МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программно-аппаратные средства защиты информации

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения 2021
Изучается в 5-6 семестре

г. Пятигорск 20__ **г.**

1. Цели и задачи освоения дисциплины

Целью дисциплины «Программно-аппаратные средства защиты информации» является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств; содействие развитию системного мышления.

Задачами дисциплины являются: дать основы о методах и средствах защиты информации в компьютерных системах; дать основы правил разграничения доступа и основных функций СЗИ, его обеспечивающих; дать основы практических аспектов построения систем ограничения доступа и других СЗИ; дать основы аппаратной реализации различных средств защиты информации; дать основы о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД); дать основы вопросов защиты ПО от несанкционированного использования; дать основы о применении средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности; дать основы методов защиты от РПВ; дать основы методов и особенностей защиты объектов ОС; дать основы принципов построения файловой системы и моделей разграничения доступа к объектам.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к профессиональному циклу Б.1 (базовой части) ОП ВО подготовки бакалавра направления 10.03.01 «Информационная безопасность». Ее освоение происходит в 6 семестре.

3. Связь с предшествующими дисциплинами

Пререквизитами являются дисциплины:

- Теоретические основы защиты информации;
- Объектно-ориентированное программирование;
- Аппаратные средства вычислительной техники;
- Сетевые технологии CISCO.

4. Связь с последующими дисциплинами

Кореквизитами являются дисциплины:

- Программно-аппаратные комплексы защиты объектов информатизации;
- Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

5. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

5.1 Наименование компетенции

Код	Формулировка:
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты;
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

5.2 Знания, умения и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: информационные ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципы и методы информационной и организационной защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; **Уметь:** определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; применять принципы и методы информационной и организационной защиты информации; использовать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; **Владеть:** способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципами и методами информационной и организационной защиты информации; навыками использования принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;	**ОПК-7**
Знать: работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение; технологию работы на ПК в современных операционных средах; назначение и возможности прикладных программных продуктов; **Уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; выбирать архитектуру ПК, аппаратное обеспечение; применять технологию работы на ПК в современных операционных средах;	**ПК-1**

использовать возможности прикладных программных продуктов; **Владеть:** способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах; основными методами и средствами прикладных программных продуктов;	
Знать: правила разработки и оформления технической документации и установленной отчетности по утвержденным формам; правила сертификации технических средств, систем, процессов, оборудования и материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования; алгоритмы растрирования и геометрические преобразования; **Уметь:** формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты; представлять технические решения с использованием программных средств компьютерной графики и геометрического моделирования. **Владеть:** навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ; навыками разработки проектной и конструкторской документации в соответствии с требованиями стандартов; навыками работы на компьютерной технике с графическими пакетами для получения конструкторских, технологических и других документов; опытом выполнения проектов с учетом специфики направления подготовки.	**ПК-2**
Знать: основы администрирования вычислительных сетей; подсистемы информационной безопасности объекта защиты; операционные системы персональных ЭВМ; системы управления базами данных; принципы построения информационных систем; **Уметь:** применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты; пользоваться операционными системами персональных ЭВМ; анализировать системы управления базами данных; применять принципы построения информационных систем; **Владеть:** основами администрирования вычислительных сетей; способностью администрировать подсистемы информационной безопасности объекта защиты; операционными системами персональных ЭВМ; способностью управления базами данных; методами и принципами построения информационных систем;	**ПК-3**
Знать: основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; **Уметь:** использовать основные методы в работах по реализации политики информационной безопасности; применять комплексный	**ПК-4**

подход к обеспечению информационной безопасности объекта защиты; применять принципы организации информационных систем в соответствии с требованиями по защите информации; отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; **Владеть:** способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной безопасности объекта защиты; принципами организации информационных систем в соответствии с требованиями по защите информации; возможностью отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	

6. Объем учебной дисциплины/модуля

	Астр. часов	
Объем занятий: Итого	81 ч.	3 з.е.
В том числе аудиторных	36 ч.	
Из них:		
Лекций	12 ч.	
Лабораторных работ	12 ч.	
Практических занятий	12 ч.	
Самостоятельной работы	45 ч.	
Зачет с оценкой	6 семестр	

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
6 семестр							
1	Тема 1. **Предмет и задачи программно-**	ОПК-7; ПК-1;	1,5	1,5	-		4,5

	аппаратной защиты информации. Роль и назначение курса в подготовке специалистов по защите информации. Место курса среди других дисциплин учебного плана. Понятие безопасности информации. Вычислительная и операционная среда – пассивная и активная сущность компьютерной системы. Объект защиты в КС. Основные и обеспечивающие функции СЗИ.	ПК-2; ПК-3; ПК-4					
2	Тема 2. **Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.** Идентификация, аутентификация, авторизация субъекта доступа. Идентифицирующая информация. Классификация подсистем идентификации и аутентификации пользователей. Протоколы аутентификации. Парольные подсистемы идентификации и аутентификации пользователей, их достоинства и недостатки. Минимальные требования к выбору пароля и подсистемам парольной идентификации и аутентификации. Количественная оценка стойкости парольной защиты.	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	1,5	-		4,5
3	Тема 3. **Обзор и основные характеристики программно-аппаратных комплексов защиты информации.** Использование специализированных аппаратно-программных средств защиты информации (СЗИ). Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Реализация в СЗИ ограничения на вход в систему и политики разграничения доступа. Контроль технологического мусора. Обзор современных отечественных средств защиты информации. Методы и средства ограничения доступа к компонентам ЭВМ.	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	3	3		4,5
4	**Тема 4. Основные подходы к защите данных от НСД.** Основные подходы к защите данных от НСД. Шифрование, контроль доступа и разграничение доступа. Способы сокрытия факта доступа. Системы комплексного управления доступом (СКУД) и принципы их построения. Типовые решения в организации ключевых систем. Схемы безопасного хранения аутентифицирующей информации в открытых компьютерных системах и в системах со специализированной	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	3	3		4,5

	аппаратной частью. Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа, защита файлов от изменения.						
5	**Тема 5. Электронная цифровая подпись (ЭЦП)** Схема электронной подписи, защищенность, алгоритмы, применяемые для ЭЦП. Федеральный закон «Об электронной цифровой подписи».	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	-	-		9
6	**Тема 6. Программно-аппаратные средства шифрования.** Построение аппаратных компонент криптозащиты данных, защита алгоритма шифрования, принцип чувствительной области, принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Основные характеристики системы «PGP». Инициализация системы «PGP» на рабочей станции. Генерация, импортирование и экспортирование ключей. Изменение настроек сервиса PGPkeys. Шифрование и обмен шифрованной информацией.	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	-	3		3
7	**Тема 7. Защита ПО от несанкционированного копирования.** Меры противодействия взлому программных продуктов: организационно-экономические, правовые, технические. Защита программ от несанкционированного копирования. Пароли и ключи, организация хранения ключей. Технические меры защиты ПО от несанкционированного использования (НСИ).	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	3	3		9
8	**Тема 8. Защита от разрушающих программных воздействий (РПВ). Изолированная программная среда.** Компьютерные вирусы как особый класс РПВ; Необходимые и достаточные условия недопущения разрушающего воздействия. Изолированная программная среда.	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	1,5	1,5	-		6
	Итого за 6 семестр		**12**	**12**	**12**		**45**

7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма проведения
	6 семестр		

1	Тема 1. **Предмет и задачи программно-аппаратной защиты информации.** Роль и назначение курса в подготовке специалистов по защите информации. Место курса среди других дисциплин учебного плана. Понятие безопасности информации. Вычислительная и операционная среда – пассивная и активная сущность компьютерной системы. Объект защиты в КС. Основные и обеспечивающие функции СЗИ.	1,5	
2	Тема 2. **Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.** Идентификация, аутентификация, авторизация субъекта доступа. Идентифицирующая информация. Классификация подсистем идентификации и аутентификации пользователей. Протоколы аутентификации. Парольные подсистемы идентификации и аутентификации пользователей, их достоинства и недостатки. Минимальные требования к выбору пароля и подсистемам парольной идентификации и аутентификации. Количественная оценка стойкости парольной защиты.	1,5	
3	Тема 3. **Обзор и основные характеристики программно-аппаратных комплексов защиты информации.** Использование специализированных аппаратно-программных средств защиты информации (СЗИ). Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Реализация в СЗИ ограничения на вход в систему и политики разграничения доступа. Контроль технологического мусора. Обзор современных отечественных средств защиты информации. Методы и средства ограничения доступа к компонентам ЭВМ.	1,5	
4	**Тема 4. Основные подходы к защите данных от НСД.** Основные подходы к защите данных от НСД. Шифрование, контроль доступа и разграничение доступа. Способы сокрытия факта доступа. Системы комплексного управления доступом (СКУД) и принципы их построения. Типовые решения в организации ключевых систем. Схемы безопасного хранения аутентифицирующей информации в открытых компьютерных системах и в системах со специализированной аппаратной частью. Доступ к данным со стороны процесса, способы фиксации факта доступа, надежность систем ограничения доступа, защита файлов от изменения.	1,5	
5	**Тема 5. Электронная цифровая подпись (ЭЦП)** Схема электронной подписи, защищенность, алгоритмы, применяемые для ЭЦП. Федеральный закон «Об электронной цифровой подписи».	1,5	

6	**Тема 6. Программно-аппаратные средства шифрования.** Построение аппаратных компонент криптозащиты данных, защита алгоритма шифрования, принцип чувствительной области, принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Основные характеристики системы «PGP». Инициализация системы «PGP» на рабочей станции. Генерация, импортирование и экспортирование ключей. Изменение настроек сервиса PGPkeys. Шифрование и обмен шифрованной информацией.	1,5	
7	**Тема 7. Защита ПО от несанкционированного копирования.** Меры противодействия взлому программных продуктов: организационно-экономические, правовые, технические. Защита программ от несанкционированного копирования. Пароли и ключи, организация хранения ключей. Технические меры защиты ПО от несанкционированного использования (НСИ).	1,5	
8	**Тема 8. Защита от разрушающих программных воздействий (РПВ). Изолированная программная среда.** Компьютерные вирусы как особый класс РПВ; Необходимые и достаточные условия недопущения разрушающего воздействия. Изолированная программная среда.	1,5	
	Итого за 6 семестр	**12**	

7.3 Наименование лабораторных работ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма проведения
	6 семестр		
Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.			
2	Лабораторная работа 1. Межсетевые экраны.	3	Компьютерные симуляции
Тема 3. Обзор и основные характеристики программно-аппаратных комплексов защиты информации.			
3	Лабораторная работа 2. Программное восстановление данных.	3	Компьютерные симуляции
Тема 4. Основные подходы к защите данных от НСД.			
4	Лабораторная работа 3 Обнаружение и предотвращение вторжений.	3	
Тема 5. Электронная цифровая подпись (ЭЦП)			
5	Лабораторная работа 4 Электронная цифровая подпись.	1,5	
Тема 6. Программно-аппаратные средства шифрования.			

6	Лабораторная работа 5 Программно-аппаратное шифрование данных при их хранении.	1,5	
	Итого за 6 семестр	**12**	**3**

7.4 Наименование практических занятий

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивая форма проведения
	6 семестр		
Тема 1. Предмет и задачи программно-аппаратной защиты информации.			
1	Практическая работа 1. Сбор данных об информационной системе с помощью средств администрирования Windows.	1,5	
Тема 1. Предмет и задачи программно-аппаратной защиты информации.			
1	Практическая работа 2. Сбор данных о топологии сети с помощью средства администрирования сетей.	1,5	
Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.			
2	Практическая работа 3. Идентификация и аутентификация систем семейства Microsoft Windows.	1,5	
Тема 2. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация, особенности их реализации.			
2	Практическая работа 4. Аутентификация по протоколу Kerberos.	1,5	
Тема 3. Обзор и основные характеристики программно-аппаратных комплексов защиты информации.			
3	Практическая работа 5. Настройка локальной политики парольной безопасности операционной системы.	1,5	
Тема 5. Электронная цифровая подпись (ЭЦП)			
5	Практическая работа 6. Инфраструктура открытых ключей. Цифровые сертификаты.	1,5	Круглый стол
Тема 6. Программно-аппаратные средства шифрования.			
6	Практическая работа 7. Использование цифровых сертификатов.	1,5	Круглый стол
Тема 6. Программно-аппаратные средства шифрования.			
6	Практическая работа 8. Резервное копирование в Windows Server 2008.	1,5	
	Итого 6 семестр	**12**	**3**

7.5 Технологическая карта самостоятельной работы студента

Технологическая карта

Коды реализуемой компете	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии	Объем часов, в том числе		
				СРС	Контактная	Всего

нции			оценки		работа с преподавателем	
ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	Самостоятельное изучение литературы по теме 1,2	Конспект	Собеседование	69,66	7,74	77,4
ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	Подготовка к лекциям	Конспект	Собеседование	1,08	0,12	1,2
ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	Подготовка к лабораторным и практическим работам	Отчет	Отчет письменный	2,16	0,24	2,4
Итого за 6 семестр				**72,9**	**8,1**	**81**
Итого				**72,9**	**8,1**	**81**

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Код оцениваемой компетенции	**Этап формирования компетенции (№ темы)**	**Средства и технологии оценки**	**Тип контроля (текущий/промежуточный)**	**Вид контроля (текущий/промежуточный)**	**Наименование оценочного средства**
ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	Темы 1,2	собеседование	текущий	устный	Вопросы для собеседования
ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4	Темы 6,7	Круглый стол	текущий	Перечень дискуссионных тем для круглого стола	Вопросы для собеседования

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровни сфомированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов
	ОПК-7				

Базовый	**Знает:** информационные ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципы и методы ин-формационной и организационной защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи ин-формации;	*Не знает:* информационные ресурсы, подлежащие защите, угрозы безопасности информации;	*Знает:* информационные ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;	*Знает:* информационные ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания инфор-мационных процессов и особенно-стей функциони-рования объекта защиты; принципы и методы ин-формационной и организационной защиты информации; принципы и методы противо-действия несанк-ционированному информационному воздействию на вычислительные системы и системы передачи ин-формации;	
	Умеет: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; при-менять принципы и методы информационной и организационной за-щиты информации; использовать принципы и методы противодей-ствия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;	*Не умеет:* определять информационные ресурсы, подлежащие защите, угрозы безопасности информации;	*Умеет:* определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;	*Умеет:* определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; при-менять принципы и методы информационной и организационной за-щиты информации; использовать принципы и методы противодей-ствия несанкционированному информационному воздействию на вы-числительные системы и системы передачи информации;	
	Владеет: способностью	*Не владеет:* способност	*Владеет:* способностью	*Владеет:* способностью	

	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципами и методами информационной и организационной защиты информации; навыками использования принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;	ью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации;	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципами и методами информационной и организационной защиты информации; навыками использования принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;	
	ПК-1				
Базовый	**Знает:** работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение; технологию работы на ПК в современных операционных средах; назначение и возможности прикладных программных продуктов;	*Не знает:* работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации;	*Знает:* работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение;	*Знает:* работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение; технологию работы на ПК в современных операционных средах; назначение и возможности прикладных программных продуктов;	

	Умеет: выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; выбирать архитектуру ПК, аппаратное обеспечение; применять технологию работы на ПК в современных операционных средах; использовать возможности прикладных программных продуктов;	*Не умеет:* выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации;	*Умеет:* выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; выбирать архитектуру ПК, аппаратное обеспечение;	*Умеет:* выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; выбирать архитектуру ПК, аппаратное обеспечение; применять технологию работы на ПК в современных операционных средах; использовать возможности прикладных программных продуктов;	
	Владеет: способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах; основными методами и средствами прикладных программных продуктов;	*Не владеет* способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации;	*Владеет* способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах;	*Владеет* способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах; основными методами и средствами прикладных программных продуктов;	
ПК-2					
Базовый	**Знает:** правила разработки и оформления технической документации и установленной отчетности по утвержденным формам; правила сертификации технических средств, систем, процессов,	*Не знает:* правила разработки и оформления технической документации и установленной отчетности	*Знает:* правила разработки и оформления технической документации и установленной отчетности по утвержденным формам; правила	*Знает:* правила разработки и оформления технической документации и установленной отчетности по утвержденным формам; правила сертификации технических средств, систем, процессов, оборудования и	

	оборудования и материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования; алгоритмы растрирования и геометрические преобразования;	по утвержденным формам;	сертификации технических средств, систем, процессов, оборудования и материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования;	материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования; алгоритмы растрирования и геометрические преобразования;	
	Умеет: формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты; представлять технические решения с использованием программных средств компьютерной графики и геометрического моделирования.	*Не умеет:* формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники;	*Умеет:* формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты;	*Умеет:* формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты; представлять технические решения с использованием программных средств компьютерной графики и геометрического моделирования;	
	Владеет: навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ; навыками разработки проектной	*Не владеет:* навыками самостоятельной работы на компьютере и в компьютерных сетях;	*Владеет:* навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ;	*Владеет:* навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ; навыками разработки проектной и конструкторской документации в соответствии с требованиями стандартов; навыками	

	и конструкторской документации в соответствии с требованиями стандартов; навыками работы на компьютерной технике с графическими пакетами для получения конструкторских, технологических и других документов; опытом выполнения проектов с учетом специфики направления подготовки.			работы на компьютерной технике с графическими пакетами для получения конструкторских, технологических и других документов; опытом выполнения проектов с учетом специфики направления подготовки;	
ПК-3					
Базовый	**Знает:** основы администрирования вычислительных сетей; подсистемы информационной безопасности объекта защиты; операционные системы персональных ЭВМ; системы управления базами данных; принципы построения информационных систем.	*Не знает:* основы администрирования вычислительных сетей;	*Знает:* основы администрирования вычислительных сетей; подсистемы информационной безопасности объекта защиты;	*Знает:* основы администрирования вычислительных сетей; подсистемы информационной безопасности объекта защиты; операционные системы персональных ЭВМ; системы управления базами данных; принципы построения информационных систем;	
	Умеет: применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты; пользоваться операционными системами персональных ЭВМ; анализировать системы управления базами данных; применять принципы построения информационных систем.	*Не умеет:* применять основы администрирования вычислительных сетей;	*Умеет:* применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты;	*Умеет:* применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты; пользоваться операционными системами персональных ЭВМ; анализировать системы управления базами данных; применять принципы построения информационных систем;	
	Владеет: основами администрирования вычислительных	*Не владеет:* основами администрирования вычислител	*Владеет:* основами администрирования вычислительны	*Владеет:* основами администрирования вычислительных сетей; способностью администрировать	

	сетей; способностью администрировать подсистемы информационной безопасности объекта защиты; операционными системами персональных ЭВМ; способностью управления базами данных; методами и принципами построения информационных систем;	ьных сетей;	х сетей; способностью администрировать подсистемы информационной безопасности объекта защиты;	подсистемы информационной безопасности объекта защиты; операционными системами персональных ЭВМ; способностью управления базами данных; методами и принципами построения информационных систем;	
ПК-4					
Базовый	**Знает:** основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	*Не знает:* основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты;	*Знает:* основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации;	*Знает:* основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	
	Умеет: использовать основные методы в работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению информационной безопасности объекта защиты; применять принципы	*Не умеет:* использовать основные методы в работах по реализации политики информационной безопасности;	*Умеет:* использовать основные методы в работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению	*Умеет:* использовать основные методы в работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению информационной безопасности объекта защиты; применять принципы организации информационных	

	организации информационных систем в соответствии с требованиями по защите информации; отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;		информационной безопасности объекта защиты;	систем в соответствии с требованиями по защите информации; отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	
	Владеет: способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной безопасности объекта защиты; принципами организации информационных систем в соответствии с требованиями по защите информации; возможностью отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	*Не владеет:* способностью участвовать в работах по реализации политики информационной безопасности;	*Владеет:* способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной безопасности объекта защиты;	*Владеет:* способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной безопасности объекта защиты; принципами организации информационных систем в соответствии с требованиями по защите информации; возможностью отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;	
	ОПК-7				
Повышенный	**Знает:** информационные				*Знает:*

	ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципы и методы ин-формационной и организационной защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;				информационные ресурсы, подлежащие защите, угрозы безопасности информации; возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципы и методы информационной и организационной защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
	Умеет: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; при-				*Умеет:* определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; находить возможные пути их реализации на основе анализа структуры и содержания информационных

	менять принципы и методы информационной и организационной защиты информации; использовать принципы и методы противодей-ствия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;				процессов и особенностей функционирования объекта защиты; применять принципы и методы информационной и организационной за-щиты информации; использовать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
	Владеет: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципами и методами информационной и организационной защиты информации; навыками использования принципов и методов противодействия несанкционированно				*Владеет:* способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации; способностью находить возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; принципами и методами информационной и организационной защиты информации;

	му информационному воздействию на вычислительные системы и системы передачи информации;				навыками использования принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
	ПК-1				
Повышенный	**Знает:** работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение; технологию работы на ПК в современных операционных средах; назначение и возможности прикладных программных продуктов;				*Знает:* работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; архитектуру ПК, аппаратное обеспечение; технологию работы на ПК в современных операционных средах; назначение и возможности прикладных программных продуктов;
	Умеет: выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; выбирать				*Умеет:* выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и

	архитектуру ПК, аппаратное обеспечение; применять технологию работы на ПК в современных операционных средах; использовать возможности прикладных программных продуктов;				технических средств защиты информации; выбирать архитектуру ПК, аппаратное обеспечение; применять технологию работы на ПК в современных операционных средах; использовать возможности прикладных программных продуктов;
	Владеет: способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах; основными методами и средствами прикладных программных продуктов;				*Владеет*: способностью выполнять работы по установке, настройке и обслуживанию программных, программно – аппаратных (в том числе криптографических) и технических средств защиты информации; навыками работы на ПК в современных операционных средах; основными методами и средствами прикладных программных продуктов;
ПК-2					
Повышенный	**Знает:** правила разработки и оформления технической документации и установленной отчетности по утвержденным формам; правила сертификации				*Знает:* правила разработки и оформления технической документации и установленной отчетности по

	технических средств, систем, процессов, оборудования и материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования; алгоритмы растрирования и геометрические преобразования;				утвержденным формам; правила сертификации технических средств, систем, процессов, оборудования и материалов; информационное обеспечение систем автоматизации и управления на основе современных технологий программирования; алгоритмы растрирования и геометрические преобразования;
	Умеет: формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты; представлять технические решения с использованием программных средств компьютерной графики и геометрического моделирования.				*Умеет:* формировать наглядные изображения реальных объектов сложных технических форм с использованием средств вычислительной техники; разрабатывать и оформлять конструкторскую документацию на типовые объекты; представлять технические решения с использованием программных средств компьютерной графики и геометрического моделировани

					я.
	Владеет: навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ; навыками разработки проектной и конструкторской документации в соответствии с требованиями стандартов; навыками работы на компьютерной технике с графическими пакетами для получения конструкторских, технологических и других документов; опытом выполнения проектов с учетом специфики направления подготовки;				*Владеет:* навыками самостоятельной работы на компьютере и в компьютерных сетях; осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ; навыками разработки проектной и конструкторской документации в соответствии с требованиями стандартов; навыками работы на компьютерной технике с графическими пакетами для получения конструкторских, технологических и других документов; опытом выполнения проектов с учетом специфики направления подготовки;
ПК-3					
Повышенный	**Знает:** основы администрирования вычислительных сетей; подсистемы информационной безопасности объекта защиты;				*Знает:* основы администрирования вычислительных сетей; подсистемы информацион

	операционные системы персональных ЭВМ; системы управления базами данных; принципы построения информационных систем;				ной безопасности объекта защиты; операционные системы персональных ЭВМ; системы управления базами данных; принципы построения информационных систем;
	Умеет: применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты; пользоваться операционными системами персональных ЭВМ; анализировать системы управления базами данных; применять принципы построения информационных систем;				*Умеет:* применять основы администрирования вычислительных сетей; использовать подсистемы информационной безопасности объекта защиты; пользоваться операционными системами персональных ЭВМ; анализировать системы управления базами данных; применять принципы построения информационных систем;
	Владеет: основами администрирования вычислительных сетей; способностью администрировать подсистемы информационной безопасности объекта защиты; операционными системами персональных ЭВМ; способностью управления базами				*Владеет:* основами администрирования вычислительных сетей; способностью администрировать подсистемы информационной безопасности объекта защиты; операционными системами

	данных; методами и принципами построения информационных систем;				персональных ЭВМ; способностью управления базами данных; методами и принципами построения информационных систем;
ПК-4					
	Знает: основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;				*Знает:* основные методы в работах по реализации политики информационной безопасности; принципы и методы комплексного подхода к обеспечению информационной безопасности объекта защиты; принципы организации информационных систем в соответствии с требованиями по защите информации; технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
	Умеет: использовать основные методы в				*Умеет:* использовать основные

	работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению информационной безопасности объекта защиты; применять принципы организации информационных систем в соответствии с требованиями по защите информации; отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;				методы в работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению информационной безопасности объекта защиты; применять принципы организации информационных систем в соответствии с требованиями по защите информации; отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
	Владеет: способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной безопасности объекта				*Владеет:* способностью участвовать в работах по реализации политики информационной безопасности; принципами и методами комплексного подхода к обеспечению информационной

	защиты; принципами организации информационных систем в соответствии с требованиями по защите информации; возможностью отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;				безопасности объекта защиты; принципами организации информационных систем в соответствии с требованиями по защите информации; возможностью отслеживать технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	6 семестр		
1.	Сдача отчетов по лабораторным работам 1,2. Собеседование по темам 1-3	5-ая неделя	15
2.	Сдача отчетов по лабораторным работам 3,4. Собеседование по темам 4-6.	12-ая неделя	15
3.	Сдача отчетов по лабораторным работам 5. Собеседование по темам 7,8.	16 –ая неделя	25
	Итого за 6 семестр		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация

Промежуточная аттестация в форме **зачета с оценкой**.

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	**Количество баллов за зачет ($S_{зач}$)**
$50 \le R_{сем} \le 60$	**40**
$39 \le R_{сем} < 50$	**35**
$33 \le R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций для проведения промежуточной аттестации

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Текущая аттестация студентов проводится преподавателем, ведущим практические и лабораторные занятия, в следующих формах: отчет (письменный), собеседование.

Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Максимальное количество баллов студент получает, если оформление отчета соответсвует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижением оценки являются:

- частичное несоотвествие установленным требованиям
- в неполном объеме выполнена практическое задание

Отчет может быть отправлен на доработку в следующих случаях:

- полностью нессотвествует установлеенным требованиям
- не выполено пракическое задание

Критерии оценивания индивидуальных заданий, собеседования, круглого стола приведены в Фонде оценочных средств по дисциплине «Программно-аппаратные средства защиты информации».

9. Методические указания для обучающихся по освоению дисциплины

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации:

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
	6 семестр				
1	Самостоятельное изучение литературы	1-2	1-2	1-3	1-2
2	Подготовка к практическим работам	1-2	1-2	1-3	1-2
3	Подготовка к лабораторным работам	1-2	1-2	1-3	1-2

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

10.1.1. Перечень основной литературы

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

10.1.2. Перечень дополнительной литературы

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М.; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Программно-аппаратные средства защиты информации».

2. Методические указания по выполнению практических работ по дисциплине «Программно-аппаратные средства защиты информации».

3. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине дисциплине «Программно-аппаратные средства защиты информации»

10.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Университетская библиотека online. http://www.biblioclub.ru.

2. ЭБС «IPRbooks». http://www.iprbookshop.ru.

3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.

4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа: . Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, переносной ноутбук, переносной проектор.

Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин

2. Учебная аудитория для проведения занятий семинарского типа (лабораторных работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер преподавателя, проектор , доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета

3. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер преподавателя, проектор , доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета