

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

---

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

**Рабочая программа дисциплины**  
**ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ**  
**БЕЗОПАСНОСТИ**

<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.03</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>1 семестр - 5;</b>
<b>Часов (всего) по учебному плану:</b>	<b>180 часов</b>
<b>Лекции</b>	<b>1 семестр - 32 часа;</b>
<b>Практические занятия</b>	<b>1 семестр - 64 часа;</b>
<b>Лабораторные работы</b>	<b>не предусмотрено учебным планом</b>
<b>Консультации</b>	<b>1 семестр - 2 часа;</b>
<b>Самостоятельная работа</b>	<b>1 семестр - 81,5 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>включая:</b> <b>Отчет</b> <b>Реферат</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	<b>1 семестр - 0,5 часа;</b>

**Москва 2024**

**ПРОГРАММУ СОСТАВИЛ:**

Преподаватель

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

О.Р. Баронов

**СОГЛАСОВАНО:**

Руководитель  
образовательной программы

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

А.С. Минзов

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 обучаемых знаний методов и технологий мониторинга, анализа и обеспечения целостности информации в финансовой, экономической и управленческой деятельности путем интеллектуальной фильтрации совершаемых транзакций в информационных системах с целью противодействия легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

### Задачи дисциплины

- формирование у обучаемых системных теоретических знаний и практических навыков по организации информационно-аналитического обеспечения безопасности;
- приобретение навыков принятия и обоснования решений, направленных на совершенствование системы информационной безопасности на основе использования информационно-аналитических систем безопасности;
- формирование умения творчески мыслить, решая сложные аналитические и трудно формализуемые задачи.

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-2 Способен применять математические методы и инновационные технологии при построении процедур оценки и управления рисками информационной безопасности	ИД-3 <sub>ПК-2</sub> Осуществляет мониторинг защищенности компьютерных систем и сетей, в том числе и инструментальными средствами	знать: - современные технические средства и информационные технологии, используемые для решения задач информационно-аналитической деятельности специалиста в области информационной безопасности.  уметь: - анализировать и содержательно интерпретировать результаты полученные с использованием информационно-аналитических систем безопасности; - использовать отечественные и зарубежные источники информации, собирать необходимые данные анализировать их и готовить информационный обзор и/или аналитический отчет; - выполнять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Базируется на уровне высшего образования (бакалавриат, специалитет).

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 5 зачетных единиц, 180 часов.

№ 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	Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта.	42	1	14	-	14	-	-	-	-	-	14	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта."</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 "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта." 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 форме распечатанных презентационных</p>
1.1	Вводная тема.	6		2	-	2	-	-	-	-	-	2	-	
1.2	Тема 1. Аналитическая работа в повседневной деятельности предприятия в области ИБ.	12		4	-	4	-	-	-	-	-	4	-	
1.3	Тема 2. Системы обеспечения информационной безопасности предприятия	12		4	-	4	-	-	-	-	-	4	-	
1.4	Тема 3. Информационно аналитические системы защиты и безопасности	12		4	-	4	-	-	-	-	-	4	-	

													<p>слайдов. В качестве тем докладов студентам предлагаются следующие варианты:</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта." подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта."</p> <p><b><u>Изучение материалов литературных источников:</u></b> [1], 50-150 [2], 4-45 [3], 152-157 [6], 5-9</p>
2	Информационные технологии в системе информационно-аналитического обеспечения безопасности	102	18	-	50	-	-	-	-	-	34	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Информационные технологии в системе информационно-аналитического обеспечения безопасности"</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 "Информационные технологии в системе информационно-аналитического обеспечения безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры</p>
2.1	Тема 4. Технологии системы информационно-аналитического обеспечения безопасности	8	2	-	4	-	-	-	-	-	2	-	
2.2	Тема 5. DLP-системы функционирование и модель.	8	2	-	4	-	-	-	-	-	2	-	
2.3	Тема 6. Основы функционирования DLP-системы Контур	36	4	-	16	-	-	-	-	-	16	-	

	информационной безопасности SearchInform в информационной системе организации.												выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <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:
2.4	Тема 7. SIEM-системы архитектура и основы функционирования.	11	2	-	6	-	-	-	-	-	3	-	представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:
2.5	Тема 8. «СёрчИнформ SIEM» архитектура и основы функционирования	15	4	-	8	-	-	-	-	-	3	-	<b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Информационные технологии в системе информационно-аналитического обеспечения безопасности" подготовка к выполнению заданий на практических занятиях
2.6	Тема 9. «MaxPatrol SIEM» архитектура и основы функционирования.	24	4	-	12	-	-	-	-	-	8	-	<b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Информационные технологии в системе информационно-аналитического обеспечения безопасности" <b><u>Подготовка реферата:</u></b> В рамках реферативной части студенту необходимо провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: <b><u>Изучение материалов литературных источников:</u></b> [4], 1-110 [5], 1-106
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	

	<b>Всего за семестр</b>	<b>180.0</b>		32	-	64	-	2	-	-	0.5	48	33.5	
	<b>Итого за семестр</b>	<b>180.0</b>		32	-	64	2		-		0.5	81.5		

**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. Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта.**

##### **1.1. Вводная тема.**

Термины и определения в сфере информационно-аналитического обеспечения информационной безопасности. Задачи информационно-аналитического обеспечения безопасности информационных активов в финансовой, экономической и управленческой деятельности..

##### **1.2. Тема 1. Аналитическая работа в повседневной деятельности предприятия в области ИБ.**

Понятие информационно-аналитической работы. Направления аналитической работы. Этапы аналитической работы. Методы аналитической работы. Назначение и общая характеристика аудита информационной безопасности. Характеристика этапов проведения аудита информационной безопасности информационной системы организации..

##### **1.3. Тема 2. Системы обеспечения информационной безопасности предприятия**

Методика построения корпоративной системы обеспечения информационной безопасности. Разновидности аналитических работ по оценке защищенности. Модель и методика корпоративной системы защиты информации. Формирование организационной политики безопасности..

##### **1.4. Тема 3. Информационно аналитические системы защиты и безопасности**

Цель, задачи и характеристика основных направлений деятельности информационно-аналитической системы (ИАС) обеспечения безопасности. Функции информационно-аналитических служб. Характеристика основ использования информационно-аналитических систем безопасности. Общая структура ИАС защиты и безопасности. Инструментальные средства аналитических приложений в ИАСОБ по статическому анализу, динамическому анализу и моделирования и прогнозирования.

#### **2. Информационные технологии в системе информационно-аналитического обеспечения безопасности**

##### **2.1. Тема 4. Технологии системы информационно-аналитического обеспечения безопасности**

Комплексный мониторинг информационных систем в компьютерных системах. Сканеры безопасности информационных систем. Система комплексного мониторинга информационной безопасности MaxPatrol 8. Основы использования MaxPatrol 8. Порядок оценки защищенности информационной системы с использованием MaxPatrol 8. Сканеры безопасности отечественного и зарубежного производства..

##### **2.2. Тема 5. DLP-системы функционирование и модель.**

Основы функционирования DLP-систем в информационной системе организации. Принципы функционирования DLP-систем. Технологии предотвращения утечки информации. Применение DLP-систем и SIEM-систем..

##### **2.3. Тема 6. Основы функционирования DLP-системы Контур информационной безопасности SearchInform в информационной системе организации.**

Назначение, архитектура построения и функциональные возможности DLP-системы «Контур информационной безопасности SearchInform. Принципы функционирования DLP-систем. Сравнительный анализ отечественных и зарубежных DLP-систем. Практическое применение DLP-системы Контур информационной безопасности SearchInform..

2.4. Тема 7. SIEM-системы архитектура и основы функционирования.

Основы функционирования SIEM-систем в информационной системе организации. Архитектура SIEM-систем и их основные функции. Классификация задач, решаемых в SIEM. Сравнительная характеристика зарубежных и отечественных SIEM-систем. Тенденции развития SIEM..

2.5. Тема 8. «СёрчИнформ SIEM» архитектура и основы функционирования

Порядок функционирования . «СёрчИнформ SIEM» в информационной системе организации. Цели и задачи системы «СёрчИнформ SIEM». Архитектура и алгоритм работы системы «СёрчИнформ SIEM». Преимущества продукта «СёрчИнформ SIEM»..

2.6. Тема 9. «MaxPatrol SIEM» архитектура и основы функционирования.

Порядок функционирования . «MaxPatrol SIEM» в информационной системе организации. Цели и задачи системы «MaxPatrol SIEM». Архитектура и алгоритм работы системы «MaxPatrol SIEM». Преимущества продукта «MaxPatrol SIEM».

### 3.3. Темы практических занятий

1. 17. Архитектура и алгоритм работы системы «MaxPatrol SIEM». Преимущества продукта «MaxPatrol SIEM». (4 часа).;
2. 2. Направления аналитической работы. Этапы аналитической работы. Методы аналитической работы (2 часа).;
3. 3. Характеристика этапов проведения аудита информационной безопасности информационной системы организации (2 часа).;
4. 4. Разновидности аналитических работ по оценке защищенности (2 часа).;
5. 5. Модель и методика корпоративной системы защиты информации (2 часа).;
6. 16. Порядок функционирования . «MaxPatrol SIEM» в информационной системе организации (4 часа).;
7. 6. Характеристика основ использования информационно-аналитических систем безопасности (2 часа).;
8. 9. Сканер безопасности MaxPatrol цели, назначение, структура, технологии работы (2 часа).;
9. 10. Основы использования MaxPatrol 8. (4 часа).;
10. 11. Назначение, архитектура построения и функциональные возможности DLP-системы «Контур информационной безопасности SearchInform. (2 часа).;
11. 12. Практическое применение DLP-системы Контур информационной безопасности SearchInform. (16 часов).;
12. 13. SIEM-системы, цели, назначение, структура, технологии работы (2 часа).;
13. 14. Порядок функционирования «СёрчИнформ SIEM» в информационной системе организации. Цели и задачи системы «СёрчИнформ SIEM». (2 часа).;
14. 15. Архитектура и алгоритм работы системы «СёрчИнформ SIEM». Преимущества продукта «СёрчИнформ SIEM». (4 часа).;
15. 8. Сканеры безопасности информационных систем. (2 часа).;
16. 1. Задачи информационно-аналитического обеспечения безопасности информационных активов в финансовой, экономической и управленческой деятельности (2 часа).;
17. 7. Инструментальные средства аналитических приложений в ИАСОБ по

статическому анализу, динамическому анализу и моделирования и прогнозирования (2 часа).;

18. Практическое применение «КОМРАД SIEM» в информационной системе организации (8 часов)..

### **3.4. Темы лабораторных работ**

не предусмотрено

### **3.5 Консультации**

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

1. Обсуждение материалов по кейсам раздела "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта."
2. Обсуждение материалов по кейсам раздела "Информационные технологии в системе информационно-аналитического обеспечения безопасности"

#### Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта."
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Информационные технологии в системе информационно-аналитического обеспечения безопасности"

### **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	
<b>Знать:</b>				
современные технические средства и информационные технологии, используемые для решения задач информационно-аналитической деятельности специалиста в области информационной безопасности	ИД-3ПК-2		+	Отчет/2.Контрольное задание № 2. Практика применения сканера безопасности
<b>Уметь:</b>				
выполнять сбор, анализ и обработку данных, необходимых для решения профессиональных задач аудита информационной безопасности информационных систем и объектов информатизации	ИД-3ПК-2	+	+	Отчет/1.Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации
использовать отечественные и зарубежные источники информации, собирать необходимые данные анализировать их и готовить информационный обзор и/или аналитический отчет	ИД-3ПК-2	+	+	Реферат/Выполнение/защита реферата
анализировать и содержательно интерпретировать результаты полученные с использованием информационно-аналитических систем безопасности	ИД-3ПК-2		+	Отчет/3.Контрольно задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности» Отчет/Контрольное задание № 4. Практика применения MaxPatrol SIEM.

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

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

#### **1 семестр**

Форма реализации: Выполнение задания

1. Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации (Отчет)
2. Контрольное задание № 2. Практика применения сканера безопасности (Отчет)
3. Выполнение/защита реферата (Реферат)
4. Контрольное задание № 4. Практика применения MaxPatrol SIEM. (Отчет)

Форма реализации: Компьютерное задание

1. Контрольное задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности» (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

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

Экзамен (Семестр №1)

В диплом выставляется оценка за 1 семестр.

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

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

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

1. Унижаев, Н. В. ИАО: Информационно-аналитическое обеспечение безопасности организации. (Методы и модели поиска информации, использование новые информационных технологий) / Н. В. Унижаев . – М. : ВНИИГеосистем, 2014 . – 388 с. - ISBN 978-5-8481-0168-3 .;
2. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов . – М. : БИНОМ. Лаборатория знаний : Интернет-Ун-т информ. технологий, 2010 . – 176 с. – (Основы информационных технологий) . - ISBN 978-5-9963-0237-6 .;
3. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие для вузов по специализациям специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / В. И. Васильев . – 2-е изд., испр . – М. : Машиностроение, 2013 . – 172 с. – (Для вузов) . - ISBN 978-5-94275-667-3 .;
4. 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 .;
5. Минзов, А. С. Управление рисками информационной безопасности : [монография] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов ; ред. А. С. Минзов ; Нац. исслед. ун-т "МЭИ"

(НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – Москва : ВНИИгеосистем, 2019 . – 106 с. - ISBN 978-5-8481-0240-6 .;

6. Бахаров Л. Е.- "Информационная безопасность и защита информации", Издательство: "МИСИС", Москва, 2015 - (43 с.)

<https://e.lanbook.com/book/116711>.

## 5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др).

## 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. Электронные ресурсы издательства Springer - <https://link.springer.com/>
5. База данных Web of Science - <http://webofscience.com/>
6. База данных Scopus - <http://www.scopus.com>
7. Национальная электронная библиотека - <https://rusneb.ru/>
8. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
9. Журнал Science - <https://www.sciencemag.org/>
10. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
11. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>  
<http://docs.cntd.ru/>
12. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	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 аттестации	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор,

	информации"	стенд лабораторный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, 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****Информационно-аналитические системы безопасности**

(название дисциплины)

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

- КМ-1 1.Контрольное задание № 1. Практическая разработка этапов проведения аудита информационной безопасности информационной системы организации (Отчет)
- КМ-2 2.Контрольное задание № 2. Практика применения сканера безопасности (Отчет)
- КМ-3 Выполнение/защита реферата (Реферат)
- КМ-3 3.Контрольное задание № 3. Практика применения DLP-системы SearchInform «Контур безопасности» (Отчет)
- КМ-4 Контрольное задание № 4. Практика применения MaxPatrol SIEM. (Отчет)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-3	КМ-4
		Неделя КМ:	4	8	12	12	15
1	Информационно-аналитическая деятельность в системе обеспечения безопасности хозяйствующего субъекта.						
1.1	Вводная тема.		+				
1.2	Тема 1. Аналитическая работа в повседневной деятельности предприятия в области ИБ.		+		+		
1.3	Тема 2. Системы обеспечения информационной безопасности предприятия		+				
1.4	Тема 3. Информационно аналитические системы защиты и безопасности		+				
2	Информационные технологии в системе информационно-аналитического обеспечения безопасности						
2.1	Тема 4. Технологии системы информационно-аналитического обеспечения безопасности			+	+		
2.2	Тема 5. DLP-системы функционирование и модель.			+			
2.3	Тема 6. Основы функционирования DLP-системы Контур информационной безопасности SearchInform в информационной системе организации.		+	+		+	+
2.4	Тема 7. SIEM-системы архитектура и основы функционирования.			+			
2.5	Тема 8. «СёрчИнформ SIEM» архитектура и основы функционирования		+	+	+	+	+
2.6	Тема 9. «MaxPatrol SIEM» архитектура и основы функционирования.		+	+		+	+



Bec KM, %:	25	25	10	15	25
------------	----	----	----	----	----