

**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: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Рабочая программа дисциплины**  
**МАТЕМАТИЧЕСКИЕ МОДЕЛИ РИСКОВ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	Вариативная
<b>№ дисциплины по учебному плану:</b>	Б1.В.09.03.01
<b>Трудоемкость в зачетных единицах:</b>	5 семестр - 4;
<b>Часов (всего) по учебному плану:</b>	144 часа
<b>Лекции</b>	5 семестр - 32 часа;
<b>Практические занятия</b>	5 семестр - 32 часа;
<b>Лабораторные работы</b>	не предусмотрено учебным планом
<b>Консультации</b>	проводится в рамках часов аудиторных занятий
<b>Самостоятельная работа</b>	5 семестр - 79,7 часа;
<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> Семинар Деловая игра	
<b>Промежуточная аттестация:</b>	
<b>Зачет с оценкой</b>	5 семестр - 0,3 часа;

**Москва 2019**

## ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

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

(подпись)

А.С. Минзов

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной программы

(должность, ученая степень, ученое звание)

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

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий выпускающей  
кафедры

(должность, ученая степень, ученое звание)

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

(подпись)

А.Ю. Невский

(расшифровка  
подписи)

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** освоение профессиональных компетенций по моделированию угроз, оценке и анализу рисков информационной безопасности с использованием различных современных методик управления рисками информационной безопасности

### Задачи дисциплины

- получение обучаемыми знаний в области моделирования угроз и управления рисками информационной безопасности в различных концепциях построения систем информационной безопасности.

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-2 способностью применять соответствующий математический аппарат для решения профессиональных задач		знать: - требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины; - основы анализа и синтеза систем информационной безопасности на основе отдельных подсистем и структурных элементов.  уметь: - выполнять работы по компьютерному моделированию и проектированию отдельных элементов систем информационной безопасности на основе управления рисками.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		уметь: - проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программы Организация и технология защиты информации (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	Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности	24	5	8	-	4	-	-	-	-	-	12	-	<p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности" подготовка к выполнению заданий на практических занятиях</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 "Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности" 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 к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности"</p> <p><b><u>Самостоятельное изучение</u></b></p>	
1.1	Введение. Термины и определения. Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса	8		4	-	2	-	-	-	-	-	-	2		-
1.2	Моделирование угроз информационной безопасности	16		4	-	2	-	-	-	-	-	-	10		-



													<u>источников:</u> [1], 1-110	
3	Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков	18	6	-	2	-	-	-	-	-	-	10	-	<b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков"
3.1	Многофакторные модели рисков	18	6	-	2	-	-	-	-	-	-	10	-	<b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков" подготовка к выполнению заданий на практических занятиях <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 рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <b><u>Подготовка к аудиторным занятиям:</u></b> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков" материалу. <b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Управление рисками в концепции стандарта

														ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков" <b><u>Изучение материалов литературных источников:</u></b> [1], 1-110
4	Моделирование рисков информационной безопасности на примере модели филиала АКБ	36		6	-	20	-	-	-	-	-	10	-	<b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Моделирование рисков информационной безопасности на примере модели филиала АКБ" <b><u>Подготовка к аудиторным занятиям:</u></b>
4.1	Моделирование рисков информационной безопасности на примере модели филиала АКБ	36		6	-	20	-	-	-	-	-	10	-	Проработка лекции, выполнение и подготовка к защите лаб. работы <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Моделирование рисков информационной безопасности на примере модели филиала АКБ" <b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Моделирование рисков информационной безопасности на примере модели филиала АКБ" подготовка к выполнению заданий на практических занятиях <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 "Моделирование рисков информационной безопасности на примере модели филиала АКБ" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <b><u>Изучение материалов литературных источников:</u></b>

														[1], 1-110 [2], 215-221
	Зачет с оценкой	18.0	-	-	-	-	-	-	-	0.3	-	17.7		
	Всего за семестр	144.0	32	-	32	-	-	-	-	0.3	62	17.7		
	Итого за семестр	144.0	32	-	32	-	-	-	-	0.3	79.7			

**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. Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности

1.1. Введение. Термины и определения. Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса

Введение. Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков. Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса. История развития методик управления рисками в различных концепциях создания систем информационной безопасности..

#### 1.2. Моделирование угроз информационной безопасности

Цели и задачи моделирования угроз информационной безопасности. Различные подходы к формализованному описанию угроз информационной безопасности. Базовая модель угроз: достоинства и недостатки. Современные подходы к моделированию угроз на основе вербального (описательного), параметрического и когнитивного моделирования. Достоинства и недостатки этих подходов к моделированию угроз..

### 2. Управление рисками в концепциях отечественных и зарубежных стандартов

#### 2.1. Управление рисками в концепции стандарта NIST

Концепция управления рисками в стандарте США NIST 800-30 «Руководство по управлению информационными рисками ИТ-систем». Девять этапов методологии оценки рисков: характеристика системы, идентификация угроз, идентификация уязвимостей, анализ мероприятий защиты, определение вероятностей использования уязвимостей, анализ воздействия, определение рисков, рекомендации по мероприятиям защиты, разработка итоговых документов..

#### 2.2. Управление рисками в концепции стандарта BS 7799-3

Концепция управления рисками в британском стандарте BS-7799-3. Четыре фазы управления рисками: оценка рисков, включающая анализ и вычисление рисков; обработка риска — выбор и реализация мер и средств безопасности; контроль рисков путем мониторинга, тестирования, анализа механизмов безопасности, а также аудита системы; оптимизация рисков путем модификации и обновления правил, мер и средств безопасности. Достоинства и недостатки стандарта. Другие концепции управления рисками: COBIT, CORBA и др..

#### 2.3. Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005

Назначение стандарта. Область действия стандарта и его применимость. Основные этапы процесса менеджмента риска информационной безопасности: установление контекста, оценка риска, обработка риска, принятие риска, коммуникация риска, мониторинг и переоценка риска информационной безопасности. Особенности стандарта и процессный подход к оценке рисков. Сущность и содержание процессного подхода к оценке рисков. Достоинства и недостатки стандарта. Возможные направления его развития.

### 3. Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005.

#### Многофакторные модели рисков

#### 3.1. Многофакторные модели рисков

Концепция многофакторных моделей рисков, позволяющая учитывать кроме основных и дополнительные факторы, а также соотношения между ними. Понятие «стратегия

управления» рисками. Методика анализа рисков с использованием многофакторных моделей. Задачи, решаемые с использованием многофакторных моделей управления рисками. Имитационное моделирование на основе многофакторных моделей. Оценка погрешностей моделирования..

#### 4. Моделирование рисков информационной безопасности на примере модели филиала АКБ

##### 4.1. Моделирование рисков информационной безопасности на примере модели филиала АКБ

Постановка деловой игры. Анализ исходных данных и результатов аудита информационной безопасности. Анализ бизнес-процессов модели хозяйствующего субъекта. Классификация и оценка ценности информационных активов организации. Моделирование угроз информационной безопасности. Оценка и моделирование рисков при различных стратегиях управления ими. Разработка плана управления рисками. Обоснование предлагаемых решений управления рисками..

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

1. Термины и определения;
2. Применение методик моделирования угроз на примере модели хозяйствующего субъекта. Разработка методики моделирования угроз в стандарте IDEF0;
3. Разработка методики управления рисками NIST в стандарте IDEF0;
4. Разработка методики управления рисками BS 7799 в стандарте IDEF0;
5. Разработка методики управления рисками по ГОСТ 27005 в стандарте IDEF0;
6. Разработка методики управления рисками факторных моделей;
7. Управление рисками информационной безопасности на модели хозяйствующего субъекта АКБ «XtrimBank» (деловая игра).

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

### **3.5 Консультации**

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

1. Обсуждение материалов по кейсам раздела "Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Управление рисками в концепциях отечественных и зарубежных стандартов"
3. Обсуждение материалов по кейсам раздела "Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков"
4. Обсуждение материалов по кейсам раздела "Моделирование рисков информационной безопасности на примере модели филиала АКБ"

#### Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление рисками в концепциях отечественных и зарубежных стандартов"

3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Моделирование рисков информационной безопасности на примере модели филиала АКБ"

### **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>						
основы анализа и синтеза систем информационной безопасности на основе отдельных подсистем и структурных элементов	ОПК-2(Компетенция)	+				Семинар/Практическое задание 1 Семинар/Практическое задание 2
требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины	ОПК-2(Компетенция)		+			Семинар/Практическое задание 3 Семинар/Практическое задание 4 Семинар/Практическое задание 5
<b>Уметь:</b>						
выполнять работы по компьютерному моделированию и проектированию отдельных элементов систем информационной безопасности на основе управления рисками	ОПК-2(Компетенция)			+		Семинар/Практическое задание 6
проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	ПК-10(Компетенция)				+	Деловая игра/Деловая игра

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

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

**5 семестр**

Форма реализации: Смешанная форма

1. Деловая игра (Деловая игра)
2. Практическое задание 1 (Семинар)
3. Практическое задание 2 (Семинар)
4. Практическое задание 3 (Семинар)
5. Практическое задание 4 (Семинар)
6. Практическое задание 5 (Семинар)
7. Практическое задание 6 (Семинар)

Балльно-рейтинговая структура дисциплины является приложением А.

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

*Зачет с оценкой (Семестр №5)*

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 5 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. В. Ю. Королев, В. Е. Бенинг, С. Я. Шоргин- "Математические основы теории риска", (2-е изд., перераб. и доп.), Издательство: "Физматлит", Москва, 2011 - (620 с.)  
<https://biblioclub.ru/index.php?page=book&id=457667>.

### **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. Национальная электронная библиотека - <https://rusneb.ru/>
5. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
6. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
7. Портал открытых данных Российской Федерации - <https://data.gov.ru>
8. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
9. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
10. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
11. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
12. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;http://docs.cntd.ru/>
13. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
14. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
15. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>
16. Официальный сайт Министерства науки и высшего образования Российской Федерации - <https://minobrnauki.gov.ru>
17. Официальный сайт Федеральной службы по надзору в сфере образования и науки - <https://obrnadzor>
18. 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	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	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-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной	НТБ-303, Компьютерный	стол компьютерный, стул, стол письменный, вешалка для одежды,

работы	читальный зал	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-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
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

## Математические модели рисков

(название дисциплины)

## 5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Практическое задание 1 (Семинар)  
 КМ-2 Практическое задание 2 (Семинар)  
 КМ-3 Практическое задание 3 (Семинар)  
 КМ-4 Практическое задание 4 (Семинар)  
 КМ-5 Практическое задание 5 (Семинар)  
 КМ-6 Практическое задание 6 (Семинар)  
 КМ-7 Деловая игра (Деловая игра)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7
		Неделя КМ:	4	4	8	8	8	12	15
1	Термины и определения. Цели и задачи курса. Моделирование угроз информационной безопасности								
1.1	Введение. Термины и определения. Цели и задачи курса. Структура дисциплины и требования к результатам изучения курса		+	+					
1.2	Моделирование угроз информационной безопасности		+	+					
2	Управление рисками в концепциях отечественных и зарубежных стандартов								
2.1	Управление рисками в концепции стандарта NIST				+	+	+		
2.2	Управление рисками в концепции стандарта BS 7799-3				+	+	+		
2.3	Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005				+	+	+		
3	Управление рисками в концепции стандарта ГОСТ ИСО/МЭК 27005. Многофакторные модели рисков								
3.1	Многофакторные модели рисков							+	
4	Моделирование рисков информационной безопасности на примере модели филиала АКБ								
4.1	Моделирование рисков информационной безопасности на								+

	примере модели филиала АКБ							
	Вес КМ, %:	10	10	10	10	10	20	30