ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Худякова Т. А.
Пользователь: khudiakovata
Дата подписания: 02.06.2022

Т. А. Худякова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.М1.06 Системы обеспечения информационной безопасности
для направления 38.04.05 Бизнес-информатика
уровень Магистратура
магистерская программа Бизнес-аналитика в экономике и управлении
форма обучения очная
кафедра-разработчик Цифровая экономика и информационные технологии

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.04.05 Бизнес-информатика, утверждённым приказом Минобрнауки от 12.08.2020 № 990

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

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Худякова Т. А.
Пользователь: khudiakovata
Дата подписания: 02.06.2022

Т. А. Худякова

Разработчик программы, преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зайцев А. В.
Пользователь: zaitsevav
Дата подписания: 02.06.2022

А. В. Зайцев

Челябинск

1. Цели и задачи дисциплины

Цель изучения дисциплины - получить базовые знания в области защиты информации в корпоративных информационных системах (КИС). Задачи изучения дисциплины: освоение методов защиты рабочих станций и серверов, входящих в состав КИС; получение навыков проектирования, внедрения и сопровождения эксплуатации защищенных каналов передачи информации в распределенных корпоративных информационных системах.

Краткое содержание дисциплины

Защищенность информационной среды организации и ее составной части КИС — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности КИС должен быть неотъемлемой частью системы управления любой организации. Дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения КИС, практическими приемами защиты рабочих станций и серверов, составляющих КИС.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Знает: Принципы формирования политики информационной безопасности в информационных системах на всех этапах ИТ-проекта Умеет: Разрабатывать частные политики информационной безопасности информационных систем ИТ-проекта Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите Разрабатывать модели угроз и нарушителей информационной безопасности информационных систем на всех этапах жизненного цикла проекта Имеет практический опыт: Организации службы защиты информации на предприятии при реализации ИТ-проекта Оценки уровня риска информационных угроз в информационных системах
ПК-4 Способен выполнять работы и управлять проектами по созданию и модификации информационных систем на основании современных стандартов и методик моделирования бизнес-процессов на всех стадиях жизненного цикла	Знает: Концепцию информационной безопасности, конституционные и законодательные основы ее реализации Направления и методы обеспечения безопасности информационных ресурсов Стандарты информационной безопасности Критерии оценки информационной безопасности информационных систем Умеет: Проводить анализ степени защищенности информации Выявлять угрозы

	несанкционированного доступа к информации Имеет практический опыт: Практического обеспечения защиты информации и безопасного использования программных средств в информационных системах Ведения аналитической работы по выявлению угроз Использования средств и систем защиты информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Проектирование и совершенствование архитектуры предприятия, Современные технологии прикладного программирования и обработки данных	Внутрифирменное планирование на IT-предприятиях

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

Дисциплина	Требования
Современные технологии прикладного программирования и обработки данных	Знает: Базовые принципы алгоритмизации и программирования, базовые принципы организации реляционных баз данных, Базовые принципы формализации требований к программной системе Умеет: Составлять алгоритм решения задачи, проектировать схему реляционной базы данных, Выполнять постановку задачи на разработку программной системы Имеет практический опыт: Программирования на языке Python, моделирования и оценки моделей с помощью статистических библиотек языка Python, Составления технического задания на разработку программной системы
Проектирование и совершенствование архитектуры предприятия	Знает: Стандарты, подходы, методы и средства создания архитектуры предприятияАктуальные источники профессиональной информации, Основные подходы к проектированию архитектуры предприятияОсновные принципы и методики описания, разработки и документирования архитектуры предприятияМетодологии и инструментальные средства разработки моделей архитектуры предприятияМетодики организации и планирования архитектурного процесса и оценки зрелости архитектуры предприятия, Основные нотации моделирования бизнес-процессовМетоды управления проектами Умеет: Анализировать архитектуру предприятия и выбирать средства для реализации задач по совершенствованию архитектуры предприятия и

	информационных системРассматривать возникающие задачи в междисциплинарном контексте, Проводить переговоры с заинтересованными сторонами; разрабатывать документы по архитектуре предприятия, Разрабатывать и анализировать архитектуру предприятияПрименять современные модели разработки архитектуры предприятияСравнивать различные методики проектирования архитектуры предприятияРазрабатывать планы по созданию и модификации архитектуры предприятияАнализировать исходные данные для проектирования и совершенствования архитектуры предприятия Имеет практический опыт: Планирования и организации проекта создания и развития архитектуры предприятия и информационной системы, Сбора и анализа информации, необходимой для инициации проектов по проектированию архитектуры предприятияПроведения изменений в архитектуре предприятия, Согласования планов разработки архитектуры предприятия с заинтересованными лицамиРазработки рекомендаций по совершенствованию архитектуры предприятия

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	35,75	35,75
Подготовка к зачету	8	8
Подготовка к аудиторным занятиям	7,75	7.75
Подготовка к выполнению практических заданий № 1-4	20	20
Консультации и промежуточная аттестация	4,25	4,25
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	Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности	8	4	4	0
2	Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	8	4	4	0
3	Советы и рекомендации. Практика разработки систем безопасности КИС. Методы безопасного кодирования. Полезные ресурсы.	16	8	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Характерные проблемы, связанные с безопасностью, при использовании КИС. Последствия слабой системы безопасности КИС . Классификация атак на сервисы безопасности КИС. Правила обеспечения безопасности рабочих станций и серверов КИС	2
2	1	Настройка брандмауэров сетевого периметра КИС. Построение демилитаризованной зоны КИС. Настройка персональных брандмауэров рабочих станций и серверов в составе КИС. Администрирование КИС под учетной записью пользователя с минимально необходимым уровнем привилегий	2
3	2	Серверные и клиентские цифровые сертификаты	2
4	2	Безопасные коммуникации на основе TLS/SSL.	2
5	3	Практика разработки систем безопасности КИС.	2
6	3	Методы безопасного кодирования	2
7	3	Факторы безопасности алгоритмов шифрования, хэширования, цифровой подписи	2
8	3	Криптографические стандарты КИС.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Оценка уязвимостей КИС (на примере Nessus, nmap)	2
2	1	Разграничение доступа и обеспечение конфиденциальности данных КИС	2
3	2	Проектирование демилитаризованной зоны (ДМЗ) для защиты периметра КИС от внутренних и внешних сетевых угроз.	2
4	2	Разработка правил внутреннего и внешнего фаерволов ДМЗ	2
5	3	Настройка удаленного доступа к ресурсам КИС.	2
6	3	Защита баз данных и web-приложений КИС	2
7	3	Аудит защищенности КИС	2
8	3	Защита почтовых протоколов, используемых КИС	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
Подготовка к зачету	ПУМД Основная литература: Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия, Дополнительная литература: Правовое обеспечение информационной безопасности Учеб. пособие для вузов по специальностям: 075200 - Компьютер.безопасность, 075500 - Комплекс. обеспечение информ. безопасности автоматизир. систем, 075600 - Информ. безопасность телекоммуникац. систем С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.; Под ред. С. Я. Казанцева. - М.: Академия, 2005. - 238, [1] с. Мельников, В. П. Защита информации [Текст] учебник для вузов по направлению 230100 "Информатика и вычисл. техника" (бакалавриат) В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М.: Академия, 2014. - 296 с. ил., Учебно методическая литература: Защита информации в корпоративных информационных системах: коспект лекций и практических занятий / Б. М. Суховилов – Челябинск: ЮУрГУ. – 40 с. ЭУМД Основная литература: Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247 (дата обращения: 02.06.2022). — Режим доступа: для авториз. пользователей. Дополнительная литература: Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 02.06.2022). — Режим	2	8

	доступа: для авториз. пользователей., Учебно методическая литература: Обеспечение информационной безопасности : методические указания / составители Т. И. Сергеева, М. Ю. Сергеев. — Воронеж : ВГТУ, 2022. — 37 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/222722 (дата обращения: 02.06.2022). — Режим доступа: для авториз. пользователей.		
Подготовка к аудиторным занятиям	ПУМД Основная литература: Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия, Дополнительная литература: Правовое обеспечение информационной безопасности Учеб. пособие для вузов по специальностям: 075200 - Компьютер.безопасность, 075500 - Комплекс. обеспечение информ. безопасности автоматизир. систем, 075600 - Информ. безопасность телекоммуникац. систем С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.; Под ред. С. Я. Казанцева. - М.: Академия, 2005. - 238, [1] с. Мельников, В. П. Защита информации [Текст] учебник для вузов по направлению 230100 "Информатика и вычисл. техника" (бакалавриат) В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М.: Академия, 2014. - 296 с. ил.	2	7,75
Подготовка к выполнению практических заданий № 1-4	Защита информации в корпоративных информационных системах: коспект лекций и практических занятий / Б. М. Суховилов – Челябинск: ЮУрГУ. – 40 с.	2	20

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-ет

							ется в ПА
1	2	Текущий контроль	Контрольное мероприятие (защита выполненных заданий)	1	5	По итогам выполнения практических заданий, структура и содержание которых раскрыты в методических указаниях Защита информации в корпоративных информационных системах (Задание 1 тема Архитектура корпоративных почтовых систем и протоколов;). Студент выполненное задание, загружает в Электронный ЮУрГУ 2.0. Критерии оценивания загруженных работ: 5 баллов - студент выполнил правильно работу, ответил на вопросы; 4 балла - правильно выполнен работу, ответил не на все вопросы; 3 балла - есть замечания по самостоятельным работам, но во время защиты ошибки были исправлены; 2 балла - выполнена самостоятельная работа с ошибками, не на все вопросы даны правильные ответы; 1 балл - работы сделаны с ошибками, сданы после рока; 0 баллов - срок сдачи превысил 2 занятия	зачет
2	2	Текущий контроль	Контрольное мероприятие (защита выполненных заданий)	1	5	По итогам выполнения практических заданий, структура и содержание которых раскрыты в методических указаниях Защита информации в корпоративных информационных системах (Задание 2 тема использование программ с открытыми исходными кодами для обеспечения конфиденциальности корпоративной электронной почты). Студент выполненное задание, загружает в Электронный ЮУрГУ 2.0. Критерии оценивания загруженных работ: 5 баллов - студент выполнил правильно работу, ответил на вопросы; 4 балла - правильно выполнен работу, ответил не на все вопросы; 3 балла - есть замечания по самостоятельным работам, но во время защиты ошибки были исправлены; 2 балла - выполнена самостоятельная работа с ошибками, не на все вопросы даны правильные ответы; 1 балл - работы сделаны с ошибками, сданы после рока; 0 баллов - срок сдачи превысил 2 занятия	зачет
3	2	Текущий контроль	Контрольное мероприятие (защита выполненных заданий)	1	5	По итогам выполнения практических заданий, структура и содержание которых раскрыты в методических указаниях Защита информации в корпоративных информационных системах (Задание 3 тема Анализ и настройка защищенности	зачет

						Интернет-коммуникаций корпоративных почтовых и web-систем;). Студент выполненное задание, загружает в Электронный ЮУрГУ 2.0. Критерии оценивания загруженных работ: 5 баллов - студент выполнил правильно работу, ответил на вопросы; 4 балла - правильно выполнен работу, ответил не на все вопросы; 3 балла - есть замечания по самостоятельным работам, но во время защиты ошибки были исправлены; 2 балла - выполнена самостоятельная работа с ошибками, не на все вопросы даны правильные ответы; 1 балл - работы сделаны с ошибками, сданы после рока; 0 баллов - срок сдачи превысил 2 занятия	
4	2	Текущий контроль	Контрольное мероприятие (защита выполненных заданий)	1	5	По итогам выполнения практических заданий, структура и содержание которых раскрыты в методических указаниях Защита информации в корпоративных информационных системах (Задание 4 тема Использование корпоративного «Центра сертификации» для защиты электронной почты и web-систем.). Студент выполненное задание, загружает в Электронный ЮУрГУ 2.0. Критерии оценивания загруженных работ: 5 баллов - студент выполнил правильно работу, ответил на вопросы; 4 балла - правильно выполнен работу, ответил не на все вопросы; 3 балла - есть замечания по самостоятельным работам, но во время защиты ошибки были исправлены; 2 балла - выполнена самостоятельная работа с ошибками, не на все вопросы даны правильные ответы; 1 балл - работы сделаны с ошибками, сданы после рока; 0 баллов - срок сдачи превысил 2 занятия	зачет
5	2	Проме-жуточная аттестация	Тестирование для повышение рейтинга	-	40	При недостаточной и/или не устраивающей студента величине рейтинга ему может быть предложено пройти тестирование по основным разделам дисциплины. Промежуточная аттестация проводится в форме тестирования по итогам освоения всех разделов дисциплины. Контрольные мероприятия промежуточной аттестации проводятся во время зачета. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена	зачет

						приказом ректора от 24.05.2019 г. № 179). Тест состоит из 40 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 40 мин. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов. Максимальное количество баллов за промежуточную аттестацию - 40 баллов	

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 "Системы обеспечения информационной безопасности" 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	5
УК-2	Знает: Принципы формирования политики информационной безопасности в информационных системах на всех этапах ИТ-проекта	+	+			+
УК-2	Умеет: Разрабатывать частные политики информационной безопасности информационных систем ИТ-проекта Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите Разрабатывать модели угроз и нарушителей информационной безопасности информационных систем на всех этапах жизненного цикла проекта	+	+	+		+
УК-2	Имеет практический опыт: Организации службы защиты информации на предприятии при реализации ИТ-проекта Оценки уровня риска информационных угроз в информационных системах	+	+	+		+
ПК-4	Знает: Концепцию информационной безопасности, конституционные и законодательные основы ее реализации Направления и методы обеспечения безопасности информационных ресурсов Стандарты информационной безопасности Критерии оценки информационной безопасности информационных систем					+
ПК-4	Умеет: Проводить анализ степени защищенности информации Выявлять угрозы несанкционированного доступа к информации	+		+		+
ПК-4	Имеет практический опыт: Практического обеспечения защиты информации и безопасного использования программных средств в информационных	+			+	+

	системах Ведения аналитической работы по выявлению угроз Использования средств и систем защиты информации					

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия

б) дополнительная литература:

1. Правовое обеспечение информационной безопасности Учеб. пособие для вузов по специальностям: 075200 - Компьютер.безопасность, 075500 - Комплекс. обеспечение информ. безопасности автоматизир. систем, 075600 - Информ. безопасность телекоммуникац. систем С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.; Под ред. С. Я. Казанцева. - М.: Академия, 2005. - 238, [1] с.
2. Мельников, В. П. Защита информации [Текст] учебник для вузов по направлению 230100 "Информатика и вычисл. техника" (бакалавриат) В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М.: Академия, 2014. - 296 с. ил.

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

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Обеспечение информационной безопасности : методические указания / составители Т. И. Сергеева, М. Ю. Сергеев. — Воронеж : ВГТУ, 2022. — 37 с

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Обеспечение информационной безопасности : методические указания / составители Т. И. Сергеева, М. Ю. Сергеев. — Воронеж : ВГТУ, 2022. — 37 с

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247 . — Режим

			доступа: для авториз. пользователей.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 . — Режим доступа: для авториз. пользователей.
3	Методические пособия для самостоятельной работы студента	Электронно-библиотечная система издательства Лань	Обеспечение информационной безопасности : методические указания / составители Т. И. Сергеева, М. Ю. Сергеев. — Воронеж : ВГТУ, 2022. — 37 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/222722. — Режим доступа: для авториз. пользователей.

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)
4. -Microsoft Visual Studio (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
Контроль самостоятельной работы	115 (3б)	Компьютерный класс с 30 рабочими станциями с требуемым программным обеспечением, мультимедийное оборудование для показа презентаций
Лекции	265 (2)	Мультимедийное оборудование для показа презентаций
Практические занятия и семинары	115 (3б)	компьютерный класс с 30 рабочими станциями с требуемым программным обеспечением, мультимедийное оборудование для показа презентаций
Самостоятельная работа студента	115 (3б)	Компьютерный класс с 30 рабочими станциями с требуемым программным обеспечением, мультимедийное оборудование для показа презентаций
Зачет,диф.зачет	115 (3б)	Компьютерный класс с установленной тестирующей программой