Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.О.39

Программно-аппаратные средства защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 80
самостоятельная работа 28
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	15 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	16	16	16	16
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Консультации перед экзаменом	1	1	1	1
В том числе в форме практ.подготовки	18	18	18	18
Итого ауд.	80	80	80	80
Контактная работа	81,3	81,3	81,3	81,3
Сам. работа	28	28	28	28
Часы на контроль	34,7	34,7	34,7	34,7
Итого	144	144	144	144

Программу составил(и):
к.т.н., доцент кафедры Математики и вычислительной техники, Капустин С.А.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Программно-аппаратные средства защиты информации

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целями освоения учебной дисциплины «Программно-аппаратные средства защиты информации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.
Задачи: Ознакомление с основными терминами и определениями. Ознакомление с основными типами угроз и атак. Модели разграничения доступа к защищаемой информации. Эксплуатация программно-аппаратных средств защиты информации.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Администрирование сетей
2.1.3	Безопасность компьютерных сетей
2.1.4	Безопасность операционных систем
2.1.5	Сети и телекоммуникации
2.1.6	Аппаратные средства вычислительной техники
2.1.7	Методы и средства криптографической защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информационных процессов в компьютерных системах
2.2.2	Основы управления информационной безопасностью
2.2.3	Специализированные вычислительные устройства защиты информации
2.2.4	Выполнение и защита выпускной квалификационной работы
2.2.5	Комплексная защита объектов информатизации
2.2.6	Производственная практика: Технологическая практика
2.2.7	Производственная практика: Преддипломная практика
2.2.8	Производственная практика: Эксплуатационная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	
ОПК-10.1: Реализует требования политик безопасности на объектах информатизации	
Знать	
Уровень 1	Знает требования политик безопасности на объектах информатизации, но реализует с ошибками
Уровень 2	Знает требования политик безопасности на объектах информатизации, но реализует с незначительными ошибками
Уровень 3	Знает требования политик безопасности на объектах информатизации, реализует без ошибок
ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	
Уметь	
Уровень 1	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, но допускает ошибки
Уровень 2	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, но допускает незначительные ошибки
Уровень 3	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности без ошибок
ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	
Владеть	
Уровень 1	Выполняет настройку средств защиты информации с ошибками
Уровень 2	Выполняет настройку средств защиты информации с незначительными ошибками
Уровень 3	Выполняет настройку средств защиты информации без ошибок

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	
ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
Знать	
Уровень 1	Знает информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, но допускает ошибки в их определении
Уровень 2	Знает информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, но допускает незначительные ошибки в их определении
Уровень 3	Знает информационную инфраструктуру и информационные ресурсы организации, подлежащие защите,определяет их без ошибок
ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
Уметь	
Уровень 1	Умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, но допускает ошибки
Уровень 2	Умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, но допускает незначительные ошибки
Уровень 3	Умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, ошибок не допускает
ОПК-12.3: Оценивает информационные риски в автоматизированных системах	
Владеть	
Уровень 1	Оценивает информационные риски в автоматизированных системах, но допускает ошибки в оценке
Уровень 2	Оценивает информационные риски в автоматизированных системах, но допускает незнаяительные ошибки в оценке
Уровень 3	Оценивает информационные риски в автоматизированных системах,, ошибок не допускает
ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	
Уметь	
Уровень 1	Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений, но допускает ошибки
Уровень 2	Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений, но допускает незначительнвые ошибки
Уровень 3	Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений, ошибок не допускает

ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	
ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем	
Знать	
Уровень 1	Знает подлежащие защите информационные ресурсы автоматизированных систем, но допускает ошибки при их определении
Уровень 2	Знает подлежащие защите информационные ресурсы автоматизированных систем, но допускает незначительные ошибки при их определении
Уровень 3	Знает подлежащие защите информационные ресурсы автоматизированных систем, при их определении ошибок не допускает
ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	
Уметь	
Уровень 1	Умеет составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, но допускает ошибки
Уровень 2	Умеет составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, но допускает незначительные ошибки
Уровень 3	Умеет составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, ошибок не допускает
ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации	
Владеть	
Уровень 1	Организацией работы персонала автоматизированной системы с учетом требований по защите информации, но допускает ошибки
Уровень 2	Организацией работы персонала автоматизированной системы с учетом требований по защите информации,

	но допускает незначительные ошибки
Уровень 3	Организацией работы персонала автоматизированной системы с учетом требований по защите информации, ошибок не допускает
ОПК-4.1.4: Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	
Уметь	
Уровень 1	Умеет подготавливать документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, но допускает ошибки
Уровень 2	Умеет подготавливать документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, но допускает незначительные ошибки
Уровень 3	Умеет подготавливать документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, ошибок не допускает

ОПК-4.3: Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	
ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы	
Знать	
Уровень 1	Знает порядок автономной наладки технических и программных средств системы защиты информации автоматизированной системы, но допускает ошибки
Уровень 2	Знает порядок автономной наладки технических и программных средств системы защиты информации автоматизированной системы, но допускает незначительные ошибки
Уровень 3	Знает порядок автономной наладки технических и программных средств системы защиты информации автоматизированной системы, ошибок не допускает
ОПК-4.3.2: Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	
Уметь	
Уровень 1	Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах, но допускает ошибки
Уровень 2	Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах, но допускает незначительные ошибки
Уровень 3	Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах, ошибок не допускает
ОПК-4.3.3: Устраняет известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	
Владеть	
Уровень 1	Способами устранения известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации, но допускает ошибки
Уровень 2	Способами устранения известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации, но допускает незначительные ошибки
Уровень 3	Способами устранения известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации, ошибок не допускает

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Тема 1. Введение. Основные понятия. Требования руководящих документов по защите информации					

1.1	Основные понятия. Требования руководящих документов по защите информации /Лек/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
1.2	Требования РД по ЗИ /Пр/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
1.3	/Ср/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
	Раздел 2. Тема 2. Модели разграничения доступа					
2.1	Модели разграничения доступа /Лек/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	

2.2	Дискреционная модель разграничения доступа /Пр/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
2.3	Мандатная модель разграничения доступа /Лаб/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	4
2.4	Ролевая модель разграничения доступа /Лаб/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	4
2.5	/Ср/	7	8	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
	Раздел 3. Тема 3. Идентификация и аутентификация пользователей					

3.1	Идентификация и аутентификация пользователей /Лек/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
3.2	Идентификация и аутентификация пользователей /Пр/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
3.3	Идентификация и аутентификация пользователей /Лаб/	7	8	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	2
3.4	/Ср/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
	Раздел 4. Тема 4. Программно-аппаратные средства шифрования					

4.1	Программно-аппаратные средства шифрования /Лек/	7	8	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
4.2	Программно-аппаратные средства шифрования /Лаб/	7	8	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
4.3	/Ср/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
	Раздел 5. Тема 5. Электронная подпись					
5.1	Электронная подпись /Лек/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	

5.2	Электронная подпись /Лаб/	7	8	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	8
5.3	Электронная подпись /Пр/	7	4	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
5.4	/Ср/	7	6	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	
	Раздел 6. Промежуточная аттестация					
6.1	Консультация /Консл/	7	1	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	

6.2	Экзамен /КАЭ/	7	0,3	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3 ОПК-4.1.4 ОПК-4.3.1 ОПК-4.3.2 ОПК-4.3.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.7 Л1.8Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Общие принципы построения подсистемы защиты компьютерной системы
2. Перечень основных функций подсистемы безопасности защищенной компьютерной системы
3. Основные требования к подсистеме разграничения доступа
4. Избирательное разграничение доступа
5. Полномочное разграничение доступа
6. Разграничение доступа в Windows
7. Дескриптор защиты объекта
8. Разграничение доступа в Linux
9. Объекты, субъекты, методы и права доступа в Linux
10. Формат атрибутов защиты объекта доступа Linux
11. Механизмы идентификации
12. Механизмы аутентификации
13. Аутентификация с использованием внешних носителей информации
14. Биометрическая аутентификация
15. Архитектура подсистемы аутентификации Windows
16. Аутентификация в Linux.
17. Компьютерные вирусы.

5.2. Темы письменных работ

1. Принципы программно-аппаратных средств защиты информации
2. Симметричное и асимметричное шифрование в программно-аппаратных средствах защиты информации
3. Биометрические технологии и их роль в обеспечении безопасности информации
4. Аппаратная защита информации на уровне микропроцессора
5. Программное обеспечение для защиты информации на серверах
6. Защита информации при передаче по сети: роль программно-аппаратных средств
7. Возможности и ограничения программно-аппаратных систем контроля и анализа трафика
8. Защита информации на уровне операционной системы: программные и аппаратные средства
9. Технологии контроля и обнаружения вторжений в программах и аппаратуре
10. Роль программно-аппаратных средств в обеспечении цифровой подписи и электронного документооборота
11. Программно-аппаратные средства защиты информации в облачных вычислениях
12. Программное обеспечение для анализа уязвимостей и сканирования информационных систем
13. Аппаратно-программные комплексы для защиты информации в электронной коммерции
14. Программно-аппаратные средства обнаружения и предотвращения атак типа DDoS
15. Защита информации от вредоносного программного обеспечения: программные и аппаратные средства
16. Возможности и ограничения программно-аппаратных средств контроля доступа в информационных системах
17. Аппаратные средства аутентификации и управления доступом
18. Защита информации в сетях Wi-Fi: программно-аппаратные средства
19. Программно-аппаратные средства защиты информации от утечек данных
20. Роль программно-аппаратных средств в обнаружении и борьбе с социальной инженерией

5.3. Фонд оценочных средств

1. Общие принципы построения подсистемы защиты компьютерной системы
2. Перечень основных функций подсистемы безопасности защищенной компьютерной системы
3. Основные требования к подсистеме разграничения доступа
4. Избирательное разграничение доступа
5. Полномочное разграничение доступа
6. Разграничение доступа в Windows
7. Дескриптор защиты объекта
8. Разграничение доступа в Linux
9. Объекты, субъекты, методы и права доступа в Linux

10. Формат атрибутов защиты объекта доступа Linux
11. Механизмы идентификации
12. Механизмы аутентификации
13. Аутентификация с использованием внешних носителей информации
14. Биометрическая аутентификация
15. Архитектура подсистемы аутентификации Windows
16. Аутентификация в Linux.
17. Компьютерные вирусы.

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.2	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814
Л1.3	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909
Л1.4	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020, URL: http://znanium.com/catalog/document?id=358722
Л1.5	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=361143
Л1.6	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=364911
Л1.7	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2022, URL: https://znanium.com/catalog/document?id=393765
Л1.8	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум + еПриложение: Учебное пособие	Москва: КноРус, 2023, URL: https://book.ru/book/949452

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2021, URL: https://book.ru/book/938255
Л2.2	Конюх В.Л.	Проектирование автоматизированных систем производства: Учебное пособие	Москва: ООО "КУРС", 2019, URL: https://znanium.com/catalog/document?id=355804
Л2.3	Семеновых В.И., Перминов А.А.	Проектирование автоматизированных систем: Учебное пособие	Вологда: Инфра-Инженерия, 2022, URL: https://znanium.com/catalog/document?id=417415
Л2.4	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2022, URL: https://book.ru/book/944006

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Электронная библиотечная система Ibooks. - Режим доступа: http://www.ibooks.ru
Э2	Электронная библиотечная система Znanium. - Режим доступа: http://znanium.com
Э3	Электронная библиотечная система BOOK.ru. - Режим доступа: http://www.book.ru
Э4	Единое окно доступа к образовательным ресурсам. - Режим доступа: http://window.edu.ru

Э5	Техническая документация Windows для разработчиков и ИТ-специалистов. - Режим доступа: https://docs.microsoft.com/ru-RU/windows
Э6	Интернет университет информационных технологий ИНТУИТ. - Режим доступа: https://www.intuit.ru/studies/courses
Э7	Электронные ресурсы Академии ИМСИТ. - Режим доступа: http://eios.imsit.ru
Э8	Справочный центр Astra Linux. - Режим доступа: https://wiki.astralinux.ru
Э9	База знаний Astra. - Режим доступа: https://wiki.astralinux.ru/kb
Э10	Совет Безопасности Российской Федерации. - Режим доступа: http://www.scrf.gov.ru
Э11	Информационно-правовой портал ГАРАНТ.РУ. - Режим доступа: https://www.garant.ru
Э12	Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». - Режим доступа: https://docs.cntd.ru
Э13	Федеральная служба по техническому и экспортному контролю. - Режим доступа: https://fstec.ru
Э14	Консультант Плюс. - Режим доступа: http://www.consultant.ru
Э15	Криптографическая защита информации . - Режим доступа: https://znanium.com/catalog/product/1899016
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.3	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.1.5	Notepad++. Тектовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL
6.3.1.6	Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.7	Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL
6.3.1.8	Adobe Reader DC Adobe Acrobat — пакет программ, предназначенный для создания и просмотра электронных публикаций в формате PDF Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017
6.3.1.9	Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)
6.3.1.10	Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.11	10-Страйк Сканирование Сети Сканирование Сети - программа-сканер TCP-портов и IP-адресов Лицензионный сертификат от 01.01.2011
6.3.1.12	Traffic inspector Special Unlimited ОРГАНИЗАЦИЯ ДОСТУПА В ИНТЕРНЕТ. NAT, ПРОКСИ-СЕРВЕР, VPN, AD Лицензионный договор №649 от 23.09.2019
6.3.1.13	Astra Linux Операционная система семейства Linux. Версия "Орел" Программное обеспечение по лицензии GNU GPL
6.3.1.14	Secren Net LSP Средство защиты информации от несанкционированного доступа для операционных систем семейства Linux Договор №КБ/04085/1/11 от 14.02.2022
6.3.1.15	Astra Linux Special Edition Операционная система Astra Linux Special Edition "Смоленск" Лицензионный договор №А-2023-3968-ВУЗ 08 августа 2023 г.
6.3.1.16	Secren Net Studio Единая система управление продуктами для защиты Windows, Linux и платами доверенной загрузки Договор №КБ/04085/1/11 от 14.02.2022
6.3.1.17	PostgreSQL Система управления базами данных Программное обеспечение по лицензии GNU GPL
6.3.1.18	vGate Средство микросегментации и защиты жизненного цикла виртуальных машин Договор №КБ/04085/1/11 от 14.02.2022
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Портал выбора технологий и поставщиков http://www.tadviser.ru
6.3.2.2	Проект IDEF.ru http://idef.ru
6.3.2.3	Консультант Плюс http://www.consultant.ru
6.3.2.4	Global CIO Официальный портал ИТ-директоров http://www.globalcio.ru
6.3.2.5	ARIS BPM Community https://www.ariscommunity.com
6.3.2.6	ABOUT THE UNIFIED MODELING LANGUAGE SPECIFICATION https://www.omg.org/spec/UML
6.3.2.7	ИСО Международная организация по стандартизации https://www.iso.org/ru/home.html
6.3.2.8	РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии https://www.gost.ru/portal/gost/

6.3.2.9	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)			
Ауд	Наименование	ПО	Оснащение
114а	Лаборатория программно-аппаратных средств защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
121	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Программно-аппаратные средства защиты информации». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.
Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем.
Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося

Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные
источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Основными задачами самостоятельной работы студентов, являются: во–первых, продолжение изучения дисциплины в домашних условиях по программе, предложенной преподавателем; во–вторых, привитие студентам интереса к технической и математической литературе, инженерному делу. Изучение и изложение информации, полученной в результате изучения научной литературы и практических материалов, предполагает развитие у студентов как владения навыками устной речи, так и способностей к четкому письменному изложению материала.
Основной формой контроля за самостоятельной работой студентов являются практические занятия, а также еженедельные консультации преподавателя.
Практические занятия – наиболее подходящее место для формирования умения применять полученные знания в практической деятельности.
При подготовке к практическим занятиям следует соблюдать систематичность и последовательность в работе. Необходимо сначала внимательно ознакомиться с содержанием плана практических занятий. Затем, найти в учебной литературе соответствующие разделы и прочитать их. Осваивать изучаемый материал следует по частям. После изучения какой-либо темы или ее отдельных разделов необходимо полученные знания привести в систему, связать воедино весь проработанный материал.
При подведении итогов самостоятельной работы преподавателем основное внимание должно уделяться разбору и оценке лучших работ, анализу недостатков. По предложению преподавателя студент может изложить содержание выполненной им письменной работы на практических занятиях.