

**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**  
**СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**  
**ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА**

<b>Блок:</b>	Блок 1 «Дисциплины (модули)»
<b>Часть образовательной программы:</b>	Вариативная
<b>№ дисциплины по учебному плану:</b>	Б1.В.04
<b>Трудоемкость в зачетных единицах:</b>	10 семестр - 6;
<b>Часов (всего) по учебному плану:</b>	216 часов
<b>Лекции</b>	10 семестр - 14 часов;
<b>Практические занятия</b>	10 семестр - 14 часов;
<b>Лабораторные работы</b>	не предусмотрено учебным планом
<b>Консультации</b>	10 семестр - 2 часа;
<b>Самостоятельная работа</b>	10 семестр - 185,5 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>	
<b>Тестирование</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	10 семестр - 0,5 часа;

**Москва 2018**

## ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Потехецкий С.В.
	Идентификатор	R83b30a44-PotekhetskySV-31b213d

(подпись)

С.В. Потехецкий

(расшифровка подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	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)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	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 общекультурных и профессиональных компетенций по системному анализу назначения, организации, построению и структуры системы обеспечения информационной безопасности (СОИБ) на предприятии, а также по вопросам управления ею и порядку оценки ее эффективности

### Задачи дисциплины

- изучение теории по вопросам назначения, целей, решаемых задач, структуры СОИБ и организации ее функционирования в концепции системного подхода;
- формирование готовности и способности к активной профессиональной деятельности по организации и обеспечению функционирования СОИБ в условиях современного информационного противоборства;
- приобретение навыков системного анализа и синтеза сложных организационно-иерархических систем.

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-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: - комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности; - нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО.  уметь: - организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		знать: - комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия.  уметь: - правильно разработать и оформить документы политики информационной безопасности предприятия в различных

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		сферах деятельности, в том числе и на объектах энергетики.
ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности		<p>знать:</p> <ul style="list-style-type: none"> <li>- психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности;</li> <li>- применять системный подход к управлению информационной безопасностью предприятия;</li> </ul>
ПСК-3 Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП		<p>знать:</p> <ul style="list-style-type: none"> <li>- теорию анализа и синтеза сложных организационно-иерархических систем;</li> <li>- состав и перечень информационных активов предприятия, относящихся к защищаемой информации.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса;</li> <li>- составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;</li> </ul>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений 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 6 зачетных единиц, 216 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	Основы организации и функционирования СОИБ предприятия	56	10	3	-	3	-	-	-	-	-	50	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Основы организации и функционирования СОИБ предприятия"</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Основы организации и функционирования СОИБ предприятия" подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Основы организации и функционирования СОИБ предприятия"</p> <p><b><u>Изучение материалов литературных источников:</u></b></p> <p>[1], 1-372 [2], 1-106 [3], 1-48 [4], 1-176</p>	
1.1	Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта	12		1	-	1	-	-	-	-	-	-	10		-
1.2	Система обеспечения информационной безопасности предприятия	32		1	-	1	-	-	-	-	-	-	30		-
1.3	Перечень факторов, влияющих на организацию СОИБ предприятия	12		1	-	1	-	-	-	-	-	-	10		-
2	Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия	124		11	-	11	-	-	-	-	-	-	102		-
2.1	Правовые основы функционирования СОИБ предприятия	19	2	-	2	-	-	-	-	-	-	15	-	<p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Назначение и общая характеристика видов обеспечения</p>	

2.2	Организационные основы функционирования СОИБ предприятия	6	1	-	1	-	-	-	-	-	4	-	(подсистем) СОИБ предприятия" подготовка к выполнению заданий на практических занятиях <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия" <u>Изучение материалов литературных источников:</u> [1], 1-372 [2], 1-106 [3], 1-48 [4], 1-176
2.3	Кадровое обеспечение СОИБ предприятия	12	1	-	1	-	-	-	-	-	10	-	
2.4	Финансово-экономическое обеспечение функционирования СОИБ предприятия	12	1	-	1	-	-	-	-	-	10	-	
2.5	Инженерно-техническое обеспечение СОИБ	14	1	-	1	-	-	-	-	-	12	-	
2.6	Программно-аппаратное обеспечение функционирования СОИБ предприятия	14	1	-	1	-	-	-	-	-	12	-	
2.7	Подсистема аудита информационной системы предприятия	23	2	-	2	-	-	-	-	-	19	-	
2.8	Управление СОИБ предприятия	24	2	-	2	-	-	-	-	-	20	-	
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	
	<b>Всего за семестр</b>	<b>216.0</b>	<b>14</b>	<b>-</b>	<b>14</b>	<b>-</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>0.5</b>	<b>152</b>	<b>33.5</b>	
	<b>Итого за семестр</b>	<b>216.0</b>	<b>14</b>	<b>-</b>	<b>14</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>0.5</b>	<b>185.5</b>			

**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. Основы организации и функционирования СОИБ предприятия

1.1. Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта

Основы системного подхода к обеспечению информационной безопасности предприятия малого и среднего бизнеса. Этапы реализации системного подхода.

1.2. Система обеспечения информационной безопасности предприятия

Понятие, сущность, назначение и задачи СОИБ предприятия. Методологические основы организации СОИБ. Основные требования, предъявляемые к СОИБ и содержательная характеристика этапов ее разработки.

1.3. Перечень факторов, влияющих на организацию СОИБ предприятия

Форма собственности, организационно-правовая форма и характер основной деятельности хозяйствующего субъекта. Состав, объем и степень конфиденциальности защищаемой информации. Структура и территориальное расположение; режим функционирования, ресурсообеспечение и уровень автоматизации (цифровизации) основных информационных процессов. Политика информационной безопасности. Политика по управлению информационной безопасностью..

#### 2. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия

2.1. Правовые основы функционирования СОИБ предприятия

Структура правового обеспечения ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации. Лицензирование, сертификация и аттестация в области информационной безопасности.

2.2. Организационные основы функционирования СОИБ предприятия

Назначение, цели и задачи организационного обеспечения. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности.

2.3. Кадровое обеспечение СОИБ предприятия

Назначение, цели и задачи кадрового обеспечения. Основные мероприятия, проводимые при подборе, работе, увольнении сотрудников подразделений ИБ. Программы повышения осведомленности в области ИБ. Особенности профессиональной этики специалиста в области ИБ.

2.4. Финансово-экономическое обеспечение функционирования СОИБ предприятия

Экономические основы СОИБ. Модели для оценки экономической эффективности инвестиций в СОИБ предприятия.

2.5. Инженерно-техническое обеспечение СОИБ

Инженерно-техническая защита территорий, зданий и помещений предприятия. Организация защиты информации от утечки по техническим каналам. Методы и средства защиты информации от утечки по техническим каналам.

2.6. Программно-аппаратное обеспечение функционирования СОИБ предприятия

Назначение, цели и задачи подсистемы программно-аппаратного обеспечения СОИБ. Силы и программные средства защиты информации.

#### 2.7. Подсистема аудита информационной системы предприятия

Назначение, цели и задачи подсистемы аудита информационной безопасности. Направления деятельности подсистемы аудита. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита.

#### 2.8. Управление СОИБ предприятия

Понятие и цели управления. Сущность процессов управления СОИБ. Принципы управления и анализ системы управления СОИБ. Структура и содержание управления СОИБ организации.

### 3.3. Темы практических занятий

1. Организация инженерно-технической защиты территорий, зданий и помещений предприятия. Организация мероприятий защиты информации предприятия от утечки по техническим каналам;
2. Моделирование и оценка экономической эффективности инвестиций в СОИБ предприятия;
3. Кадровое обеспечение функционирования КСОИБ. Особенности работы с персоналом СОИБ. Особенности профессиональной этики специалиста в области ИБ;
4. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности. Моделирование информационной системы предприятия с позиций безопасности;
5. Выявление состава информационных активов предприятия. Определение перечня информации, составляющей коммерческую тайну. Разработка проекта перечня сведений, составляющих коммерческую тайну. Политика информационной безопасности предприятия. Основные положения и документы Политики ИБ. Разработка модели информационной системы ХС с позиций безопасности;
6. Внутренние организационно-распорядительные документы СОИБ, их состав и содержание;
7. Сущность и задачи СОИБ предприятия, принципы организации, этапы разработки и факторы, влияющие на организацию СОИБ;
8. Основы организации и функционирования СОИБ предприятия;
9. Организация защиты компьютерной (цифровой) информации в информационной системе предприятия. Программно-аппаратное обеспечение функционирования СОИБ предприятия;
10. Правовые основы функционирования СОИБ предприятия. Структура законодательства РФ в сфере ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации СОИБ;
11. Направления деятельности подсистемы аудита информационной безопасности. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита.

### 3.4. Темы лабораторных работ не предусмотрено

### 3.5 Консультации

*Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы организации и функционирования СОИБ предприятия"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия"

### **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>				
нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО	ОПК-7(Компетенция)		+	Тестирование/Тест 2 Тестирование/Тест 3 Тестирование/Тест 4 Тестирование/Тестирование
комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности	ОПК-7(Компетенция)		+	Тестирование/Тест 2 Тестирование/Тест 3 Тестирование/Тест 4 Тестирование/Тестирование
комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия	ПК-4(Компетенция)		+	Тестирование/Тест 3 Тестирование/Тест 4 Тестирование/Тестирование
психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	ПК-14(Компетенция)	+		Тестирование/Тестирование
состав и перечень информационных активов предприятия, относящихся к защищаемой информации	ПСК-3(Компетенция)		+	Тестирование/Тестирование
теорию анализа и синтеза сложных организационно-иерархических систем	ПСК-3(Компетенция)	+		Тестирование/Тестирование
<b>Уметь:</b>				
организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного	ОПК-7(Компетенция)		+	Тестирование/Тест 3

подхода в предметной области дисциплины				
правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики	ПК-4(Компетенция)		+	Тестирование/Тест 3 Тестирование/Тестирование
применять системный подход к управлению информационной безопасностью предприятия;	ПК-14(Компетенция)	+	+	Тестирование/Тест 2 Тестирование/Тест 3 Тестирование/Тестирование
на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности	ПК-14(Компетенция)	+		Тестирование/Тест 2 Тестирование/Тест 3 Тестирование/Тестирование
составить полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	ПСК-3(Компетенция)		+	Тестирование/Тест 2 Тестирование/Тестирование
выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса	ПСК-3(Компетенция)		+	Тестирование/Тест 2 Тестирование/Тестирование

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

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

**10 семестр**

Форма реализации: Письменная работа

1. Тест 2 (Тестирование)
2. Тест 3 (Тестирование)
3. Тест 4 (Тестирование)
4. Тестирование (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

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

*Экзамен (Семестр №10)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих (экзамена, проводимого по билетам)

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

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

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

1. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .

[http://elib.mpei.ru/action.php?kt\\_path\\_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468](http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468);

2. 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 .;

3. А. Абденов, Г. Дронова, В. Трушин- "Современные системы управления информационной безопасностью", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2017 - (48 с.)

<https://biblioclub.ru/index.php?page=book&id=574594>;

4. А. А. Анисимов- "Менеджмент в сфере информационной безопасности: курс лекций", Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний", Москва, 2009 - (176 с.)

<https://biblioclub.ru/index.php?page=book&id=232981>.

### **5.2 Лицензионное и свободно распространяемое программное обеспечение:**

1. СДО "Прометей";
2. Office;
3. Windows;

4. Майнд Видеоконференции;
5. 7-zip.

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

### **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

<b>Тип помещения</b>	<b>Номер аудитории, наименование</b>	<b>Оснащение</b>
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	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	3-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения	Ж-120, Машинный зал ИВЦ	сервер, кондиционер

промежуточной аттестации	3-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
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	3-512, Учебная аудитория	парта, 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**

Система обеспечения информационной безопасности хозяйствующего субъекта

(название дисциплины)

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

КМ-1 Тестирование (Тестирование)

КМ-2 Тест 2 (Тестирование)

КМ-3 Тест 3 (Тестирование)

КМ-4 Тест 4 (Тестирование)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Основы организации и функционирования СОИБ предприятия					
1.1	Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта		+	+	+	
1.2	Система обеспечения информационной безопасности предприятия		+			
1.3	Перечень факторов, влияющих на организацию СОИБ предприятия		+	+	+	
2	Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия					
2.1	Правовые основы функционирования СОИБ предприятия		+		+	
2.2	Организационные основы функционирования СОИБ предприятия		+	+	+	
2.3	Кадровое обеспечение СОИБ предприятия				+	
2.4	Финансово-экономическое обеспечение функционирования СОИБ предприятия		+	+		
2.5	Инженерно-техническое обеспечение СОИБ		+			
2.6	Программно-аппаратное обеспечение функционирования СОИБ предприятия		+			
2.7	Подсистема аудита информационной системы предприятия		+	+	+	+
2.8	Управление СОИБ предприятия		+	+	+	+
Вес КМ, %:			25	25	25	25