

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

---

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная


**Рабочая программа дисциплины**  
**ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	Базовая
<b>№ дисциплины по учебному плану:</b>	Б1.Б.29
<b>Трудоемкость в зачетных единицах:</b>	8 семестр - 4;
<b>Часов (всего) по учебному плану:</b>	144 часа
<b>Лекции</b>	8 семестр - 16 часов;
<b>Практические занятия</b>	8 семестр - 16 часов;
<b>Лабораторные работы</b>	не предусмотрено учебным планом
<b>Консультации</b>	8 семестр - 2 часа;
<b>Самостоятельная работа</b>	8 семестр - 109,5 часов;
<b>в том числе на КП/КР</b>	не предусмотрено учебным планом
<b>Иная контактная работа</b>	проводится в рамках часов аудиторных занятий
<b>включая:</b>	
<b>Коллоквиум</b>	
<b>Деловая игра</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	8 семестр - 0,5 часа;

**Москва 2019**

**ПРОГРАММУ СОСТАВИЛ:**


Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

А.С. Минзов


**СОГЛАСОВАНО:**

Руководитель  
образовательной программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

О.Р. Баронов

Заведующий выпускающей  
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю. Невский

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** формирование у студентов системы знаний о принципах, методах, подходах и инструментах эффективного управления информационной безопасностью в современной организации на основе использования системного подхода

### Задачи дисциплины

- получение обучаемыми знаний в области управления информационной безопасностью корпоративных информационных систем на основе концепции управления PDCA;
- формирование знаний в сфере моделирования процессов управления на основе различных подходов к управлению рисками информационной безопасности;
- изучение методов и технологий работы с первичными руководящими документами и стандартами в сфере управления информационной безопасностью.

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
ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности		знать: - основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ.  уметь: - использовать правовые нормы для управления рисками информационной безопасности; - определять необходимые правовые нормы для формирования политик информационной безопасности.
ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		знать: - основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах.  уметь: - определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
ПК-10 способностью проводить анализ информационной безопасности объектов и		знать: - основные требования стандартов в области информационной безопасности.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
систем на соответствие требованиям стандартов в области информационной безопасности		<p>уметь:</p> <ul style="list-style-type: none"> <li>- использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации.</li> </ul>
ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации		<p>знать:</p> <ul style="list-style-type: none"> <li>- методы управления СМИБ на основе методик управления рисками.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- использовать полученные в процессе обучения знания для проведения анализа состояния объектов и систем на соответствие требованиям стандартов по информационной безопасности.</li> </ul>
ОК-8 способностью к самоорганизации и самообразованию		<p>знать:</p> <ul style="list-style-type: none"> <li>- содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей совершенствования</li> </ul> <p>Индивидуальный устный опрос, письменный опрос, тестирование в профессиональной деятельности.</p> <p>уметь:</p> <ul style="list-style-type: none"> <li>- работать самостоятельно и в коллективе, руководить людьми и подчинять личные интересы общей цели; формулировать результат; публично представить собственные и известные научные результаты.</li> </ul>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, 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	Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008	24	8	4	-	4	-	-	-	-	-	16	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008"</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><b><u>Подготовка доклада, выступления:</u></b> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в</p>	
1.1	Введение в курс. Термины и определения	12		2	-	2	-	-	-	-	-	-	8		-
1.2	Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008	12		2	-	2	-	-	-	-	-	-	8		-

													<p>форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008" подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008"</p> <p><b><u>Изучение материалов литературных источников:</u></b></p> <p>[1], 6-14 [2], 9-19</p>
2	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)	38	8	-	4	-	-	-	-	-	26	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)"</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)" материалу.</p>
2.1	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)	38	8	-	4	-	-	-	-	-	26	-	<p>Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)" материалу.</p>

														<p>Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><b><u>Подготовка доклада, выступления:</u></b> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)" <b><u>Изучение материалов литературных источников:</u></b> [1], 33-63</p>
3	Разработка СМИБ на примере АКБ (деловая ситуация)	46		4	-	8	-	-	-	-	-	34	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Разработка СМИБ на примере АКБ (деловая ситуация)"</p>
3.1	Разработка СМИБ на примере АКБ (деловая ситуация)	46		4	-	8	-	-	-	-	-	34	-	<p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы <b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Разработка СМИБ на примере АКБ (деловая ситуация)" материалу. Дополнительно студенту необходимо изучить литературу и</p>

														разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Разработка СМИБ на примере АКБ (деловая ситуация)" подготовка к выполнению заданий на практических занятиях <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Разработка СМИБ на примере АКБ (деловая ситуация)" <b><u>Изучение материалов литературных источников:</u></b> [1], 76-83
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5		
	Всего за семестр	144.0	16	-	16	-	2	-	-	0.5	76	33.5		
	Итого за семестр	144.0	16	-	16		2		-	0.5		109.5		

**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. Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008

##### 1.1. Введение в курс. Термины и определения

Введение в дисциплину. Термины и определения. Системы менеджмента и оценка возможности их применения в сфере информационной безопасности. Концепции систем управления информационной безопасностью. Методы моделирования процессов и деятельности. Практическое задание по анализу различных подходов по управлению информационной безопасностью с использованием методов системного анализа.

##### 1.2. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008

Концепция защиты информации в системе стандартов ГОСТ ИСО/МЭК 27000. Назначение и взаимосвязи отдельных стандартов. Общие подходы по защите информации в информационных системах на основе стандарта ГОСТ ИСО/МЭК 27001: требования, порядок организации защиты на основе процессного подхода. Анализ основных этапов создания системы менеджмента информационной безопасности (СМИБ) с использованием методологии моделирования IDEF0. Основные документы, разрабатываемые в СМИБ..

#### 2. Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)

##### 2.1. Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)

Политика безопасности и последовательность ее разработки. Организация ИБ. Управление активами и определение их ценности. Безопасность, определяемая персоналом. Физическая безопасность и защита от воздействия окружающей среды. Управление коммуникациями и работами. Управление доступом. Приобретение, разработка и эксплуатация информационных систем. Менеджмент инцидентов. Менеджмент непрерывности бизнеса..

#### 3. Разработка СМИБ на примере АКБ (деловая ситуация)

##### 3.1. Разработка СМИБ на примере АКБ (деловая ситуация)

Принципы сертификации и последовательность ее реализации. Необходимые документы при проведении сертификации..

### **3.3. Темы практических занятий**

1. Коллоквиум 2. Моделирование процессов управления СМИБ в стандарте IDEF0.;
2. Контрольное задание 4. Деловая игра. Подготовка положения о применимости системы СМИБ.;
3. Контрольное задание 3. Деловая игра. Оценка рисков.;
4. Контрольное задание 2. Деловая игра. Разработка методологии оценки рисков.;
5. Контрольное задание 1. Деловая игра. Разработка политики СМИБ.;
6. Коллоквиум 4. Моделирование процессов управления рисками в различных концепциях.;
7. Коллоквиум 3. Формализованное представление документов СМИБ.;
8. Коллоквиум 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000.

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

### **3.5 Консультации**

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

1. Обсуждение материалов по теме 1
2. Обсуждение материалов по теме 2
3. Обсуждение материалов по теме 3
4. Обсуждение материалов по теме 4
5. Обсуждение материалов по кейсам раздела "Разработка СМИБ на примере АКБ (деловая ситуация)"

#### *Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Разработка СМИБ на примере АКБ (деловая ситуация)"

### **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	
<b>Знать:</b>					
основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ	ОПК-5(Компетенция)	+			Коллоквиум/КМ-1
основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах	ОПК-7(Компетенция)	+			Коллоквиум/КМ-1
основные требования стандартов в области информационной безопасности	ПК-10(Компетенция)			+	Деловая игра/КМ-3
методы управления СМИБ на основе методик управления рисками	ПК-13(Компетенция)	+			Коллоквиум/КМ-2
содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей совершенствования Индивидуальный устный опрос, письменный опрос, тестирование в профессиональной деятельности	ОК-8(Компетенция)			+	Деловая игра/КМ-3
<b>Уметь:</b>					
определять необходимые правовые нормы для формирования политик информационной безопасности	ОПК-5(Компетенция)		+		Коллоквиум/КМ-2
использовать правовые нормы для управления рисками информационной безопасности	ОПК-5(Компетенция)		+		Коллоквиум/КМ-2
определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК-7(Компетенция)	+			Коллоквиум/КМ-1
использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	ПК-10(Компетенция)			+	Деловая игра/КМ-3
использовать полученные в процессе обучения знания для проведения анализа состояния объектов и систем на соответствие требованиям	ПК-13(Компетенция)		+		Коллоквиум/КМ-2

стандартов по информационной безопасности					
работать самостоятельно и в коллективе, руководить людьми и подчинять личные интересы общей цели; формулировать результат; публично представить собственные и известные научные результаты	ОК-8(Компетенция)		+		Коллоквиум/КМ-2

#### **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: Защита задания

1. КМ-3 (Деловая игра)

Форма реализации: Смешанная форма

1. КМ-1 (Коллоквиум)
2. КМ-2 (Коллоквиум)

Балльно-рейтинговая структура дисциплины является приложением А.

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

*Экзамен (Семестр №8)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной / экзаменационной составляющих.

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. Управление событиями информационной безопасности : учебное пособие / А. С. Минзов, О. Р. Баронов, С. А. Минзов, П. А. Осипов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" ; ред. А. Ю. Невский . – Москва : ВНИИгеосистем, 2020 . – 110 с. - Для студентов бакалавриата, магистратуры, аспирантов и преподавателей, занимающихся вопросами создания эффективных систем управления кибербезопасностью . - ISBN 978-5-8481-0244-4 .;
2. А. К. Шилов- "Управление информационной безопасностью", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2018 - (121 с.)  
<https://biblioclub.ru/index.php?page=book&id=500065>.

##### **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. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. Национальная электронная библиотека - <https://rusneb.ru/>
7. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
8. База данных диссертаций ProQuest Dissertations and Theses Global - <https://search.proquest.com/pqdtglobal/index>
9. Журнал Science - <https://www.sciencemag.org/>
10. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
11. Портал открытых данных Российской Федерации - <https://data.gov.ru>
12. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
13. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
14. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
15. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
16. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
17. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>  
<http://docs.cntd.ru/>
18. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
19. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
20. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>
21. Официальный сайт Министерства науки и высшего образования Российской Федерации - <https://minobrnauki.gov.ru>
22. Официальный сайт Федеральной службы по надзору в сфере образования и науки - <https://obrnadzor>
23. Федеральный портал "Российское образование" - <http://www.edu.ru>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Учебные аудитории для проведения промежуточной	М-509, Учебная лаборатория "Инженерно-	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер

аттестации	техническая защита информации"	персональный, кондиционер, телевизор, стенд лабораторный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
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
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

**БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ****Основы управления информационной безопасностью**

(название дисциплины)

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

КМ-1 КМ-1 (Коллоквиум)

КМ-2 КМ-2 (Коллоквиум)

КМ-3 КМ-3 (Деловая игра)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	13
1	Введение в курс. Термины и определения. Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008				
1.1	Введение в курс. Термины и определения		+		
1.2	Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008		+	+	
2	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)				
2.1	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)			+	
3	Разработка СМИБ на примере АКБ (деловая ситуация)				
3.1	Разработка СМИБ на примере АКБ (деловая ситуация)				+
Вес КМ, %:			30	35	35