите государственной тайны; Уметь: применять на практике теоретические знания в области криптографии и стеганографии; Владеть: практическими навыками раз-работки и применения в профессиональной деятельности криптографических и стеганографических алгоритмов.
		ПК-1.2	умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике,	
		ПК-1.3	имеет практический опыт научно-исследовательской деятельности в математике и информатике	
ПК-4	Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	ПК-4.1	Знает 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,	Знать: методы и средства защиты конфиденциальности информации, методы контроля целостности и аутентификации данных, принципы организации скрытых каналов передачи информации; Уметь: разрабатывать и применять на практике специализированные программные средства в интересах обеспечения безопасности и целостности данных; Владеть: практическими навыками применения специализированных
		ПК-4.2	умеет классифицировать защищаемую информацию	

			по видам тайны и степеням конфиденциальности,	программных средств, предназначенных для обеспечения без-опасности и целостности данных.
		ПК-4.3.	умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	

12. Объем дисциплины в зачетных единицах/час. — 3/108.

Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра - 8	№ семестра	итого
Аудиторные занятия		36	36		36
в том числе:	лекции	24	24		24
	практические	12	12		12
	лабораторные				
Самостоятельная работа		36	36		36
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – 36 час.)*		36	36		36
Итого:		108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Основы государственной информационной политики и информационной безопасности Российской Федерации	Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика. Информационные ресурсы. Проблемы информационной войны. Проблемы информационной безопасности в сфере государственного и муниципального управления.	Создан электронный курс, размещены материалы к лекции.
1.2	Информационная безопасность автоматизированных систем	Современная постановка задачи защиты информации. Организационно-правовое обеспечение, информационной безопасности. Информационные системы. Угрозы информации. Методы и модели оценки уязвимости информации.	Создан электронный курс, размещены материалы к лекции.
1.3	Методы и модели оценки уязвимости информации	Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита».	Создан электронный курс, размещены материалы к лекции.
1.4	Рекомендации по использованию моделей оценки уязвимости информации	Рекомендации по использованию моделей оценки уязвимости информации	Создан электронный курс, размещены материалы к лекции.
1.5	Методы определения требований к защите информации	Методы определения требований к защите информации	Создан электронный курс, размещены материалы к лекции.

1.6	Функции и задачи защиты информации	Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации	Создан электронный курс, размещены материалы к лекции.
1.7	Стратегии защиты информации	Стратегии защиты информации.	Создан электронный курс, размещены материалы к лекции.
1.8	Способы и средства защиты информации	Способы и средства защиты информации.	Создан электронный курс, размещены материалы к лекции.
1.9	Криптографические методы защиты информации	Требования ккриптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хеш-функции. Криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Цифровые водяные знаки (ЦВЗ), виды реализации, практические области применения.	Создан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
1.10	Архитектура систем защиты информации	Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации.	Создан электронный курс, размещены материалы к лекции.
2. Практические занятия			
2.1	нет		
3. Лабораторные работы			
3.1	Криптографические методы защиты информации	1. Практическое изучение работы алгоритмов блочного симметричного шифрования. 2. Изучение криптографических генераторов случайных чисел. 3. Практическое изучение работы асимметричных алгоритмов шифрования. 4. Изучение частотных характеристик текстовых сообщений. 5. Изучение алгоритмов стеганографического скрытия данных в пространственной и частотной области контейнеров (на примере цифровых изображений). 6. Практическое изучение принципов и методов стегоанализа (на примере визуального и статистического стегоанализа цифровых изображений).	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	2			4	6
2	Информационная безопасность автоматизированных систем	2			4	6
3	Методы и модели оценки уязвимости информации	2			4	6
4	Рекомендации по использованию моделей оценки уязвимости информации	2			2	4
5	Методы определения требований к защите информации	2			2	4

6	Функции и задачи защиты информации	2			2	4
7	Стратегии защиты информации	2			2	4
8	Способы и средства защиты информации	2			2	4
9	Криптографические методы защиты информации	6		12	12	30
10	Архитектура систем защиты информации	2			2	4
	Итого:	24		12	36	72

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	Элементы теории чисел и критозащита : учебное пособие / Воронеж. гос. ун-т; сост. : Б.Н. Воронеков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 87 с. : ил .— Библиогр.: с.87 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-95.pdf>.

б) дополнительная литература:

№ п/п	Источник
1	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.
2	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.
3	Теоретические основы компьютерной безопасности (учебное пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.

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
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	*Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.*

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; MATLAB “Total Academic Headcount – 25”; Dr. Web

3) 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, видеокоммутатор, 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.	Основы государственной информационной политики и информационной безопасности Российской Федерации	ПК-1, ПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
2.	Информационная безопасность автоматизированных систем	ПК-1, ПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос
3.	Методы и модели оценки уязвимости информации	ПК-1, ПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-5.1, ОПК-5.2, ОПК-5.3, ОПК-5.4	Устный опрос
4.	Рекомендации по использованию моделей оценки уязвимости информации	ПК-1, ПК-4		Устный опрос
5.	Методы определения требований к защите информации	ПК-1, ПК-4		Устный опрос
6.	Функции и задачи защиты информации	ПК-1, ПК-4		Устный опрос
7.	Стратегии защиты информации	ПК-1, ПК-4		Устный опрос
8.	Способы и средства защиты информации	ПК-1, ПК-4		Устный опрос
9.	Криптографические методы защиты информации	ПК-1, ПК-4		Устный опрос Тест Лабораторная работа
10.	Архитектура систем защиты информации	ПК-1, ПК-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	Лабораторная работа	Содержит 6 лабораторных заданий, предусматривающих разработку и тестирование криптографических и стеганографических алгоритмов .	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.

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.
30. На чем основывается надежность алгоритма RSA.
31. Какие преобразования лежат в основе криптосистем с открытым ключом.

Пример задания для выполнения лабораторной работы

Лабораторная работа

«Изучение работы асимметричных алгоритмов шифрования»

Цель работы

Изучение работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов - 2

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Провести дешифрование текста, зашифрованного алгоритмом RSA, на основе известного открытого ключа K_p и шифрованного текста C.

$$K_p = \{n=471090785117207;\ e=12377\}$$

$$C = 31499911228106520536170634151732 1987491098667$$

20.2. Промежуточная аттестация

Примерный перечень вопросов к экзамену

№	Содержание
1	Основы государственной информационной политики и информационной безопасности Российской Федерации
2	Угрозы информационной безопасности, модели нарушителей
3	Методы и модели оценки уязвимости информации
4	Рекомендации по использованию моделей оценки уязвимости информации
5	Функции и задачи защиты информации
6	Предметная область криптографии
7	Алгоритмы симметричного шифрования, сеть Фейстеля
8	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
9	Криптосистемы с открытым ключом, однонаправленные функции
10	Однонаправленные хэш-функции
11	Электронная подпись
12	Программные датчики ПСП чисел
13	Принципы работы криптоаналитических алгоритмов.
14	Предметная область стеганографии
15	Стеганографическое скрытие данных в пространственной области контейнера
16	Стеганографическое скрытие данных в частотной области контейнера, методы кодирования с расширением спектра
17	Статистические и структурные методы скрытия информации

18	Цифровые водяные знаки
19	Стегоанализ. Визуальный, статистический, универсальный стегоанализ.
20	Архитектура систем защиты информации
21	Общие требования к построению надежной системы защиты

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
«____»_____ 2021

Направление подготовки / специальность 02.03.01 Математика и компьютерные науки

Дисциплина Б1.В.12 Информационная безопасность

Форма обучения Очное

Вид контроля экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB).
2. Цифровые водяные знаки.

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.