Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ ТЕСТИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
3	2	72	8	24	0		40	0	З
Итого	2	72	8	24	0	2	40	0	

Москва, 2020

АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ, направленных на тестирование средств защиты информации (СЗИ).

Задачи дисциплины – дать основы разработки тестов, выделить основные понятия, объяснить цели и задачи тестирования, фазы тестирования, роли участников группы тестирования, оценки рисков требований, ранжирование тестов, изменение требований в процессе разработки, методы оценки несоответствия СЗИ, анализ требований к ПО с точки зрения пригодности к тестированию, составление тестов на основе требований, эволюцию автоматизированного тестирования, внедрение автоматизированного тестирования в проект, планирование и подготовку автоматизированного тестирования, проведение тестирования и анализ результатов.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения дисциплины является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ, направленных на тестирование средств защиты информации (СЗИ).

Для этого поставлены основные задачи, которые включают в себя: основы разработки тестов, выделить основные понятия, объяснить цели и задачи тестирования, фазы тестирования, роли участников группы тестирования, оценки рисков требований, ранжирование тестов, изменение требований в процессе разработки, методы оценки несоответствия СЗИ, анализ требований к ПО с точки зрения пригодности к тестированию, составление тестов на основе требований, эволюцию автоматизированного тестирования, внедрение автоматизированного тестирования в проект, планирование и подготовку автоматизированного тестирования, проведение тестирования и анализ результатов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Основы тестирования СЗИ» относится к числу дисциплин специализации «Обеспечение безопасности информации ключевых систем информационной инфраструктуры».

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

- знать основные понятия теории информации, математической логики и информатики, теоретических основ компьютерной безопасности;
- уметь использовать математический аппарат теории вероятностей и дискретной математики;
- владеть основами программирования.

Знания, полученные при изучении дисциплины «Основы аттестации выделенных помещений» являются базовыми, для дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность» по образовательной программе подготовки «Обеспечение безопасности информации ключевых систем информационной инфраструктуры».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем У-ОПК-1 [1] – Уметь: проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности
ОПК-2 [1] – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	З-ОПК-2 [1] – Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации У-ОПК-2 [1] – Уметь: обосновывать применяемые методы решения задач защиты информации, проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов, разрабатывать модели угроз и нарушителей информационной безопасности В-ОПК-2 [1] – Владеть: навыками проектирования систем информационной безопасности

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности	Средства и технологии обеспечения безопасности	ПК-2 [1] - Способен разрабатывать технические задания на проектирование	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и

(СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	значимых объектов критической информационной инфраструктуры	систем обеспечения ИБ иди информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных

			систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от

			несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
научно- исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по

			проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2
2	Второй раздел	9-16			25	КИ-16	З-ОПК-1, У-ОПК-1, В-ОПК-1,

							З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 3 Семестр		8/24/0		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	3 Семестр	8	24	0
1-8	**Первый раздел**	4	12	
1	**Основные понятия** Жизненный цикл разработки ПО. Тестирование ПО.	Всего аудиторных часов 2 Онлайн		
2	**Цели и задачи процесса тестирования** Определение тестирования, ошибка, дефект, отказ, предотвращение и минимизация ошибок до и после выпуска, эффективность тестирования.	Всего аудиторных часов 2 Онлайн		
3	**Определение тестирования** Определение тестирования, ошибка, дефект, отказ, предотвращение и минимизация ошибок до и после выпуска, эффективность тестирования. Анализ документации СЗИ: определение области функционального, нагрузочного и регрессионного тестирования.	Всего аудиторных часов Онлайн	2	
4	**Анализ требований к ПО** Анализ требований к ПО с точки зрения пригодности к тестированию. Составление тестов на основе требований.	Всего аудиторных часов Онлайн	2	
5	**Особенности требований к ПО** Особенности требований к ПО, критерии при тестировании требований, доступность, надежность, производительность, тестирование производительности, переносимость, тестирование конфигураций.	Всего аудиторных часов Онлайн	2	
6	**Оценка рисков** Оценка рисков требований, изменение требований в процессе разработки	Всего аудиторных часов Онлайн	2	
7	**Автоматизация тестирования** Принятие решения об автоматизации тестирования	Всего аудиторных часов Онлайн	2	

8	**Преодоление ложных ожиданий в области автоматизированного тестирования** Преодоление ложных ожиданий в области автоматизированного тестирования, преимущества автоматизированного тестирования, среда системной разработки организации, инструменты, поддерживающие жизненный цикл тестирования, изучение инструмента тестирования, определение оценочной области, практическая оценка инструмента тестирования.	Всего аудиторных часов		
			2	
		Онлайн		
9-16	**Второй раздел**	4	12	
9	**Внедрение автоматизированного тестирования** Внедрение автоматизированного тестирования в проект	Всего аудиторных часов		
		2	2	
		Онлайн		
10	**Анализ процесса тестирования** Анализ процесса тестирования, обзор процессов, цели и задачи тестирования, стратегии тестирования, изучение инструмента тестирования, критический просмотр системных требований проекта, обзор приложения, предназначенного для тестирования.	Всего аудиторных часов		
		2	2	
		Онлайн		
11	**Планирование** Планирование и подготовка тестирования.	Всего аудиторных часов		
			2	
		Онлайн		
12	**Работы по планированию тестирования** Работы по планированию тестирования, среда тестирования, план тестирования, анализ требований к тестам, проектирование тестов, разработка тестов, структура разработки тестов, инфраструктура автоматизации.	Всего аудиторных часов		
			2	
		Онлайн		
13	**Проведение тестирования** Проведение тестирования и анализ результатов.	Всего аудиторных часов		
			1	
		Онлайн		
14	**Фазы тестирования** Фазы тестирования и оценка результатов, отслеживание дефектов и процесс изучения новой версии, отслеживание хода выполнения программы тестирования, изучение и оценка программы тестирования.	Всего аудиторных часов		
			1	
		Онлайн		
15	**Разработка тестовых наборов** Разработка тестовых наборов	Всего аудиторных часов		
			1	
		Онлайн		
16	**Анализ результатов тестирования** Анализ результатов тестирования, дальнейшее совершенствование тестирования.	Всего аудиторных часов		
			1	
		Онлайн		

Сокращенные наименования онлайн опций:

Обозна	**Полное наименование**

чение	
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	3 Семестр
1 - 2	**Основные понятия. Жизненный цикл разработки ПО. Тестирование ПО.** Основные понятия. Жизненный цикл разработки ПО. Тестирование ПО.
3 - 4	**Автоматизация тестирования.** Автоматизация тестирования.
5 - 6	**Анализ документации СЗИ: определение области функционального, нагрузочного и регрессионного тестирования.** Анализ документации СЗИ: определение области функционального, нагрузочного и регрессионного тестирования.
7 - 8	**Выбор инструментов для автоматизации функционального, нагрузочного и регрессионного тестирования.** Выбор инструментов для автоматизации функционального, нагрузочного и регрессионного тестирования.
9 - 10	**Разработка тестовых наборов для функционального тестирования.** Разработка тестовых наборов для функционального тестирования.
11 - 12	**Разработка тестовых наборов для нагрузочного тестирования.** Разработка тестовых наборов для нагрузочного тестирования.
13 - 14	**Разработка тестовых наборов для регрессионного тестирования.** Разработка тестовых наборов для регрессионного тестирования.
15 - 16	**Анализ результатов тестирования, дальнейшее совершенствование тестирования.** Анализ результатов тестирования, дальнейшее совершенствование тестирования.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Практические занятия, самостоятельная работа, контроль знаний проходят в учебно-лабораторном комплексе кафедры.

Лаборатория состоит из 8 автоматизированных рабочих мест студентов (АРМ-У) и автоматизированного рабочего места преподавателя (АРМ-П), объединенных в локальную вычислительную сеть.

Учебно-лабораторный комплекс реализует полный цикл учебно-методических задач по практической подготовке специалистов по тестированию средств защиты информации с использованием специального программного обеспечения для автоматизации тестирования.

В процессе обучения используется специальное программное обеспечение для тестирования – IBM Rational Functional Tester.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ОПК-1	З-ОПК-1	З, КИ-8, КИ-16
	У-ОПК-1	З, КИ-8, КИ-16
	В-ОПК-1	З, КИ-8, КИ-16
ОПК-2	З-ОПК-2	З, КИ-8, КИ-16
	У-ОПК-2	З, КИ-8, КИ-16
	В-ОПК-2	З, КИ-8, КИ-16
ПК-2	З-ПК-2	З, КИ-16
	У-ПК-2	З, КИ-16
	В-ПК-2	З, КИ-16
ПК-3	З-ПК-3	З, КИ-16
	У-ПК-3	З, КИ-16
	В-ПК-3	З, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно

			усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Н 56 Основы информационной безопасности : учебное пособие, Санкт-Петербург: Лань, 2019

2. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Москва: НИЯУ МИФИ, 2018

3. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Москва: НИЯУ МИФИ, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 М 60 Управление рисками информационной безопасности Кн.2 , Москва: Горячая линия - Телеком, 2017

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Целью освоения дисциплины является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ по проведению тестирования СЗИ.

Для этого поставлены основные задачи, которые включают в себя: основы разработки тестов, выделить основные понятия, объяснить цели и задачи тестирования, фазы тестирования, роли участников группы тестирования, оценки рисков требований, ранжирование тестов, изменение требований в процессе разработки, методы оценки несоответствия СЗИ, анализ требований к ПО с точки зрения пригодности к тестированию, составление тестов на основе требований, эволюцию автоматизированного тестирования, внедрение автоматизированного тестирования в проект, планирование и подготовку автоматизированного тестирования, проведение тестирования и анализ результатов.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Аттестация по разделам:

КР8, КИ16 - максим. балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к экзамену.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимание следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Горбатов Виктор Сергеевич, к.т.н., доцент

Рецензент(ы):
Дураковский А.П.