

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**

**ОСОБЕННОСТИ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В СОВРЕМЕННОЙ ЭЛЕКТРОННОЙ  
АППАРАТУРЕ**

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
1	2	72	16	16	0	40	0	3
Итого	2	72	16	16	0	40	0	

## АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ (исследований) по обеспечению технической защиты информации от утечки информации по техническим каналам.

Дисциплина «Особенности каналов утечки информации в современной электронной аппаратуре» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом (ФГОСЗ++), содействует формированию научного мировоззрения и системного мышления; посвящена изучению основных разделов физики, участвующих в процессе переноса информации с помощью технических средств и методам противодействия созданию каналов утечки.

### 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Особенности каналов утечки информации в современной электронной аппаратуре» является формирование общих представлений о методах технической защиты конфиденциальной информации, лежащих в основе обеспечения информационной безопасности и особенностей каналов утечки информации в современной электронной аппаратуре.

Задачи дисциплины – дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области технической защиты конфиденциальной информации (ТЗКИ); порядка выявления утечки информации по техническим каналам; практической отработки методик проведения специальных исследований технических средств обработки информации (ТСОИ) в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации.

В результате обучения студенты должны ознакомиться с:

физическими явлениями, обуславливающими возможные технические каналы утечки информации

устройствами и принципами функционирования защищенных АС,

критериями и методами оценки защищенности АС,

средствами и методами несанкционированного доступа (НСД) к информации АС.

В результате изучения дисциплины студенты должны

иметь представление:

о перспективных направлениях развития теории компьютерной безопасности,

о методах анализа угроз информации,

о архитектуре защищенных АС,

о принципах построения защищенных систем,

о типичных атаках на защищенные АС;

знать:

угрозы и методы нарушения безопасности АС,

формальные модели, лежащие в основе систем защиты АС,

методы и средства реализации защищенных АС,

методы и средства верификации и анализа надежности защищенных АС;

уметь:

реализовывать системы защиты информации в АС;

иметь навыки:

использования критериев оценки защищенности АС,

построения формальных моделей систем защиты информации АС.

Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

Для усвоения учебной дисциплины «Особенности каналов утечки информации в современной электронной аппаратуре» студенты должны знать следующие дисциплины: «Общая алгебра»; «Математический анализ»; «Линейная алгебра»; «Теория вероятностей и математическая статистика»; «Дискретная математика»; «Информатика»; «Теория информации».

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

- знать потенциальные угрозы безопасности информации за счет технических каналов утечки информации;
- уметь использовать математический аппарат теории вероятностей и дискретной математики;
- владеть основами электротехники и радиотехники.

## 3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 [1] – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 [1] – Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 [1] – Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 [1] – Владеть: методологией системного и критического анализа проблемных ситуаций; методиками

	<p>постановки цели, определения способов ее достижения, разработки стратегий действий</p>
<p>ОПК-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</p>	<p>З-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем</p> <p>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.</p> <p>В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности</p>
<p>ОПК-2 [1] – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности</p>	<p>З-ОПК-2 [1] – Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации</p> <p>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</p> <p>В-ОПК-2 [1] – Владеть: навыками проектирования систем информационной безопасности</p>

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары) / Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>1 Семестр</i>						
1	Первый раздел	1-8			25	КИ-8	3-ОПК-

							1, У- ОПК- 1, 3- ОПК- 2, У- ОПК- 2, 3-УК- 1, У- УК-1
2	Второй раздел	9-16			25	КИ-16	3- ОПК- 1, У- ОПК- 1, В- ОПК- 1, 3- ОПК- 2, У- ОПК- 2, В- ОПК- 2, 3-УК- 1, У- УК-1, В- УК-1
	<i>Итого за 1 Семестр</i>		16/16/0		50		
	<b>Контрольные мероприятия за 1 Семестр</b>				50	3	3- ОПК- 1, У- ОПК- 1, В- ОПК- 1, 3- ОПК- 2, У-

							ОПК-2, В-ОПК-2, 3-УК-1, У-УК-1, В-УК-1
--	--	--	--	--	--	--	--

\* – 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.
	<i>1 Семестр</i>	16	16	0
<b>1-8</b>	<b>Первый раздел</b>	8	8	
1 - 4	<b>Тема 1. Организационные вопросы обеспечения информационной безопасности</b> Мероприятия, необходимые для обеспечения защищенности на объекте информатизации. Типовой объект информатизации. Угрозы безопасности информации при потенциальной возможности ее утечки по техническим каналам применительно к типовому объекту информатизации.	Всего аудиторных часов		
		4	4	
		Онлайн		
5 - 8	<b>Тема 2. Причины и физические явления, обуславливающие возможные технические каналы утечки информации</b> Электрические и магнитные поля рассеивания от технических средств обработки информации. Паразитная генерация, возникающая при неустойчивой работе усилителей и генераторов. Акустоэлектрические преобразования на элементах технических средств. Электромагнитные наводки. Информативные сигналы в цепях технических средств обработки информации как источник возникновения технических каналов утечки информации. Другие реализации технических каналов утечки информации. Классификация технических каналов	Всего аудиторных часов		
		4	4	
		Онлайн		

	утечки информации. Угрозы, реализуемые по различным техническим каналам утечки информации.			
9-16	<b>Второй раздел</b>	8	8	
9 - 12	<b>Тема 3. Методы и средства обеспечения безопасности информации на объектах информатизации при ее обработке техническими средствами</b> Экранирование технических средств. Электростатическое экранирование. Магнитостатическое экранирование. Электромагнитное экранирование. Заземление технических средств. Фильтрация информативных сигналов. Пространственное и линейное шумление.	Всего аудиторных часов		
		4	4	
		Онлайн		
13 - 16	<b>Тема 4. Классификация и характеристики методов и средств поиска электронных устройств перехвата информации</b> Демаскирующие признаки электронных устройств перехвата информации. Классификация методов и средств поиска электронных устройств перехвата информации. Средства поиска электронных устройств перехвата информации. Методы поиска электронных устройств перехвата информации. Средства поиска электронных устройств перехвата информации. Организация защиты информации от утечки по техническим каналам. Рекомендации по организации работ по защите информации от утечки по техническим каналам на объектах технических средств обработки информации.	Всего аудиторных часов		
		4	4	
		Онлайн		

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
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
	<i>1 Семестр</i>
1 - 4	<b>Глава 1. Организационные вопросы обеспечения информационной безопасности. Решение задач</b> Мероприятия, необходимые для обеспечения защищенности на объекте информатизации. Типовой объект информатизации. Угрозы безопасности информации при потенциальной возможности ее утечки по техническим каналам применительно к типовому

	объекту информатизации. Решение задач.
5 - 8	<p><b>Глава 2. Причины и физические явления, обуславливающие возможные технические каналы утечки информации. Решение задач</b></p> <p>Электрические и магнитные поля рассеивания от технических средств обработки информации. Паразитная генерация, возникающая при неустойчивой работе усилителей и генераторов. Акустоэлектрические преобразования на элементах технических средств. Электромагнитные наводки. Информативные сигналы в цепях технических средств обработки информации как источник возникновения технических каналов утечки информации. Другие реализации технических каналов утечки информации. Классификация технических каналов утечки информации. Угрозы, реализуемые по различным техническим каналам утечки информации. Решение задач.</p>
9 - 12	<p><b>Глава 3. Методы и средства обеспечения безопасности информации на объектах информатизации при ее обработке техническими средствами. Решение задач.</b></p> <p>Технические каналы утечки информации (ТКУИ) и их особенности. Типовая структура, виды и основные показатели ТКУИ. Побочные электромагнитные излучения и наводки (ПЭМИН). Побочные преобразования акустических сигналов в электрические сигналы. Паразитные связи и наводки. НЧ и ВЧ излучения технических средств. Экранирование технических средств. Электростатическое экранирование. Магнитостатическое экранирование. Электромагнитное экранирование. Заземление технических средств. Фильтрация информативных сигналов. Пространственное и линейное зашумление. Решение задач.</p>
13 - 16	<p><b>Раздел 4. Классификация и характеристики методов и средств поиска электронных устройств перехвата информации. Решение задач</b></p> <p>Демаскирующие признаки электронных устройств перехвата информации. Классификация методов и средств поиска электронных устройств перехвата информации. Средства поиска электронных устройств перехвата информации. Методы поиска электронных устройств перехвата информации. Средства поиска электронных устройств перехвата информации. Организация защиты информации от утечки по техническим каналам. Рекомендации по организации работ по защите информации от утечки по техническим каналам. Решение задач.</p>

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области технической защиты конфиденциальной информации,

организационно-распорядительные, нормативные и информационные документы ГК Росатом, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия по техническим каналам утечки информации, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по атомной энергетике и обеспечению требованиям технической защиты конфиденциальной информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических и семинарских работах.

## 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-16
ОПК-2	З-ОПК-2	З, КИ-8, КИ-16
	У-ОПК-2	З, КИ-8, КИ-16
	В-ОПК-2	З, КИ-16
УК-1	З-УК-1	З, КИ-8, КИ-16
	У-УК-1	З, КИ-8, КИ-16
	В-УК-1	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»	E	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			
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 А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014
2. ЭИ К 77 Методы защиты информации : учебное пособие, Санкт-Петербург: Лань, 2021

### ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 Т38 Технические средства и методы защиты информации : учебное пособие для вузов, Москва: Горячая линия - Телеком, 2009
2. 004 Х79 Защита информации от утечки по техническим каналам Ч.1 Технические каналы утечки информации, , М.: Гостехкомиссия России, 1998

## 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**

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 аттестации объектов информатизации по требованиям безопасности информации от утечки по техническим каналам в современной электронной аппаратуре; 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.

### Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области технической защиты конфиденциальной информации от утечки по техническим каналам в современной электронной аппаратуре, организационно-распорядительные, нормативные и информационные документы ФСБ России, ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, связанные с утечкой по техническим каналам в современной электронной аппаратуре. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических и семинарских занятий по отработке практических навыков использования математических методов и программных средств технической защиты

информации. Результаты, полученные в ходе практических работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные и контрольные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических занятиях.

## **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 аттестации объектов информатизации по требованиям безопасности информации от утечки по техническим каналам в современной электронной аппаратуре; 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.

### **Особенности изучения разделов дисциплины**

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области технической защиты конфиденциальной информации от утечки по техническим каналам в современной электронной аппаратуре, организационно-распорядительные, нормативные и информационные документы ФСБ России, ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, связанные с утечкой по техническим каналам в современной электронной аппаратуре. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических и семинарских занятий по отработке практических навыков использования математических методов и программных средств технической защиты информации. Результаты, полученные в ходе практических работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные и контрольные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических занятиях.

### **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 четко 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):

Гавдан Григорий Петрович

Рецензент(ы):

Дураковский А.П.