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

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 Криптографические протоколы и стандарты

1. Код и наименование направления специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Специализация: "Автоматизация информационно-аналитической деятельности", "Информационная безопасность финансовых и экономических структур"

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра математического анализа математического факультета

6. Составители программы: доц., к.ф.-м.н. Садчиков П.В.

7. Рекомендована: Научно-методическим советом математического факультета Протокол № 0500-07 от 29.06.2021

8. Учебный год: 2025/ 2026 Семестр(ы): 10

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

- изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации;
- формирование у студентов научного представления о работе с протоколами.

Задачи учебной дисциплины:

- обучение студентов принципам работы основных протоколов;
- овладение методами классической и современной криптографии.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Криптографические протоколы и стандарты» относится к части Блока 1, формируемой участниками образовательных отношений.

Для его успешного освоения необходимы знания и умения, приобретенные в результате обучения по предшествующим (а также параллельно изучаемым) дисциплинам: информатика, технология и методы программирования, методы и алгоритмы цифровой обработки данных, основы информационной безопасности, безопасность сетей ЭВМ, современные технологии хранения данных, методы и средства криптографической защиты информации, тактики и техники реализации компьютерных атак, анализ защищенности информационных систем, техническая защита информации.

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-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1.	Способен анализировать безопасность информации с помощью формальных моделей	Знать: основные криптографические средства защиты информации в ИАС, протоколы и стандарты Уметь: строить алгоритмы протоколов, обеспечивающих конфиденциальность и аутентичность информации Владеть: средствами защиты информации в ИАС и современными методами криптографии

12. Объем дисциплины в зачетных единицах/час.— __4__/__144___.

Форма промежуточной аттестации: Экзамен – 10 семестр

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			10 семестр
Контактная работа		54	54
в том числе:	лекции	22	22
	практические	-	-
	лабораторные	32	32

	курсовая работа	-	-
Самостоятельная работа		54	54
Промежуточная аттестация		36	36
Итого:		**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.	Основные понятия криптографии	Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.	
1.2.	Симметричные криптосистемы.	Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров	
1.3.	Основные алгоритмы с открытым ключом.	Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности	
1.4.	Управление ключами	Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.	
1.5.	Протоколы цифровых денег и электронного голосования.	Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.	
1.6	Протоколы идентификации + личностная криптография.	Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы(ID-based	

		распределенные системы).	
2. Лабораторные занятия			
1.1.	Основные понятия криптографии	Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.	
1.2.	Симметричные криптосистемы.	Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров	
1.3.	Основные алгоритмы с открытым ключом.	Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности	
1.4.	Управление ключами	Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.	
1.5.	Протоколы цифровых денег и электронного голосования.	Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.	
1.6	Протоколы идентификации + личностная криптография.	Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятель-ная работа	Всего
1	Основные понятия криптографии	2		2	9	13
2	Симметричные криптосистемы.	4		6	9	19
3	Основные алгоритмы с открытым ключом.	4		6	9	19
4	Управление ключами	4		6	9	19
5	Протоколы цифровых денег и электронного голосования.	4		6	9	19

6	Протоколы идентификации + личностная криптография.	4		6	9	19
	Итого:	22		32	54	108

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на лабораторных занятиях с помощью компьютера решаются задачи по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Криптографические протоколы и стандарты» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки теорем, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.
2. Перед лабораторным занятием обязательно повторить лекционный материал.
3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры.
4. Выбрать время для работы с литературой по дисциплине в библиотеке.
5. Обычный курс размещен в системе «Электронный университет».

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

а) основная литература:

№ п/п	Источник
1	**Авдошин, С. М.** Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. — Москва : ДМК Пресс, 2017 .— 352 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-408-3 .— <URL:https://e.lanbook.com/book/93575>.

б) дополнительная литература:

№ п/п	Источник
1	**Ищукова, Е. А.** Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ ; Южный федеральный университет ; Инженерно-технологическая академия .— Таганрог : Издательство Южного федерального университета, 2016 .— 80 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-9275-2066-4 .— <URL:http://biblioclub.ru/index.php?page=book&id=493059>

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

№ п/п	Ресурс
1	*http://eqworld.ipmnet.ru – интернет-портал, посвященный уравнениям и методам их решений*
2	*http://www.lib.vsu.ru - электронный каталог ЗНБ ВГУ*
3	*ЭБС «Университетская библиотека онлайн»*
4	*Электронный курс*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Антонов В.О. Теоретико-числовые методы в криптографии : практикум / ; авт.-сост. Ф. Б.

	Тебуева ; авт.-сост. В. О. Антонов ; Министерство образования и науки РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет» .— Ставрополь : СКФУ, 2017 .— 107 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=483838>

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

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ»

Перечень необходимого программного обеспечения: операционная система Windows или Linex, Microsoft, Windows Office, LibreOffice 5*, Calc, Math,* браузер Mozilla Firefox, Opera или Internet.

18. Материально-техническое обеспечение дисциплины:

Специализированная мебель.

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации (394018, г. Воронеж, площадь Университетская, д. 1, пом. I)

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	Основные понятия криптографии	ПК-2	ПК-2.1	Опрос
2	Симметричные криптосистемы.	ПК-2	ПК-2.1	Опрос
3	Основные алгоритмы с открытым ключом.	ПК-2	ПК-2.1	Опрос
4	Управление ключами	ПК-2	ПК-2.1	Опрос
5	Протоколы цифровых денег и электронного голосования.	ПК-2	ПК-2.1	Контрольная работа №1
6	Протоколы идентификации + личностная криптография.	ПК-2	ПК-2.1	Контрольная работа №2
Промежуточная аттестация Форма контроля -экзамен				Перечень вопросов к экзамену

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

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень вопросов для устного опроса

Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История

криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.
Потоковые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потоковым шифрам: Постулаты Голомба, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блоковые шифры. Определение блокового шифра. Требования к блоковым шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блоковых шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных 4 шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров
Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности
Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. K-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.
Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.
Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).

Примерный перечень заданий для контрольных работ

Контрольная работа №1

Задача 1. Оценить теоретически количество зашифрованного текста (в символах) для успешного частотного криптоанализа и подтвердить результаты экспериментально, если известно, что открытый текст – это осмысленный текст на русском языке и была использована следующая система шифрования: 1) Шифр Цезаря; 2) Аффинный шифр; 3) Шифр Вижинера с известной длиной ключа (показать зависимость от длины ключа); 4) Шифр Вижинера с неизвестной длиной ключа (показать зависимость от длины ключа). Задача 2. Простым перестановочным шифром зашифрован некий текст, при этом известно, что в качестве открытого текста использован палиндром, в котором все пробелы и знаки препинания опущены. В результате шифрования получен следующий текст: МТИССЛАИЛПНАОЛМУИЛОПИТУ Необходимо: 1) Расшифровать текст, 2) Оценить, насколько можно уменьшить сложность перебора, используя информацию об исходном сообщении; 3) При программной реализации минимизировать количество возвращаемых вариантов ответа. 4) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Задача 3. Шифром простой замены зашифровано некоторое стихотворение, при этом сохранены все пробелы и знаки препинания, одинаковые символы заменены одинаковыми, а различные - различными. В результате шифрования получился следующий текст: Э рсдх ыъсг, фрьыя сяы тцорт срэдт Юрь нфурсау уцир нэръ, мрьыя Нрусиъ рнмясяэуцэяуц нурэрт, 6 Нурэрт оячолжяуц ьрорыя. 1) Расшифровать текст, 2) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Контрольная работа №2

Задача 1. Рассмотрим MAC Картера-Вегмана (Carter--Wegman MAC) ICW = (SCW,VCW), который строится на основе стойкого одноразового MAC I=(S,V) и стойкой PRF функции F(k,m). Проверочное значение tag формируется по правилу: tag = SCW((k1, k2), m) = (r, F(k1, r) S(k2, m)), r R ← {0,1} n Построить функцию верификации для проверки сообщения VCW(m,tag).

Задача 2. Предложить хэш-функцию, стойкую к коллизиям h(H,m), на основе стойкого блокового шифра E:K × {0,1} n → {0,1} n . Предложенная хэш-функция должна

отображать h:{0,1} n × {0,1} n → {0,1} n . Какое максимальное количество различных конструкций с данными свойствами вы можете предложить?

Задача 3. Будет ли стойкой к коллизиям хэш-функция, на основе стойкого блокового шифра E:K × {0,1} n → {0,1} n , следующего вида: h(H,m) = E(m,H)⊕m? Ответ обосновать.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

Цель текущего контроля: определение уровня сформированности профессиональных компетенций, знаний и навыков деятельности в области знаний, излагаемых в курсе.

Задачи текущего контроля: провести оценивание

1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;

2. степени готовности обучающегося применять теоретические и практические знания и профессионально значимую информацию, сформированности когнитивных умений.

3. приобретенных умений, профессионально значимых для профессиональной деятельности.

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением контрольных работ.

В ходе контрольной работы обучающемуся выдается КИМ с практическим перечнем из трех заданий и предлагается решить данные задания. В ходе выполнения заданий можно пользоваться любой литературой, ограничение по времени 90 минут.

Если текущая аттестация проводится в дистанционном формате, то обучающийся должен иметь компьютер и доступ в систему «Электронный университет». Если у обучающегося отсутствует необходимое оборудование или доступ в систему, то он обязан сообщить преподавателю об этом за 2 рабочих дня. На контрольную работу в дистанционном режиме отводится ограничение по времени 90 минут

При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «неудовлетворительно». «удовлетворительно», «хорошо» и «отлично», которые формируются следующим образом:

Контрольная работа №1 – «удовлетворительно» за одну правильно решенную задачу, «хорошо» за две правильно решенные задачи, «отлично» за три правильно решенные задачи.

Контрольная работа №2 – «удовлетворительно» за одну правильно решенную задачу, «хорошо» за две правильно решенные задачи, «отлично» за три правильно решенные задачи.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Перечень теоретических вопросов:

1. Предмет и задачи. Определение шифра, понятие стойкости. 2. Предположения об исходных условиях криптоанализа 3. Симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. 4. История криптографии. Криптография древности, частотный критоанализ. 5. Криптография нового времени. 6. Криптография XX века. Принцип Керкгоффса. 7. Понятие абсолютной стойкости или теоретико-информационной стойкости. Одноразовый блокнот. 8. Понятие псевдослучайности. 9. Поточные шифры. Синхронные и самосинхронизирующиеся шифры 10. Требования к поточным шифрам: Постулаты Голомба, профиль линейной сложности. 11. Методы построения больших периодов в поточных шифрах. Регистры сдвигов с линейной

обратной связью. 12. Статистические тесты. 13. Семантическая стойкость. CPA модель атаки. 14. Требования к блочным шифрам. PRP и PRF. 15. Способы построение блочных шифров: подстановки, перестановки, сети фейстеля. 16. Примеры симметричных шифров: DES, AES. 10 17. Подходы к криптоанализу: линейный, дифференциальный, «встреча посередине». 18. Режимы использования блочных шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). 19. Детерминированные и недерминированные алгоритмы шифрования. 20. Влияние случайности на стойкость. Слабости блочных шифров. 21. Контроль целостности. MAC. Определение, модель безопасности. Построение на базе Блоковых шифров. 22. HMAC. Хэш-функции. Требования к хэш-функциям. 23. Аутентифицированное шифрование. 24. CCA модель атаки. Примеры активных атак. 25. Понятие алгоритма с открытым ключом. 26. Схема RSA. Атаки на RSA. 27. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. 28. Управление ключами. Групповые ключи. Попарные ключи. Использование мастер ключей. 29. Протоколы обмена ключами. С сервером, без сервера. 30. Известные атаки на протоколы обмена ключами. 31. K-надежные схемы распределения ключей 32. Протоколы разделения секрета. 33. Пороговая криптография. 34. Протоколы цифровых денег и электронного голосования. 35. Слепая подпись. 36. Схема идентификации Schnorr – Shamir. 37. Схема идентификации Feige – Fiat – Shamir. 38. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы). 39. Понятие анонимности пользователей. Постановки задачи. PIR (протоколы конфиденциального получения информации).

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Криптографические протоколы и стандарты» проводится в форме экзамена.

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

При проведении экзамена учитываются результаты двух контрольных работ. Для получения оценки «отлично» на экзамене в конце 10 семестра у обучающегося должны иметься или оценки «отлично» по контрольным работам или студент должен решить соответствующие задачи в ходе проведения экзамена. Для получения оценки «хорошо» на экзамене у обучающегося должны иметься или оценки «хорошо» по контрольным работам или студент должен решить соответствующие задачи в ходе проведения экзамена. Для получения оценки «удовлетворительно» на экзамене у обучающегося должны иметься или оценки «удовлетворительно» по контрольным работам или студент должен решить соответствующие задачи в ходе проведения экзамена. Кроме задач студент должен ответить на один вопрос из перечня вопросов к экзамену.

При проведении экзамена учитывается выставляемая преподавателем оценка за работу в ходе лабораторных занятий.

Критерии оценивания компетенций	Шкала оценок
Обучающийся не владеет основами учебно-программного материала, обнаружил пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий.	**«Неудовлетворительно»**
Обучающийся владеет знаниями основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий,	**"Удовлетворительно"**

предусмотренных программой, знаком с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя. Оценка «удовлетворительно» выставляется, если студент знает все определения по контрольно-измерительному материалу и может решить хотя бы один практический пример	
Обучающийся полностью владеет знаниями учебно-программного материала, успешно выполнил предусмотренные в программе задания, усвоил основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному. Оценка «хорошо» выставляется студенту, если он правильно и в полном объеме ответил на все теоретические вопросы билета, но допустил погрешности в практических примерах	**"Хорошо"**
Оценка «отлично» выставляется обучающимся, обнаружившим всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоившему основную программу и знакомому с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала. Оценка «отлично» выставляется, если студент в полном объеме и правильно ответил на все вопросы контрольно-измерительного материала (как на теоретическую, так и на практическую части)	**"Отлично"**