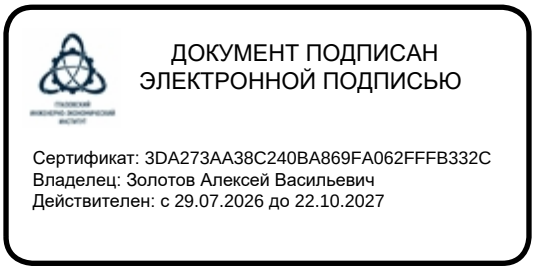
МИНОБРНАУКИ РОССИИ

Глазовский инженерно-экономический институт (филиал) Федерального государственного бюджетного образовательногоучреждения высшего образования «Ижевский государственный технический университет имени М.Т. Калашникова» (ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)





РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации

направление подготовки: **09.03.01 «Информатика и вычислительная техника»**

направленность (профиль): **Автоматизированные системы обработки информации и управления**

уровень образования: **бакалавриат**

форма обучения: **очная**

общая трудоемкость дисциплины составляет: **3 зачетные единицы**

Кафедра «Машиностроение и информационные технологии»

Составитель:

Рабочая программа составлена в соответствии с требованиями федерального государственногообразовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» и рассмотрена на заседании кафедры.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» и рассмотрена на заседании кафедры.

Протокол от 22.05.2023 г. № 5

Заведующий кафедрой  А.Г. Горбушин

22.05.2023 г.

СОГЛАСОВАНО

Количество часов рабочей программы и формируемые компетенции соответствуют учебному плану по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления».

Протокол заседания учебно-методической комиссии от 22 мая 2023 г. № 2

Председатель учебно-методической комиссии ГИЭИ

 А.Г. Горбушин

Руководитель образовательной программы  А.Г. Горбушин

22.05.2023 г.

Аннотация к дисциплине

Название дисциплины	Защита информации
Направление подготовки (специальность)	09.03.01 «Информатика и вычислительная техника»
Направленность (профиль/программа/специализация)	Автоматизированные системы обработки информации и управления
Место дисциплины	Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».
Трудоемкость (з.е. / часы)	3 з.е. / 108 часов
Цель изучения дисциплины	Формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности
Компетенции, формируемые в результате освоения дисциплины	ПК-8 Способен участвовать в разработке и эксплуатации защищенных автоматизированных систем.
Содержание дисциплины (основные разделы и темы)	Требования к построению защищенных информационных систем. Анализ угроз информационной безопасности и методология построения систем защиты информации Комплексный подход к обеспечению информационной безопасности Технологии обеспечения безопасности информации в автоматизированных системах
Форма промежуточной аттестации	Зачет (8 семестр)

1. Цели и задачи дисциплины:

Целью освоения дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности

Задачи дисциплины:

– изучение методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

– изучение методов и требований к программно- аппаратной защите информации;

– получение навыков выбора средств защиты и их применения в автоматизированных системах

2. Планируемые результаты обучения

В результате освоения дисциплины у студента должны быть сформированы

Знания, приобретаемые в ходе освоения дисциплины

№	Знания
1	Требований к построению защищенных информационных систем
2	Классификации угроз информационной безопасности
3	Основных принципов и методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

Умения, приобретаемые в ходе освоения дисциплины

№	Умения
1	Классификации автоматизированных систем с позиции обеспечения информационной безопасности
2	Выбора базового набора методов и средств защиты автоматизированной системы

Навыки, приобретаемые в ходе освоения дисциплины

№	Навыки
1	Навыки применения средств защиты информации в автоматизированных системах

Компетенции, приобретаемые в ходе освоения дисциплины

Компетенции	Индикаторы	Знания	Умения	Навыки
ПК-8 Способен участвовать в разработке и эксплуатации защищенных автоматизированных систем	ПК-8.1 Знать: современные угрозы информационной безопасности, методы и средства обеспечения безопасности в автоматизированных системах	1,2,3		
	ПК-8.2 Уметь: проводить классификацию автоматизированных систем и определять требования к построению защищенных автоматизированных систем		1,2	
	ПК-8.3 Владеть: навыками применения методов обеспечения информационной безопасности автоматизированных систем			1

3. Место дисциплины в структуре ООП

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» ООП.

Дисциплина изучается на 4 курсе в 8 семестре.

Изучение дисциплины базируется на знаниях, умениях и навыках, полученных при освоении дисциплин (модулей): «Правовые основы информационной безопасности», «Программирование», «Базы данных», «Операционные системы», «Сети и телекоммуникации».

Перечень последующих дисциплин (модулей), для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной (модулем): «Проектирование автоматизированных систем обработки информации и управления».

4. Структура и содержание дисциплины

4.1 Структура дисциплин

№ п/п	Раздел дисциплины. Форма промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы					Содержание самостоятельной работы
				контактная				СРС	
				лек	пр	лаб	КЧА		
1	2	3	4	5	6	7	8	10	11
1	Введение. Требования к построению защищенных информационных систем	22	8	2	8	2		10	[1,2] Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №1, ответам на вопросы при сдаче лабораторной работы
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	16	8	4	2	-		10	[1,2] Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №2, ответам на вопросы при сдаче лабораторной работы
3	Комплексный подход к обеспечению информационной безопасности	30	8	3	8	4		15	[1,2] Практическая работа. Подготовка к вопросам по практической работе
4	Технологии обеспечения безопасности информации в автоматизированных системах	38	8	3	6	6		23	[1,2] Подготовка к устному опросу Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №3,4, ответам на вопросы при сдаче лабораторной

									работы
	Зачет	2		–	–	–	0,3	1,7	Зачет выставляется по совокупности результатов текущего контроля успеваемости или проводится в письменной форме
	Итого:	**108**		**12**	**24**	**12**	**0,3**	**59,7**	

4.2 Содержание разделов курса и формируемых в них компетенций

№ п/п	Раздел дисциплины	Коды компетенции и индикаторов	Знания	Умения	Навыки	Форма контроля
1	Введение. Требования к построению защищенных информационных систем	ПК 8.1, ПК 8.2	1	1,2	1	Практическая работа. Выполнение лабораторной работы, ответы на вопросы при сдаче работы
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	ПК 8.1, ПК 8.2	2,3	1,2	1	Устный опрос Практическая работа Тест
3	Комплексный подход к обеспечению информационной безопасности	ПК 8.1, ПК 8.2, ПК 8.3	2,3	1,2	1	Практическая работа, лабораторная работа, ответ на вопросы при сдаче работы
4	Технологии обеспечения безопасности информации в автоматизированных системах	ПК 8.2, ПК 8.3	2,3	1,2	1	Устный опрос Практическая работа Выполнение лабораторной работы, ответ на вопросы при сдаче работы

4.3 Наименование тем лекций, их содержание и объем вчасах

№ п/п	№ раздела дисциплины	Наименование лекций	Трудоемкость (час)
1.	1	Основные принципы обеспечения информационной безопасности. Методы и инструменты обеспечения информационной безопасности	1
2.	1	Классификация информационных систем по требованиям безопасности. Общий подход к построению защищенных информационных систем	1
3.	2	Анализ угроз информационной безопасности. Модель угроз информационной безопасности	1
4.	2	Каналы утечки информации. Классификация компьютерных вирусов.	1
5.	2	Методы разграничения доступа к информации. Дискреционный и мандатный принципы разграничения доступа	1
6.	2	Лицензирование, сертификация в области информационной безопасности. Понятие аттестации объектов информатизации	1

7.	3	Комплексное обеспечение информационной безопасности. Организационные и правовые методы обеспечения информационной безопасности. Политика информационной безопасности	1
8.	3	Криптографические методы защиты информации.	2
9.	4	Программно-аппаратные средства защиты информации. Методы идентификации и аутентификации.	2
10	4	Электронная подпись и функция хэширования. Стандарты цифровой подписи	1
	Всего		**12**

4.4 Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоемкость (час)
1.	1	Классификация информационных систем. Классификация информационных систем персональных данных (ИСПДН). Анализ базовых требований к защите ИСПДН.	4
2.	1	Классификация государственных информационных систем (ГИС), систем КИИ. Требования к защите ГИСи КИИ систем	4
3.	2	Анализ угроз информационной безопасности	2
4.	3	Криптографические алгоритмы защиты информации.	4
5.	3	Алгоритм цифровой подписи. Алгоритмы хэш-функций. Стандарты РФ на криптографические алгоритмы	2
6.	3	Анализ и подбор сертифицированных средств защиты информации	2
7.	4	Программно-аппаратные средства защиты информации от НСД	6
	Всего		**24**

4.5 Наименование тем лабораторных работ, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Трудоемкость (час)
1.	1	Классификация информационным системам персональных данных. Набор базовых методов по защите персональных данных. Акт классификации ИСПДн	2
2.	3	Методы шифрования	4
3.	4	Цифровые сертификаты. Установка, настройка программного обеспечения криптопровайдеров.	6
	Всего		**12**

5. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по дисциплине:

- защиты лабораторных работ
- практические работы
- тест
- зачет

Примечание: оценочные материалы (типовые варианты тестов, контрольных работ и

др.) приведены в приложении к рабочей программе дисциплины.

Промежуточная аттестация по итогам освоения дисциплины – зачет

6. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

б) дополнительная литература:

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72345.html

в) методические указания:

Стукалина Е.Ф. Макровирусы. Учебно-методическое пособие по выполнению лабораторных и самостоятельных работ по дисциплине «Защита информации»

г) перечень ресурсов информационно-коммуникационной сети Интернет:

1. Электронно-библиотечная система IPRbookshttp://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks.
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова Web ИРБИС http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN= IBIS.
3. Национальная электронная библиотека –http://нэб.рф.
4. Мировая цифровая библиотека – http://www.wdl.org/ru/.
5. Международный индекс научного цитирования WebofScience – http://webofscience.com.
6. Научная электронная библиотека eLIBRARY.RU – https://elibrary.ru/defaultx.asp.
7. Справочно-правовая система КонсультантПлюсhttp://www.consultant.ru/.

д) лицензионное и свободно распространяемое программное обеспечение:

1. Офисный пакет MS Office
2. Пакет VeraCrypt

7. Материально-техническое обеспечение дисциплины:

1. Лекционные занятия.

Учебные аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

2. Практические занятия.

Для практических занятий используются аудитория № 204, оснащенная следующим

оборудованием: Компьютеры с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде ИжГТУ имени М.Т. Калашникова

3. Лабораторные работы.

Для лабораторных занятий используются аудитория №209, оснащенная следующим оборудованием: доской, компьютерами с возможностью подключения к сети «Интернет», столами, стульями.

4. Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде ИжГТУ имени М.Т. Калашникова:

- научная библиотека ИжГТУ имени М.Т. Калашникова;
- помещение для самостоятельной работы обучающихся.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

Оценочные средства по дисциплине

Защита информации
наименование – полностью

направление 09.03.01 «Информатика и вычислительная техника»
код, наименование – полностью

профиль Автоматизированные системы обработки информации и управления
наименование – полностью

уровень образования: бакалавриат

форма обучения: очная
очная/очно-заочная/заочная

общая трудоемкость дисциплины составляет: 3 зачетные единицы

1. Оценочные средства

Оценивание формирования компетенций производится на основе результатов обучения, приведенных в п. 2 рабочей программы и ФОС. Связь разделов компетенций, индикаторов и форм контроля (текущего и промежуточного) указаны в таблице 4.2 рабочей программы дисциплины.

Оценочные средства соотнесены с результатами обучения по дисциплине и индикаторами достижения компетенций, представлены ниже.

№ п/п	Коды компетенции и индикаторов	Результат обучения *(знания, умения и навыки)*	Формы текущего и промежуточного контроля
1	ПК-8.1 Знать: современные угрозы информационной безопасности, методы и средства обеспечения безопасности в автоматизированных системах	З1.Требований к построению защищенных информационных систем З2.Классификации угроз информационной безопасности З3.Основных принципов и методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы	Ответ на вопросы по практической работе, защита лабораторной работы №1,2 тест зачет
2	ПК-8.2 Уметь: проводить классификацию автоматизированных систем и определять требования к построению защищенных автоматизированных систем	У1. Классификации автоматизированных систем с позиции обеспечения информационной безопасности У2.Выбора базового набора методов и средств защиты автоматизированной системы	Ответ на вопросы по практической работе, защита лабораторной работы №1,2, устный опрос, зачет
3	ПК-8.3 Владеть: навыками применения методов обеспечения информационной безопасности автоматизированных систем	Н1.Навыки применения средств защиты информации в автоматизированных системах	Ответ на вопросы по практической работе, защита лабораторной работы №3, устный опрос, зачет

Типовые задания для оценивания формирования компетенций

Наименование: зачет
Представление в ФОС:
Перечень вопросов для проведения зачета:

1. Понятие «информационной безопасности». Составляющие информационной безопасности. Классификация методов защиты информации. Организации - регуляторы в области ИБ.
2. Законодательство в области защиты персональных данных. Категории персональных данных. Специальная категория данных. Угрозы 1,2,3 типа при классификации персональных данных. Какая информация должна содержаться в согласии субъекта на обработку персональных данных.

3. Классификация информационных систем персональных данных (ИСПДн) и характеристика базового набора мер защиты по требованиям регуляторов
4. Классификация государственных информационных систем (ГИС) и характеристика базового набора мер защиты по требованиям регуляторов
5. Классификация систем КИИ (критической информационной инфраструктуры) и характеристика базового набора мер защиты по требованиям регуляторов
6. Угрозы ИБ. Каналы утечки информации.
7. Понятие модели угроз. Общие принципы построения модели угроз для информационных систем персональных данных. (Примеры)
8. Классификация компьютерных вирусов по деструктивным возможностям.
9. Виды "вирусоподобных" программ. Поясните механизм функционирования "троянской программы", «логической бомбы», макровируса
10. Классификация криптографических систем. Преимущества и недостатки. Требования к криптографическим системам
11. Назовите наиболее известные криптографические отечественные и зарубежные алгоритмы и дайте им краткую характеристику.
12. Методы защиты от НСД (несанкционированного доступа). Программно-аппаратные способы защиты от НСД
13. Матрица доступа принципы составления. Примеры
14. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем. . Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
15. Биометрические средства идентификации и аутентификации пользователей.
16. Аутентификация субъектов в распределенных системах. Метод одноразовых паролей, метод рукопожатия
17. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
18. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
19. Законодательный уровень применения цифровой подписи. Понятие и применение сертификата.

Критерии оценки:
Приведены в разделе 2

Наименование: защита лабораторных работ
***Представление в ФОС*:** задания и требования к выполнению представлены в методических указаниях по дисциплине
Варианты заданий:
Классификация информационным системам персональных данных.
Набор базовых методов по защите персональных данных.
Акт классификации ИСПДн
Методы шифрования
Цифровые сертификаты.
Установка, настройка программного обеспечения криптопровайдеров.

Критерии оценки:
Приведены в разделе 2

Наименование: устный опрос
***Представление в ФОС*:** перечень заданий или вопросов
Варианты заданий:
- Перечислите проблемы парольной аутентификации
- Опишите алгоритм аутентификации сервера на основе одноразовых паролей

- Опишите основную идею алгоритма аутентификации Kerberos

Критерии оценки:
Приведены в разделе 2

Наименование: практические работы
***Представление в ФОС*:** набор вариантов заданий
Варианты заданий:
- Перечислите законодательство в области защиты персональных данных
- Дайте определение и приведите примеры "Объектов критической инфраструктуры"
- Опишите роль следующих организаций в области ЗИ: ФСТЭК, ФСБ, АНБ
- Провести анализ уязвимостей MS OFFICE. Макровирусы среда распространения и методы защиты
- Найти и проанализировать методические документы на сайте регулятора ИБ www.fstec.ru.
- Опишите назначение и приведите примеры программно-аппаратных средств защиты информации

Критерии оценки:
Приведены в разделе 2

Наименование: тест
Представление в ФОС: набор тестов по разделам дисциплины
Варианты тестов:

1) Методами защиты информации являются:

1) правовые
2) военные
3) политические
4) организационные
5) радиотехнические
6) программно-технические
7) разведывательные
8) криптографические

2) Основными задачами информационной безопасности являются:
1) Обеспечение доступности информации
2) Обеспечение конфиденциальности информации
3) Подтверждение неотказуемости обработки данных
4) Обеспечение целостности информации
5) Обеспечение своевременности обработки данных

3) «Аутентификация» это_____

4) Угроза типа SQL инъекция в БД связана с:
1) С внедрением произвольной строки в SQL запрос
2) С использованием типовой учетной записи БД
3) С использованием большого объема, обрабатываемых данных в БД

5) Керберос это алгоритм (протокол) для:
1) Подтверждения подлинности клиента серверу в открытой сети
2) Для хранения секретных ключей сервера

3) Для хранения сертификатов клиентских машин

6) Информационные системы персональных даных (ИСПДн) по требованиям безопасности классифицируются по _____

7) Установка криптопровайдера (CSP) означает, что в системе установлен модуль _____

8) Какие механизмы информационной безопасности применяются в защищенных автоматизированных системах?
1) аутентификация;
2) шифрование;
3) авторизация;
4) устранение избыточности данных;
5) фильтрация данных

9) Системы шифрования бывают:
1) симметричные
2) ассиметричные
3) обратные
4) диагональные

10) Если K1 – ключ симметричной криптосистемы, а K2 – секретный ключ ассиметричной криптосистемы, то для функция длины строки Len() справедливо:
1) $\mathrm{Len(K1)} \approx \mathrm{Len(K2)}$
2) $\mathrm{Len\ (K1)} \ll \mathrm{Len(K2)}$
3) $\mathrm{Len(K1)} \gg \mathrm{Len(K2)}$

11) **Какими свойствами обладает хэш-функция_____**

Критерии оценки:
Приведены в разделе 2

Наименование: оценочные материалы для оценки уровня сформированности компетенций
Представление в ФОС: перечень заданий
1) Методами защиты информации являются:
1) правовые
2) военные
3) политические
4) организационные
5) радиотехнические
6) программно-технические
7) разведывательные
8) криптографические

2) Основными задачами информационной безопасности являются:
1) Обеспечение доступности информации
2) Обеспечение конфиденциальности информации
3) Подтверждение неотказуемости обработки данных
4) Обеспечение целостности информации

5) Обеспечение своевременности обработки данных

3) Какое определение соответствует термину «Аутентификация»?

1) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;
2) распознавание имени объекта;
3) подтверждение того, что предъявленное имя соответствует объекту;
4) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;
5) правильного определения нет

4) Угроза типа SQL инъекция в БД связана с:

1) С внедрением произвольной строки в SQL запрос
2) С использованием типовой учетной записи БД
3) С использованием большого объема, обрабатываемых данных в БД

5) Керберос это алгоритм (протокол) для:

1) Подтверждения подлинности клиента серверу в открытой сети
2) Для хранения секретных ключей сервера
3) Для хранения сертификатов клиентских машин

6) Установка криптопровайдера (CSP) позволяет:

1) Осуществлять проверку сертификата ЭП (электронной подписи)
2) Формировать контейнер для хранения криптографических ключей пользователя
3) Осуществлять шифровальные операции в ОС

7) Какие механизмы информационной безопасности применяются в защищенных автоматизированных системах?

1) аутентификация;
2) шифрование;
3) авторизация;
4) устранение избыточности данных;
5) фильтрация данных

8) Системы шифрования бывают:

1) симметричные
2) ассиметричные
3) обратные
4) диагональные

9) Если K1 – ключ симметричной криптосистемы, а K2 – секретный ключ ассиметричной криптосистемы, то для функция длины строки Len() справедливо:

1) $\mathrm{Len(K1)} \approx \mathrm{Len(K2)}$
2) $\mathrm{Len\ (K1)} \ll \mathrm{Len(K2)}$
3) $\mathrm{Len(K1)} \gg \mathrm{Len(K2)}$

10) **Какими свойствами должна обладать хэш-функция (несколько верных ответов)?**

1) Строго фиксированный размер
2) Свойство обратимости
3) Свойство необратимости

2. Критерии и шкалы оценивания

Для контрольных мероприятий (текущего контроля) устанавливается минимальное

и максимальное количество баллов в соответствии с таблицей. Контрольное мероприятие считается пройденным успешно при условии набора количества баллов не ниже минимального.

Результат обучения по дисциплине считается достигнутым при успешном прохождении обучающимся всех контрольных мероприятий, относящихся к данному результату обучения.

Разделы дисциплины	***Форма контроля***	***Количество баллов***	
		min	***max***
1	Выполнение практической работы, ответ на вопросы	5	9
1	Выполнение практической работы, ответ на вопросы	5	9
1	Выполнение лабораторной работы №1, ответ на вопросы	5	9
2	Выполнение практической работы, ответ на вопросы	5	9
3	Выполнение практической работы, ответ на вопросы	5	9
3	Выполнение практической работы, ответ на вопросы	5	9
3	Выполнение лабораторной работы №2, ответ на вопросы	5	9
4	Выполнение практической работы, ответ на вопросы	8	12
4	Выполнение лабораторной работы №3, ответ на вопросы	8	13
4	Устный опрос	9	12
	Итого	**60**	**100**

При оценивании результатов обучения по дисциплине в ходе текущего контроля успеваемости используются следующие критерии. Минимальное количество баллов выставляется обучающемуся при выполнении всех показателей, допускаются несущественные неточности в изложении и оформлении материала.

Наименование, обозначение	***Показатели выставления минимального количества баллов***
Практическая работа	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий. На защите практической работы даны правильные ответы не менее чем на 50% заданных вопросов
Лабораторная работа	Лабораторная работа выполнена в полном объеме; Продемонстрирован удовлетворительный уровень владения материалом при защите лабораторной работы, даны правильные ответы не менее чем на 50% заданных вопросов
Устный опрос	Даны правильные ответы не менее чем на 50% заданных вопросов. Продемонстрированы знания основного учебно-программного материала

Промежуточная аттестация по дисциплине проводится в форме зачета.

Итоговая оценка по дисциплине может быть выставлена на основе результатов текущего контроля с использованием следующей шкалы:

Оценка	***Набрано баллов***
«зачтено»	60-100
«не зачтено»	Менее 60

Если сумма набранных баллов менее 60 – обучающийся не допускается до промежуточной аттестации.

Если сумма баллов составляет от 60 до 100 баллов, обучающийся допускается до зачета.

При оценивании результатов обучения по дисциплине в ходе промежуточной аттестации

используются следующие критерии и шкала оценки:

Оценка	***Критерии оценки***
«зачтено»	Обучающийся демонстрирует знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы, умеет применять его при выполнении конкретных заданий, предусмотренных программой дисциплины
«не зачтено»	Обучающийся демонстрирует значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение