ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Прохорова И. А.
Пользователь: prokhorovaia
Дата подписания: 20.05.2023

И. А. Прохорова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.16 Информационная безопасность
для направления 09.03.03 Прикладная информатика
уровень Бакалавриат
форма обучения заочная
кафедра-разработчик Цифровая экономика и информационные технологии

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утверждённым приказом Минобрнауки от 19.09.2017 № 922

Зав.кафедрой разработчика,
д.экон.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Худякова Т. А.
Пользователь: khudiakovata
Дата подписания: 19.05.2023

Т. А. Худякова

Разработчик программы,
старший преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Переведенцев В. В.
Пользователь: perevedentcevvv
Дата подписания: 19.05.2023

В. В. Переведенцев

Челябинск

1. Цели и задачи дисциплины

Цель дисциплины - изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности. Задачи дисциплины: - сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния; - передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации; - сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Краткое содержание дисциплины

Защищенность информационной среды организации — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности информационной среды должен быть неотъемлемой частью системы управления любой организации. В настоящее время, персональные компьютеры (рабочие станции) пользователей, как правило, подключены к глобальной сети Интернет. Знания и умения пользователя по обеспечению информационной безопасности персонального компьютера, работающего в «агрессивной» сетевой среде, становятся одними из самых востребованных и необходимых. Данная дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем, практическими приемами защиты рабочих станций и серверов

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-2 Способен разрабатывать и адаптировать прикладное программное обеспечение	Знает: Знание современных законов, стандартов, методов и технологий в области защиты информации Умеет: Использовать современные программно-аппаратные средства защиты информации. Находить потенциальные уязвимости в коде приложений. Имеет практический опыт: Владения современными методами и средствами обеспечения защиты информации.
ПК-4 Способен разрабатывать базы данных ИС с учетом требований информационной безопасности, осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач.	Знает: Принципы безопасного проектирования базы данных информационных систем. Умеет: Обосновывать экономическую оправданность информационной защиты. Имеет практический опыт: Оценки

	защищенности базы данных информационных систем.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.09 Высокоуровневые методы информатики и программирования, 1.Ф.24 Практикум по виду профессиональной деятельности, 1.Ф.12 Интернет-программирование	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.Ф.24 Практикум по виду профессиональной деятельности	Знает: Методику проведения тестирования компонентов программного обеспечения ИС., Структуру и основные правила разработки презентаций разрабатываемых ИС., Языки программирования и базы данных; основы современных систем управления базами данных. , Предметную область автоматизации; методы верификации требований к информационной системе. Правила деловой переписки., Принципы ведения отчетности по статусу конфигурации ИС, организации исполнения работ проекта в соответствии с полученным планом., Теоретические принципы проектирования и ведения систем баз данных, управления доступом к данным и защиты данных от разрушения. Умеет: Проводить тестирование компонентов программного обеспечения ИС., Проводить презентации, переговоры, публичные выступления; организовывать эффективные презентации разрабатываемых ИС с учетом аудитории, которой представляется презентация., Разрабатывать программное обеспечение на языках программирования высокого уровня, проектировать базы данных., Анализировать функциональные и нефункциональные требования к информационной системе; анализировать исходные данные. Документировать процессы создания информационных систем на стадиях жизненного цикла., Проводить анализ рисков в проектах в области ИТ в соответствии с полученным заданием., Применять теоретические принципы проектирования и ведения систем баз данных, управления доступом к данным и защиты данных от разрушения. Имеет практический

	опыт: Тестирования компонентов программного обеспечения ИС., Применения соответствующего прикладного программного обеспечения для разработки презентаций., Кодирования на языках программирования; тестирования результатов прототипирования., Выявления первоначальных требований заказчика к ИС; сбора исходных данных у заказчика; разработки моделей бизнес-процессов; составления технической документации проектов автоматизации и информатизации прикладных процессов., Сбора информации для инициализации проекта в соответствии с полученным заданием., Разработки базы данных информационных систем с учетом требований информационной безопасности.
1.Ф.09 Высокоуровневые методы информатики и программирования	Знает: Основные понятия реляционных баз данных, Способы тестирования программного обеспечения., Способы и приёмы программирования приложений. Языки программирования C++ и C# Умеет: Осуществлять ведение базы данных, используя возможности современных языков программирования., Тестировать компоненты программного обеспечения ИС, Разрабатывать и адаптировать прикладное программное обеспечение Имеет практический опыт: Работы с различными системами управления базами данных, в частности, MS Access и MS SQL Server, Использования различных отладочных средств для тестирования программного обеспечения., Использования интегрированной среды разработки программных продуктов Microsoft Visual Studio
1.Ф.12 Интернет-программирование	Знает: Особенности и правила тестирования интернет-приложений, Язык разметки HTML, правила разработки таблицы стилей CSS. Язык программирования клиентской части интернет-приложения JavaScript и серверной части PHP, Правила работы с базами данных в интернет-приложениях Умеет: Разрабатывать план тестирования интернет-приложения, Разрабатывать и адаптировать интернет-приложения, Разрабатывать интернет-приложения, работающие с базами данных Имеет практический опыт: Работы с отладочными средствами клиентских и серверных частей интернет-приложений, Использования сред разработки и отладки интернет-приложений, Ведения базы данных и поддержки информационного обеспечения решения задач прикладной области с использованием возможностей интернет-приложений.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 18,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	12	12
Лекции (Л)	8	8
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	4	4
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	89,75	89,75
Совместная работа, организация взаимодействия команды на основе внешних решений	45,75	45.75
Подготовка к зачету	16	16
Работа в письменной форме с устным докладом	28	28
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Информационная безопасность и уровни ее обеспечения.	2	2	0	0
2	Криптографические способы защиты информации	2	2	0	0
3	Антивирусная защита	2	2	0	0
4	Информационная безопасность вычислительных сетей. Одноранговые сети, построение, безопасность, настройка маршрутизации	2	0	2	0
5	Доменные сети. построение, администрирование	2	0	2	0
6	Системы доступа, фаерволы, маршрутизация	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	2
2	2	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля.	2

		Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Криптографическая система RSA. Криптосистемы. Простые криптосистемы.	
3	3	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	2
4	6	Системы обеспечения сервисов, серверы доступа, серверы приложений, доменная организация прав пользователей	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	4	Конфигурирование VirtualBox. Настройка одноранговых сетей	2
2	5	Установка серверной ОС, настройка контроллера домена. Включение в домен серверов и рабочих станций	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Совместная работа, организация взаимодействия команды на основе внешних решений	https://docs.google.com/	9	45,75
Подготовка к зачету	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с.; Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. ; Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. ; Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с.	9	16
Работа в письменной форме с устным докладом	https://www.youtube.com/c/NETVN82 https://www.youtube.com/playlist?list=PLF27492BD5FCA29C0	9	28

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	9	Текущий контроль	Установка одноранговой сети	1	5	Группа делится на мини группы по 2 человека. Каждой подгруппе выдается индивидуальное задание, связанное с созданием виртуальной машины и одноранговой сети. При оценивании результатов работы используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 5 баллов выставляется если студент демонстрирует правильно созданную одноранговую сеть, проведено правильное конфигурирование виртуальных машин, правильно и четко отвечает на вопросы по работе, понимает и разбирается в терминах; 4 балла выставляется если студент демонстрирует правильно созданную одноранговую сеть, виртуальная машина сконфигурирована с ошибками, понимает и разбирается в терминах, отвечает на вопросы преподавателя с уточнением; 3 балла выставляется если студент демонстрирует созданную одноранговую сеть и виртуальную машину, но есть замечание по проделанной работе, правильно и четко отвечает на вопросы, понимает и разбирается в терминах; 2 балла выставляется если студент демонстрирует созданную одноранговую сеть, но есть замечание по проделанной работе, виртуальная машина сконфигурирована с замечаниями, на вопросы отвечает с уточнением; 1 балл выставляется если студент создал одноранговую сеть с грубыми ошибками, виртуальная машина сконфигурирована с замечаниями, на вопросы преподавателя отвечает с замечаниями; 0 баллов выставляется если студент не демонстрирует одноранговую сеть, виртуальная машина	зачет

						сконфигурирована неверно или не может ответить на вопросы преподавателя.	
2	9	Текущий контроль	Установка виртуальной машины для стенда	1	5	Группа делится на мини группы по 2 человека. Каждой подгруппе выдается индивидуальное задание, связанное с созданием виртуальной машины. При оценивании результатов работы используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 5 баллов выставляется если студент демонстрирует правильно созданную сеть виртуальных машин, проведено правильное конфигурирование виртуальных машин, правильно и четко отвечает на вопросы по работе, понимает и разбирается в терминах; 4 балла выставляется если студент демонстрирует конфигурацию виртуальных машин с ошибками, но при защите с помощью преподавателя исправляет их, понимает и разбирается в терминах, отвечает на вопросы преподавателя с уточнением; 3 балла выставляется если студент демонстрирует созданные виртуальные машины с ошибками, правильно и четко отвечает на вопросы, понимает и разбирается в терминах; 2 балла выставляется если студент демонстрирует созданную сеть виртуальных машин с ошибками и при защите не все ошибки может исправить, на вопросы отвечает с уточнением; 1 балл выставляется если студент создал сеть виртуальных машин с грубыми ошибками, на вопросы преподавателя отвечает с замечаниями; 0 баллов выставляется если студент не демонстрирует виртуальную машину или не может ответить на вопросы преподавателя.	зачет
3	9	Текущий контроль	Защита доклада	1	6	Для подготовки к докладу студентам выдаются темы для самостоятельного изучения. Доклад по теме готовится индивидуально. Защита доклада сопровождается презентацией, ответами на вопросы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: - содержание: 2 балла – содержание полностью соответствует теме доклада, тема раскрыта полностью; 1 балл –	зачет

						содержание доклада не полностью соответствует теме и/или раскрыты не все аспекты темы; 0 баллов – содержание доклада не соответствует теме. - - оформление: 2 балла – презентация оформлена в соответствии с выданным заданием; 1 балл – в презентации выявлены недочеты; 0 баллов – студент неверно оформил презентацию или не выполнил задание. - срочность: 2 балла – доклад защищен в назначенный срок; 1 балл – доклад защищен на следующем занятии или консультации, после назначенного срока; 0 баллов – доклад защищен позднее, чем на следующем занятии или консультации.	
4	9	Проме-жуточная аттестация	Зачет	-	15	Зачет проводится в устной форме. Каждому студенту выдается билет с 3 вопросами. Время на подготовку отводится 30 минут. За каждый вопрос выставляется баллы. Максимальный балл за вопрос - 5. 5 баллов - Грамотный полный (развернутый) ответ на теоретический вопрос; 4 балла - дан правильный, но краткий ответ на вопрос; 3 балла - дан в общем правильный ответ на вопрос, но с замечаниями; 2 балла - дан неполный ответ на вопрос, но на уточняющие вопросы отвечено; 1 балл - дан неправильный ответ на вопрос, но на уточняющие вопросы даны правильные ответы; 0 -баллов - ответ на вопрос не дан.	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	На зачете происходит оценивание знаний, умений и приобретенного опыта обучающихся по дисциплине "Информационная безопасность" на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. При недостаточной и/или не устраивающей студента величине рейтинга ему может быть предложено пройти собеседование с преподавателем по основным разделам дисциплины. В результате складывается совокупный рейтинг студента, который позволяет получить зачет по дисциплине, который проставляется в ведомость, зачетную книжку студента. Зачтено: Величина рейтинга обучающегося по дисциплине 60% и более. Не зачтено: Величина рейтинга обучающегося по дисциплине 0…59 %.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№

		КМ			
		1	2	3	4
ПК-2	Знает: Знание современных законов, стандартов, методов и технологий в области защиты информации	+	+	+	+
ПК-2	Умеет: Использовать современные программно-аппаратные средства защиты информации. Находить потенциальные уязвимости в коде приложений.	+	+	+	+
ПК-2	Имеет практический опыт: Владения современными методами и средствами обеспечения защиты информации.	+	+		+
ПК-4	Знает: Принципы безопасного проектирования базы данных информационных систем.	+	+	+	+
ПК-4	Умеет: Обосновывать экономическую оправданность информационной защиты.			+	+
ПК-4	Имеет практический опыт: Оценки защищенности базы данных информационных систем.	+	+		+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы [Текст] учеб. для вузов по направлению 552800 "Информатика и вычисл. техника" и по специальностям 220100 "Вычисл. машины, комплексы, системы и сети", 220200 "Автоматизир. системы обработки информ. и упр.", 220400 "Програм. обеспечение вычисл. техники и автоматизир. систем" В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. и др.: Питер, 2008. - 957 с. ил.

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Назаров С.В. Администрирование локальных сетей Windows NT/2000/.NET. Учеб. пособие. 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2008.
2. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер. 2007.

г) методические указания для студентов по освоению дисциплины:

1. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер. 2007.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Методические	Электронно-	Баринов, В.В. Технологии разработки и создания

	пособия для самостоятельной работы студента	библиотечная система издательства Лань	компьютерных сетей на базе аппаратуры D-LINK.Учебное пособие для вузов. [Электронный ресурс] / В.В. Баринов, А.В. Благодаров, Е.А. Богданова, А.Н. Пылькин. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 216 с. https://e.lanbook.com/book/11826
2	Основная литература	Электронно-библиотечная система издательства Лань	Чекмарев, Ю.В. Вычислительные системы, сети и телекоммуникации. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2009. — 184 с. — Режим доступа: http://e.lanbook.com/book/1146 — Загл. с экрана.
3	Основная литература	Электронно-библиотечная система издательства Лань	Платунова, С.М. Администрирование вычислительных сетей на базе MS Winsows Server 2008. Учебное пособие. [Электронный ресурс] — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 41 с. https://e.lanbook.com/book/70799
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175506 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
6	Дополнительная литература	Электронно-библиотечная система издательства Лань	Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
7	Дополнительная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
8	Основная литература	Электронно-библиотечная система издательства Лань	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

			https://e.lanbook.com/book/133924 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
9	Основная литература	Образовательная платформа Юрайт	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741 (дата обращения: 22.01.2022).

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (https://edu.susu.ru)(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Практические занятия и семинары	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Самостоятельная работа студента	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Зачет,диф.зачет	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор