

**Министерство науки и высшего образования РФ**  
**Федеральное государственное бюджетное образовательное учреждение**  
**высшего образования**  
**«Национальный исследовательский университет «МЭИ»**

---

Направление подготовки/специальность: 11.03.01 Радиотехника

Наименование образовательной программы: Беспроводные технологии и интернет вещей

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

**Рабочая программа дисциплины**  
**ЗАЩИТА ИНФОРМАЦИИ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	<b>Часть, формируемая участниками образовательных отношений</b>
<b>№ дисциплины по учебному плану:</b>	<b>Б1.Ч.01.02</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>8 семестр - 4;</b>
<b>Часов (всего) по учебному плану:</b>	<b>144 часа</b>
<b>Лекции</b>	<b>8 семестр - 8 часов;</b>
<b>Практические занятия</b>	<b>8 семестр - 4 часа;</b>
<b>Лабораторные работы</b>	<b>не предусмотрено учебным планом</b>
<b>Консультации</b>	<b>8 семестр - 2 часа;</b>
<b>Самостоятельная работа</b>	<b>8 семестр - 128,5 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>8 семестр - 1,2 часа;</b>
<b>включая:</b> <b>Тестирование</b> <b>Решение задач</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	<b>8 семестр - 0,3 часа;</b>

**Москва 2023**

**ПРОГРАММУ СОСТАВИЛ:**

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Шалимова Е.В.
	Идентификатор	Rf4bb1f0c-ShalimovaYV-f267ebd6

(подпись)

Е.В. Шалимова

(расшифровка подписи)

**СОГЛАСОВАНО:**

Заведующий выпускающей  
кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Шиндина Т.А.
	Идентификатор	Rd0ad64b2-ShindinaTA-e12224c9

(подпись)

Т.А. Шиндина

(расшифровка подписи)

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** формирование у обучающихся знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода

### Задачи дисциплины

- подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации; подготовка базовых Теоретических понятий, лежащих в основе инженерно-технической защиты информации; создание представления о роли технических средств добывания (разведки) и защиты конфиденциальной информации на объектах информатизации от утечки по техническим каналам, а также контроле за эффективностью мер защиты;

- развитие способностей к логическому и алгоритмическому мышлению, навыков использования методов и способов инженерно-технической защиты информации; использования современных технических средств для определения технических каналов утечки информации и защиты информационных ресурсов.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-1 Способен осуществлять сбор научно-технической информации для проведения оценочных расчетов отдельных блоков радиоэлектронных устройств (РЭУ), осуществлять разработку функциональных схем РЭУ и компьютерное моделирование отдельных блоков РЭУ	ИД-1 <sub>ПК-1</sub> Умеет проводить сбор и анализ научно-технической информации для проведения оценочных расчетов параметров элементов радиоэлектронных устройств, составлять научно-технические отчеты по результатам работы	знать: - основные руководящие и нормативные документы в сфере инженерно-технической защите информации; - методику организации инженерно-технической защиты информации; - основные принципы организации и методы реализации технической защиты информации.  уметь: - использовать основные принципы и методы инженерно-технической защиты информации; - различать виды защищаемой информации, идентифицировать её источники и носители.
ПК-1 Способен осуществлять сбор научно-технической информации для проведения оценочных расчетов отдельных блоков радиоэлектронных устройств (РЭУ), осуществлять разработку функциональных схем РЭУ и компьютерное	ИД-2 <sub>ПК-1</sub> Знает методы построения функциональных схем радиоэлектронного устройства и умеет выполнять компьютерное моделирование элементов радиоэлектронных устройств по типовым методикам с использованием пакетов прикладных программ	знать: - виды, источники и носители защищаемой информации; - основные угрозы безопасности информации; - методы оценки угрозы инженерно-технического добывания информации; - концепцию инженерно-технической защиты информации.  уметь: - выявлять основные угрозы

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
моделирование отдельных блоков РЭУ		безопасности информации и оценивать их степень; - использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Беспроводные технологии и интернет вещей (далее – ОПОП), направления подготовки 11.03.01 Радиотехника, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа							СР			
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
КПР	ГК	ИККП	ТК											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1. Введение в информационную безопасность	11.54	8	1.0	-	0.5	-	0.02	-	0.02	-	10	-	<p><b><u>Самостоятельное изучение теоретического материала:</u></b> Работа ориентирована на изучение литературных источников, конспектирование основных данных, прохождение пробных тестов по учебному материалу</p> <p><b><u>Изучение материалов литературных источников:</u></b> [6], 34</p>
1.1	Концепция инженерно-технической защиты информации	5.82		0.5	-	0.3	-	0.01	-	0.01	-	5	-	
1.2	Правовое обеспечение информационной безопасности	5.72		0.5	-	0.2	-	0.01	-	0.01	-	5	-	
2	Организационное обеспечение информационной безопасности	11.54		1.0	-	0.5	-	0.02	-	0.02	-	10	-	
2.1	Характеристика угроз безопасности информации	5.82	0.5	-	0.3	-	0.01	-	0.01	-	5	-	<p><b><u>Самостоятельное изучение теоретического материала:</u></b> Работа ориентирована на изучение литературных источников, конспектирование основных данных, прохождение пробных тестов по учебному материалу</p> <p><b><u>Изучение материалов литературных источников:</u></b> [5], 56</p>	
2.2	Технические средства обеспечения информационной безопасности	5.72	0.5	-	0.2	-	0.01	-	0.01	-	5	-		
3	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	36.80	2.0	-	1.0	-	0.96	-	0.04	-	32.8	-	<p><b><u>Самостоятельное изучение теоретического материала:</u></b> Работа ориентирована на изучение литературных источников, конспектирование основных данных, прохождение пробных тестов по учебному материалу</p> <p><b><u>Изучение материалов литературных источников:</u></b></p>	
3.1	Структура и	5.91	0.5	-	0.3	-	0.1	-	0.01	-	5	-		

	принципы функционирования современных вычислительных систем												<b><u>источников:</u></b> [1], 56 [4], 15
3.2	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	6.07	0.5	-	0.2	-	0.36	-	0.01	-	5	-	
3.3	Защита от компьютерных вирусов	11.11	0.5	-	0.3	-	0.3	-	0.01	-	10	-	
3.4	Уничтожение остаточных данных	13.71	0.5	-	0.2	-	0.2	-	0.01	-	12.8	-	
4	Защита от потери информации	48.12	4	-	2.0	-	1.0	-	1.12	-	40	-	<b><u>Самостоятельное изучение теоретического материала:</u></b> Работа ориентирована на изучение литературных источников, конспектирование основных данных, прохождение пробных тестов по учебному материалу
4.1	Защита от потери информации и отказов программно-аппаратных средств	11.91	1	-	0.5	-	0.3	-	0.11	-	10	-	<b><u>Изучение материалов литературных источников:</u></b>
4.2	Защита информационно-программного обеспечения на уровне операционных систем	12.2	1	-	0.5	-	0.2	-	0.5	-	10	-	[2], 34 [3], 67
4.3	Защита информации на уровне систем управления базами данных	12.3	1	-	0.5	-	0.3	-	0.5	-	10	-	
4.4	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	11.71	1	-	0.5	-	0.2	-	0.01	-	10	-	
	Экзамен	36.0	-	-	-	-	-	-	0.3	-	-	35.7	

	Всего за семестр	144.00		8.0	-	4.0	-	2.00	-	1.20	0.3	92.8	35.7	
	Итого за семестр	144.00		8.0	-	4.0	2.00		1.20		0.3	128.5		

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПр – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

## **3.2 Краткое содержание разделов**

### 1. 1. Введение в информационную безопасность

#### 1.1. Концепция инженерно-технической защиты информации

Концепция инженерно-технической защиты информации Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники.

#### 1.2. Правовое обеспечение информационной безопасности

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности.

### 2. Организационное обеспечение информационной безопасности

#### 2.1. Характеристика угроз безопасности информации

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности.

#### 2.2. Технические средства обеспечения информационной безопасности

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации.

### 3. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах

#### 3.1. Структура и принципы функционирования современных вычислительных систем

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.

#### 3.2. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам.



### 3.3. Защита от компьютерных вирусов

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Организация защиты от компьютерных вирусов.

### 3.4. Уничтожение остаточных данных

Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможностью мгновенного уничтожения данных.

## 4. Защита от потери информации

### 4.1. Защита от потери информации и отказов программно-аппаратных средств

Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервирования информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств.

### 4.2. Защита информационно-программного обеспечения на уровне операционных систем

Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.

### 4.3. Защита информации на уровне систем управления базами данных

Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных.

### 4.4. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях

Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования.

## **3.3. Темы практических занятий**

1. "Правовое обеспечение информационной безопасности";
2. "Проведение анализа защищенности объекта защиты информации";

3. "Защита информации";
4. "Средства защиты базы данных".

### **3.4. Темы лабораторных работ** не предусмотрено

### **3.5 Консультации**

#### *Групповые консультации по разделам дисциплины (ГК)*

1. Рассмотрение особенностей правового обеспечения информационной безопасности
2. Рассмотрение особенностей технических средств обеспечения информационной безопасности
3. Рассмотрение способов предотвращения несанкционированного доступа к компьютерным ресурсам и защиты программных средств
4. Рассмотрение особенностей защиты информации в локальных и глобальных компьютерных сетях

### **3.6 Тематика курсовых проектов/курсовых работ** Курсовой проект/ работа не предусмотрены

### 3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)				Оценочное средство (тип и наименование)
		1	2	3	4	
<b>Знать:</b>						
основные принципы организации и методы реализации технической защиты информации	ИД-1ПК-1	+				Тестирование/"Защита информации"
методику организации инженерно-технической защиты информации	ИД-1ПК-1	+				Тестирование/"Правовое обеспечение информационной безопасности"
основные руководящие и нормативные документы в сфере инженерно-технической защите информации	ИД-1ПК-1			+		Тестирование/"Защита информации"
концепцию инженерно-технической защиты информации	ИД-2ПК-1			+		Тестирование/"Защита информации"
методы оценки угрозы инженерно-технического добывания информации	ИД-2ПК-1			+		Тестирование/"Защита информации" Тестирование/"Правовое обеспечение информационной безопасности"
основные угрозы безопасности информации	ИД-2ПК-1			+		Тестирование/"Правовое обеспечение информационной безопасности"
виды, источники и носители защищаемой информации	ИД-2ПК-1			+		Тестирование/"Защита информации"
<b>Уметь:</b>						
различать виды защищаемой информации, идентифицировать её источники и носители	ИД-1ПК-1		+			Решение задач/"Проведение анализа защищенности объекта защиты информации" Решение задач/"Средства защиты базы данных"
использовать основные принципы и методы инженерно-технической защиты информации	ИД-1ПК-1		+			Решение задач/"Средства защиты базы данных"
использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации	ИД-2ПК-1				+	Решение задач/"Проведение анализа защищенности объекта защиты информации" Решение задач/"Средства защиты базы"

						данных"
выявлять основные угрозы безопасности информации и оценивать их степень	ИД-2ПК-1				+	Решение задач/"Проведение анализа защищенности объекта защиты информации" Решение задач/"Средства защиты базы данных"

## **4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)**

### **4.1. Текущий контроль успеваемости**

#### **8 семестр**

Форма реализации: Выполнение задания

1. "Проведение анализа защищенности объекта защиты информации" (Решение задач)
2. "Средства защиты базы данных" (Решение задач)

Форма реализации: Компьютерное задание

1. "Защита информации" (Тестирование)
2. "Правовое обеспечение информационной безопасности" (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

### **4.2 Промежуточная аттестация по дисциплине**

#### *Экзамен (Семестр №8)*

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ "МЭИ"

В диплом выставляется оценка за 8 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## **5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **5.1 Печатные и электронные издания:**

1. Андрианов, В. И. Устройства для защиты объектов информации : Справочное пособие / В. И. Андрианов, А. В. Соколов . – 2-е изд., перераб. и доп. – СПб. : Полигон, 2000 . – 256 с. – (Шпионские штучки) . - ISBN 5-89173-075-8 : 71.00 .;
2. Анин, Б. Ю. Защита компьютерной информации / Б. Ю. Анин . – СПб. : BHV, 2000 . – 384 с. - ISBN 5-8206-0104-1 : 81.20 .;
3. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова . – М. : РИОР : ИНФРА-М, 2018 . – 110 с. – (Научная мысль) . - ISBN 978-5-369-01680-0 .;
4. Акмаров П. Б.- "Кодирование и защита информации", Издательство: "Ижевская ГСХА", Ижевск, 2016 - (136 с.)  
<https://e.lanbook.com/book/133975>;
5. А. А. Титов- "Инженерно-техническая защита информации", Издательство: "Томский государственный университет систем управления и радиоэлектроники", Томск, 2010 - (195 с.)  
<https://biblioclub.ru/index.php?page=book&id=208567>;
6. А. Б. Арзуманян- "Международные стандарты правовой защиты информации и информационных технологий", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2020 - (140 с.)  
<https://biblioclub.ru/index.php?page=book&id=612162>.

## 5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

## 5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - [http://biblioclub.ru/index.php?page=main\\_ub\\_red](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>
4. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
5. Портал открытых данных Российской Федерации - <https://data.gov.ru>
6. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
7. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
8. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
9. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
10. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
11. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
12. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
13. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>
14. Официальный сайт Министерства науки и высшего образования Российской Федерации - <https://minobrnauki.gov.ru>
15. Официальный сайт Федеральной службы по надзору в сфере образования и науки - <https://obrnadzor>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Ж-417/6, Белая мультимедийная студия	стол компьютерный, доска интерактивная, компьютерная сеть с выходом в Интернет, мультимедийный проектор, компьютер персональный
	Ж-417/7, Световая черная студия	стул, компьютерная сеть с выходом в Интернет, микрофон, мультимедийный проектор, экран, оборудование специализированное, компьютер персональный
Учебные аудитории для проведения практических занятий, КР и КП	Ж-417/1, Компьютерный класс ИДДО	стол преподавателя, стол компьютерный, шкаф для документов, шкаф для одежды, стол письменный, компьютерная сеть с выходом в Интернет, доска маркерная передвижная, компьютер персональный, принтер,

		кондиционер, стенд информационный
Учебные аудитории для проведения промежуточной аттестации	Ж-417/1, Компьютерный класс ИДДО	стол преподавателя, стол компьютерный, шкаф для документов, шкаф для одежды, стол письменный, компьютерная сеть с выходом в Интернет, доска маркерная передвижная, компьютер персональный, принтер, кондиционер, стенд информационный
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	Ж-2006, Конференц-зал ИДДО	стол, стул, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	Ж-417 /2а, Помещение для инвентаря	стеллаж для хранения инвентаря, экран, указка, архивные документы, дипломные и курсовые работы студентов, канцелярский принадлежности, спортивный инвентарь, хозяйственный инвентарь, запасные комплектующие для оборудования

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

## Защита информации

(название дисциплины)

## 8 семестр

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 "Правовое обеспечение информационной безопасности" (Тестирование)

КМ-2 "Проведение анализа защищенности объекта защиты информации" (Решение задач)

КМ-3 "Защита информации" (Тестирование)

КМ-4 "Средства защиты базы данных" (Решение задач)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	3	6	9	12
1	1. Введение в информационную безопасность					
1.1	Концепция инженерно-технической защиты информации				+	
1.2	Правовое обеспечение информационной безопасности		+			
2	Организационное обеспечение информационной безопасности					
2.1	Характеристика угроз безопасности информации			+		+
2.2	Технические средства обеспечения информационной безопасности					+
3	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах					
3.1	Структура и принципы функционирования современных вычислительных систем				+	
3.2	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств				+	
3.3	Защита от компьютерных вирусов		+		+	
3.4	Уничтожение остаточных данных				+	
4	Защита от потери информации					
4.1	Защита от потери информации и отказов программно-аппаратных средств			+		+
4.2	Защита информационно-программного обеспечения на уровне операционных систем			+		+
4.3	Защита информации на уровне систем управления базами данных			+		+



4.4	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях		+		+
Вес КМ, %:		25	25	25	25