



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

СОГЛАСОВАНО
Руководитель ОП


(подпись) Боршевников А.Е.
(ФИО)

УТВЕРЖДАЮ
и.о. директора департамента информационной
безопасности

(подпись) Боршевников А.Е.
(И.О. Фамилия)
«03» марта 2023



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита в операционных системах
Направление подготовки 10.03.01 Информационная безопасность
(Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности))

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (с изменениями и дополнениями).

Рабочая программа обсуждена на заседании департамента информационной безопасности, протокол № 5 от «03» февраля 2023 г.

И.о. директора департамента информационной безопасности Боршевников А.Е.
Составитель: доцент Боршевников А.Е., ст. преп. Капецкий И.О.

Владивосток

2023

Оборотная сторона титульного листа РПД

1. *Рабочая программа пересмотрена и утверждена на заседании Департамента информационной безопасности, протокол от «__» _____202 г. №*
2. *Рабочая программа пересмотрена и утверждена на заседании Департамента информационной безопасности, протокол от «__» _____202 г. №*
3. *Рабочая программа пересмотрена и утверждена на заседании Департамента информационной безопасности, протокол от «__» _____202 г. №*
4. *Рабочая программа пересмотрена и утверждена на заседании Департамента информационной безопасности, протокол от «__» _____202 г. №*

1. Цель и задачи дисциплины:

Цель: дать основы устройства и принципов функционирования операционных систем различной архитектуры; принципов построения и защиты информации в операционных системах различной архитектуры.

Задачи:

- формирование у обучающихся представления об операционных системах (ОС) различных архитектур;
- изучение средств и методов несанкционированного доступа к ресурсам ОС;
- изучение принципов построения защиты информации от рассмотренных средств и методов НСД;
- формирование системного подхода к проблеме защиты информации в ОС.

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют формирование следующих компетенций:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Эксплуатационный	ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
		ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
		ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических

		средств защиты информации
Эксплуатационный	ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения
		ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения
		ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
экспериментально-исследовательский	ПК-5 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-5.1 Определяет состав контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
		ПК-5.2 Осуществляет организацию, контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
		ПК-5.3 Производит аттестацию объектов вычислительной техники на соответствие требованиям по защите информации
организационно-управленческий	ПК-7 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-7.1 Демонстрирует знание методологий организации технологического процесса защиты информации ограниченного доступа
		ПК-7.2 Исследует нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, составляет отчеты о проделанной работе, обзоры
		ПК-7.3 Разрабатывает технические отчеты о проделанной работе, обзоры, готовит публикации

1. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоёмкость дисциплины составляет 5 зачётных единиц (180 академических часов).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	1. Архитектура операционных систем	4	6	-	12				экзамен
2	2. Управление памятью в операционных системах	4	10	-	12				
3	3. Защита информации в современных операционных системах	4	20	-	12	-	72	36	
Итого:			36		36	-	72	36	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Архитектура операционных систем

Тема 1. Принципы построения операционных систем

1.1 Понятие об архитектуре аппаратных средств

1.2 Режимы работы операционных систем

Тема 2. Концептуальные основы операционных систем

2.1 Понятие ядра и микроядра ОС

2.2 Концепция виртуальности

Раздел II. Управление памятью в операционных системах

Тема 1. Методы связного распределения основной памяти

1.1 Связное распределение памяти для одного пользователя.

1.2 Стратегии размещения информации в памяти

Тема 2. Управление файлами и вводом-выводом в операционных системах

2.1 Методы организации данных в операционных системах.

2.2 Методы доступа к данным.

Тема 3. Управление файлами

3.1 Организация файлов.

3.2 Файловая система.

Тема 4. Основные блоки компьютера

4.1 Компоненты компьютера.

4.2 Состав системного блока.

Тема 5. Система ввода-вывода

5.1 Физическая организация устройств ввода-вывода.

5.2 Организация программного обеспечения ввода-вывода.

Раздел III. Защита информации в современных операционных системах

Тема 1. Основные понятия и положения защиты информации в информационно-вычислительных системах

1.1 Предмет защиты информации.

1.2 Объект защиты информации.

Тема 2. Угрозы безопасности информации в информационно-вычислительных системах

2.1 Анализ угроз информационной безопасности.

2.2 Методы обеспечения информационной безопасности.

Тема 3. Защита информации в современных операционных системах

3.1 Основные понятия программно-технического уровня информационной безопасности.

3.2 Требования к защите компьютерной информации.

Тема 4. Модели безопасности основных операционных систем

4.1 Механизмы защиты операционных систем.

4.2 Анализ защищенности современных операционных систем.

Тема 5. Операционная система Windows

5.1 Версии ОС Windows.

5.2 Windows для персональных компьютеров.

Тема 6. Операционная система Linux

6.1 Версии ОС Linux.

6.2 Linux для персональных компьютеров.

Тема 7. Системы защиты программного обеспечения

7.1 Классификация систем защиты программного обеспечения.

7.2 Достоинства и недостатки основных систем защиты.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия

Практическое занятие № 1.

Исследование файловых объектов с правами пользователя

Исследование файловых объектов с правами пользователя в ОС Windows.

Практическое занятие № 2.

Исследование процессов в ОС Linux

Исследование процессов в ОС Windows

Практическое занятие № 3.

Наблюдение и аудит в ОС Linux

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка к практическим занятиям	18	ПР-6
2	Сессия	Подготовка к экзамену	36	Экзамен

Рекомендации по самостоятельной работе студентов

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентами учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать

IV.

КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№п/п	Контролируемые разделы / темы дисциплины	Код индикатора достижения компетенции и результаты обучения	Оценочные средства - наименование	
			текущий контроль	промежуточная аттестация
1	Раздел I. Архитектура операционных систем	ПК-1.1 Знает основной набор методов и средств защиты информации ПК-1.2 Знает особенности эксплуатации средств защиты информации ПК-1.3 Знает методики оценки работ по настройке и обслуживанию средств защиты информации ПК-2.1 Знает состав программных средств защиты информации определенного функционала ПК-2.2 Знает методы проверки работоспособности программных средств защиты информации ПК-2.3 Знает особенности применения программных средств для решения профессиональных задач ПК-5.1 Знает виды и порядок проведения испытаний системы защиты информации компьютерной системы. ПК-5.2 Знает основные требования информационной безопасности при эксплуатации системы защиты информации ПК-5.3 Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ПК-7.1 Знает организационные меры по защите информации ПК-7.2 Знает основы проверки работоспособности средств защиты информации от несанкционированного доступа ПК-7.3 Знает правовые основы организации защиты государственной тайны и конфиденциальной информации	собеседование (УО-1)	УО-1
		Умеет определить состав работ по внедрению средств защиты информации в организации Умеет администрировать средства защиты информации Умеет осуществлять контроль за настройкой и обслуживанием средств защиты информации Умеет определить достаточность состава средств системного, прикладного и специального назначения Умеет проводить проверку работоспособности программных средств Умеет использовать программные средства системного, прикладного и специального назначения для решения задач информационной безопасности Умеет разрабатывать планы мероприятий по вводу в действие	практические работы(ПР-6),	УО-1

		<p>систем защиты информации компьютерной системы и программ и методик испытаний этих систем. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации объектов аттестации по требованиям безопасности информации Умеет пользоваться нормативными документами в области технической защиты информации Умеет разрабатывать политики безопасности информации Умеет проводить контроль защищенности информации от несанкционированного доступа и специальных воздействий с использованием программных и программно-аппаратных средств Умеет разрабатывать проекты инструкций, регламентов и организационно-распорядительных документов</p>		
		<p>Владеет навыками настройки средств защиты информации Владеет методами настройки средств защиты информации Владеет навыками оценки полноты настройки средств защиты информации Владеет навыками анализа состава программных средств защиты информации Владеет навыками анализа оценки работоспособности программных средств системного, прикладного и специального назначения Владеет навыками программирования для решения задач информационной безопасности Владеет навыками сертификации систем защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Владеет навыками проведения экспериментально-исследовательских работ при аттестации объектов Владеет методами и средствами технической защиты информации Владеет навыками разрабатывать документы в области обеспечения безопасности информации Владеет навыками оформлять отчетные документы Владеет навыками формулировать основные требования при лицензировании деятельности в области сертификации и аттестации по требованиям безопасности информации</p>	конспект (ПР-7)	УО-1
2	Раздел II. Управление	<p>ПК-1.1 Знает основной набор методов и средств защиты информации ПК-1.2 ПК-1.3 Знает особенности эксплуатации средств защиты информации ПК-2.1</p>	собеседование (УО-1)	УО-1

	<p>памятью в операционных системах</p>	<p>ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3</p> <p>Знает методики оценки работ по настройке и обслуживанию средств защиты информации</p> <p>Знает состав программных средств защиты информации определенного функционала</p> <p>Знает методы проверки работоспособности программных средств защиты информации</p> <p>Знает особенности применения программных средств для решения профессиональных задач</p> <p>Знает виды и порядок проведения испытаний системы защиты информации компьютерной системы.</p> <p>Знает основные требования информационной безопасности при эксплуатации системы защиты информации</p> <p>Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации</p> <p>Знает организационные меры по защите информации</p> <p>Знает основы проверки работоспособности средств защиты информации от несанкционированного доступа</p> <p>Знает правовые основы организации защиты государственной тайны и конфиденциальной информации</p>		
		<p>Умеет определить состав работ по внедрению средств защиты информации в организации</p> <p>Умеет администрировать средства защиты информации</p> <p>Умеет осуществлять контроль за настройкой и обслуживанием средств защиты информации</p> <p>Умеет определить достаточность состава средств системного, прикладного и специального назначения</p> <p>Умеет проводить проверку работоспособности программных средств</p> <p>Умеет использовать программные средства системного, прикладного и специального назначения для решения задач информационной безопасности</p> <p>Умеет разрабатывать планы мероприятий по вводу в действие систем защиты информации компьютерной системы и программ и методик испытаний этих систем.</p> <p>Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации объектов аттестации по требованиям безопасности информации</p> <p>Умеет пользоваться нормативными документами в области технической защиты информации</p> <p>Умеет разрабатывать политики</p>	<p>практические работы(ПР-6),</p>	<p>УО-1</p>

			<p>безопасности информации Умеет проводить контроль защищенности информации от несанкционированного доступа и специальных воздействий с использованием программных и программно-аппаратных средств Умеет разрабатывать проекты инструкций, регламентов и организационно-распорядительных документов</p>		
			<p>Владеет навыками настройки средств защиты информации Владеет методами настройки средств защиты информации Владеет навыками оценки полноты настройки средств защиты информации Владеет навыками анализа состава программных средств защиты информации Владеет навыками анализа оценки работоспособности программных средств системного, прикладного и специального назначения Владеет навыками программирования для решения задач информационной безопасности Владеет навыками сертификации систем защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Владеет навыками проведения экспериментально-исследовательских работ при аттестации объектов Владеет методами и средствами технической защиты информации Владеет навыками разрабатывать документы в области обеспечения безопасности информации Владеет навыками оформлять отчетные документы Владеет навыками формулировать основные требования при лицензировании деятельности в области сертификации и аттестации по требованиям безопасности информации</p>	конспект (ПР-7)	УО-1
3	Раздел III. Защита информации в современных операционных системах	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3 ОПК-4.1, ОПК-4.2	<p>Знает основной набор методов и средств защиты информации Знает особенности эксплуатации средств защиты информации Знает методики оценки работ по настройке и обслуживанию средств защиты информации Знает состав программных средств защиты информации определенного функционала Знает методы проверки работоспособности программных средств защиты информации Знает особенности применения программных средств для решения профессиональных задач Знает виды и порядок проведения испытаний системы защиты</p>	собеседование (УО-1)	УО-1

		<p>информации компьютерной системы. Знает основные требования информационной безопасности при эксплуатации системы защиты информации Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Знает организационные меры по защите информации Знает основы проверки работоспособности средств защиты информации от несанкционированного доступа Знает правовые основы организации защиты государственной тайны и конфиденциальной информации</p>		
		<p>Умеет определить состав работ по внедрению средств защиты информации в организации Умеет администрировать средства защиты информации Умеет осуществлять контроль за настройкой и обслуживанием средств защиты информации Умеет определить достаточность состава средств системного, прикладного и специального назначения Умеет проводить проверку работоспособности программных средств Умеет использовать программные средства системного, прикладного и специального назначения для решения задач информационной безопасности Умеет разрабатывать планы мероприятий по вводу в действие систем защиты информации компьютерной системы и программ и методик испытаний этих систем. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации объектов аттестации по требованиям безопасности информации Умеет пользоваться нормативными документами в области технической защиты информации Умеет разрабатывать политики безопасности информации Умеет проводить контроль защищенности информации от несанкционированного доступа и специальных воздействий с использованием программных и программно-аппаратных средств Умеет разрабатывать проекты инструкций, регламентов и организационно-распорядительных документов</p>	<p>практические работы(ПР-6),</p>	<p>УО-1</p>
		<p>Владеет навыками настройки средств защиты информации Владеет методами настройки средств</p>		

		<p>защиты информации Владеет навыками оценки полноты настройки средств защиты информации Владеет навыками анализа состава программных средств защиты информации Владеет навыками анализа оценки работоспособности программных средств системного, прикладного и специального назначения Владеет навыками программирования для решения задач информационной безопасности Владеет навыками сертификации систем защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Владеет навыками проведения экспериментально-исследовательских работ при аттестации объектов Владеет методами и средствами технической защиты информации Владеет навыками разрабатывать документы в области обеспечения безопасности информации Владеет навыками оформлять отчетные документы Владеет навыками формулировать основные требования при лицензировании деятельности в области сертификации и аттестации по требованиям безопасности информации</p>		
	<p>ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3</p>	<p>Знает основной набор методов и средств защиты информации Знает особенности эксплуатации средств защиты информации Знает методики оценки работ по настройке и обслуживанию средств защиты информации Знает состав программных средств защиты информации определенного функционала Знает методы проверки работоспособности программных средств защиты информации Знает особенности применения программных средств для решения профессиональных задач Знает виды и порядок проведения испытаний системы защиты информации компьютерной системы. Знает основные требования информационной безопасности при эксплуатации системы защиты информации Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Знает организационные меры по защите информации Знает основы проверки работоспособности средств защиты информации от несанкционированного</p>	<p>конспект (ПР-7)</p>	<p>УО-1</p>

		доступа Знает правовые основы организации защиты государственной тайны и конфиденциальной информации		
--	--	---	--	--

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Оглтри, Т. Firewalls. Практическое применение межсетевых экранов [Электронный ресурс] / Т. Оглтри. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 400 с. — Режим доступа: <https://e.lanbook.com/book/1075>
2. Кирклэнд, Р. Domino 5 & 6. Администрирование сервера [Электронный ресурс] / Р. Кирклэнд. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 824 с. — Режим доступа: <https://e.lanbook.com/book/1077>
3. Скудис, Э. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите [Электронный ресурс] : учебное пособие / Э. Скудис. — Электрон. дан. — Москва : ДМК Пресс, 2009. — 512 с. — Режим доступа: <https://e.lanbook.com/book/1112>

Дополнительная литература

(печатные и электронные издания)

1. Защита в операционных системах [Электронный ресурс] : Учебное пособие для вузов / Проскурин В.Г. - М. : Горячая линия - Телеком, 2014. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991203791.html>
2. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785940745181.html>
3. А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785804103782.html>

Перечень ресурсов информационно-телекоммуникационной сети

«Интернет»

1. Защита в операционных системах, Учебное пособие для вузов [Электронный ресурс]. – Электрон. дан. – Режим доступа : [Проскурин В.Г. http://www.techbook.ru/book.php?id_book=693](http://www.techbook.ru/book.php?id_book=693)

2. [Безопасность операционных систем](#) , сборник [Электронный ресурс]. – Электрон. дан. – Режим доступа : <https://works.doklad.ru/view/d-U9G-zPi2g/all.html>
3. Методы и средства защиты компьютерной информации [Электронный ресурс]. – Электрон. дан. – Режим доступа : <http://www.volpi.ru/umkd/zki/index.php?man=1&page=35>

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических работ. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка литературы для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал. Практические работы представляют собой задания различного типа, направленные на получение обучающимся практических знаний по теме. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену

студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
<p>690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13)Оборудование: ЖК-панель 47", Full HD, LGM4716 CCBA – 1 шт. Доска аудиторная, Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPPjectorPT-D2110XE</p>	<p>1С Предприятия8 (8.2), 7-Zip, ABBYY Lingvo12,Alice 3, Anaconda3,Autodesk,CodeBlocks,CorelDRAW X7,Dia,Directum4.8,DosBox-0.74,Farmanager,Firebird 2.5,FlameRobin,Foxit Reader,Free Pascal,Geany,Ghostscript,Git,Greenfoot,gsview,Inscapе0.91,Java,Java development Kit,Kaspersky,Lazarus,LibreOffice4.4,MatLab R2017b,Maxima 5.37.2,Microsoft Expression,Microsoft Office2013,Microsoft Silverlight,Microsoft Silverlight 5SDK-русский,MicrosoftSistem Center,Microsoft Visial Studio 2012,MikTeX2.9,MySQL,NetBeans,Notepad++,Oracle VM VirtualBox,PascalABC.NET,PostgreSQL 9.4,PTC Mathcad,Putty,PyQt GPL v5.4.1 for Pythonv 3.4,Pyton2.7(3.4,3.6),QGIS Brighton,RStudio,SAM CoDeC Pack,SharePoint,Strawberry Perl,Tecnomatix,TeXnicCenter,TortoiseSVN,Unity2017.3.1f1, Veusz,Vim8.1,Visual Paradigm CE,Visual Studio2013,Windows Kits,Windows Phone SDK8.1,Xilinx Design ToolsAcrobat ReaderDC,AdobeBridge CS3,AdobeDeviceCentralCS3,Adobe ExtendScript Toolkit 2,Adobe Photoshоpe CS3,DVD-студия Windows,GoogleChrome,Internet Explorer,ITMOproctor,Mozilla Firefox, Visual StudioInstaller,Windows Media Center, WinSCP,</p>
<p>690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус А, ауд. А1042 Аудитория для самостоятельной работы студентов</p>	<p>Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер ве-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C); Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными</p>	<p>Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0, Duxbury BrailleTranslator, DolphinGuide (контракт № А238-14/2); Неисключительные правана использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ppt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к</p>

	<p>возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Мемо цифровой; Устройство портативное для чтения плоскочечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Мемо цифровой.</p>	<p>внутренней информационной системе документооборота и порталу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая порталные хранилища, используемой в ДВФУ: Microsoft SharePoint; -лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center.</p>
--	---	---