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

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.31**
Трудоемкость в зачетных единицах:	**9 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**9 семестр - 16 часов;**
Практические занятия	**9 семестр - 20 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**9 семестр - 2 часа;**
Самостоятельная работа	**9 семестр - 105,5 часов;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет** **Деловая игра**	
Промежуточная аттестация:	
Экзамен	**9 семестр - 0,5 часа;**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Писаренко И.В. Идентификатор: R2828e375-PisarenkoIV-105ccd67	И.В. Писаренко
(должность)	(подпись)	(расшифровка подписи)

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование у студентов системы знаний о принципах, методах и технологиях 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-4.1 способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ИД-1$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	знать: - Методы и технологии управления СМИБ и АСУ на основе технологий искусственного интеллекта (нечетких множеств, нейронных сетей, деревьев решений, блокчейн и больших данных).
ОПК-4.1 способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ИД-2$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе	уметь: - применять информационные технологии искусственного интеллекта для решения задач информационной безопасности при оценке рисков, классификации событий безопасности и обосновании управленческих решений.
ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-2$_{ОПК-6}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	знать: - современные концепции управления информационной безопасностью; - принципы оправления на основе цикла Дёменга-Шухарта. уметь: - моделировать системы управления информационной безопасностью.
ОПК-6 способен при	ИД-3$_{ОПК-6}$ Организует	знать:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	- требования нормативных документов по формированию политики информационной безопасности. уметь: - выполнять процессы разработки основных планирующих документов и политик безопасности.
ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-2$_{ОПК-10}$ Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации	знать: - требования нормативных документов ФСТЭК и ФСБ по организации и построении систем защиты информации ограниченного доступа. уметь: - выполнять комплекс мер по обеспечению информационной безопасности.
ОПК-12 способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИД-1$_{ОПК-12}$ Проводит анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвует в проведении технико-экономического обоснования соответствующих проектных решений	знать: - методы технико-экономического обоснования проектов по информационной безопасности с использованием моделей рисков; - технологии сбора исходных данных для проектирования СМИБ. уметь: - моделировать риски информационной безопасности на основе анализа и классификации активов, уязвимостей и угроз.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к 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	Вводный раздел	12	9	2	-	4	-	-	-	-	-	6	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Вводный раздел" подготовка к выполнению заданий на практических занятиях ***Подготовка доклада, выступления:*** 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: ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Вводный раздел" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:***
1.1	Введение в курс. Термины и определения	12		2	-	4	-	-	-	-	-	6	-	

														Повторение материала по разделу "Вводный раздел" ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Вводный раздел" ***<u>Изучение материалов литературных источников:</u>*** [2], 9-19
2	Система менеджмента	30		6	-	4	-	-	-	-	-	20	-	***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Система менеджмента" ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Система менеджмента" подготовка к выполнению заданий на практических занятиях ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу Система менеджмента и подготовка к контрольной работе ***<u>Подготовка доклада, выступления:</u>*** 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: ***<u>Подготовка домашнего задания:</u>*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Система менеджмента" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка
2.1	Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008	30		6	-	4	-	-	-	-	-	20	-	

														домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Система менеджмента" ***Изучение материалов литературных источников:*** [1], 6-18
3	Управление информационной безопасностью	32		4	-	4	-	-	-	-	-	24	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление информационной безопасностью" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление информационной безопасностью" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Управление информационной безопасностью и подготовка к контрольной работе ***Подготовка доклада, выступления:*** 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: ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе
3.1	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)	32		4	-	4	-	-	-	-	-	24	-	

														"Управление информационной безопасностью" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление информационной безопасностью" ***Изучение материалов литературных источников:*** [1], 35-53
4	Разработка системы менеджмента информационной безопасности	34		4	-	8	-	-	-	-	-	22	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Разработка системы менеджмента информационной безопасности"
4.1	Разработка СМИБ на примере АКБ (деловая игра)	34		4	-	8	-	-	-	-	-	22	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка реферата:*** В рамках реферативной части студенту необходим 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: ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Разработка системы менеджмента информационной безопасности". Студенты необходимо повторить теоретический материал, разобрать примеры решения

														аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Разработка системы менеджмента информационной безопасности" ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Разработка системы менеджмента информационной безопасности" подготовка к выполнению заданий на практических занятиях ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу Разработка системы менеджмента информационной безопасности и подготовка к контрольной работе ***<u>Подготовка доклада, выступления:</u>*** 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: ***<u>Подготовка домашнего задания:</u>*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Разработка системы менеджмента информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.

														Изучение материалов литературных источников: [1], 55-98
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**16**	**-**	**20**	**-**	**2**	**-**	**-**	**0.5**	**72**	**33.5**	
	Итого за семестр	**144.0**		**16**	**-**	**20**	**2**		**-**		**0.5**	**105.5**		

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. Вводный раздел

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 безопасности с использованием методов системного анализа.

2. Система менеджмента

2.1. 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.

3. Управление информационной безопасностью

3.1. 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 воздействие окружающей среды. Управление коммуникациями и работами. Управление доступом. Приобретение, разработка и эксплуатация информационных систем. Менеджмент инцидентов. Менеджмент непрерывности бизнеса.

4. Разработка системы менеджмента информационной безопасности

4.1. Разработка СМИБ на примере АКБ (деловая игра)

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

3.3. Темы практических занятий

1. 4. Практическая работа по созданию СМИБ на модели организации (деловая игра);
2. 3. Моделирование процессов управления рисками в различных концепциях;
3. 2. Моделирование процессов управления СМИБ в стандарте IDEF0;
4. 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 кейсам раздела "Вводный раздел"
2. Обсуждение материалов по кейсам раздела "Система менеджмента"
3. Обсуждение материалов по кейсам раздела "Управление информационной безопасностью"
4. Обсуждение материалов по кейсам раздела "Разработка системы менеджмента информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Вводный раздел"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Система менеджмента"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление информационной безопасностью"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Разработка системы менеджмента информационной 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	3	4	
Знать:						
Методы и технологии управления СМИБ и АСУ на основе технологий искусственного интеллекта (нечетких множеств, нейронных сетей, деревьев решений, блокчейн и больших данных)	ИД-1$_{ОПК-4.1}$	+				Отчет/Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000
принципы оправления на основе цикла Дёменга-Шухарта	ИД-2$_{ОПК-6}$		+			Отчет/Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0
современные концепции управления информационной безопасностью	ИД-2$_{ОПК-6}$			+		Отчет/Задание 3. Моделирование процессов управления рисками в различных концепциях
требования нормативных документов по формированию политики информационной безопасности	ИД-3$_{ОПК-6}$				+	Деловая игра/Контрольные задания 1-6. Деловая игра
требования нормативных документов ФСТЭК и ФСБ по организации и построении систем защиты информации ограниченного доступа	ИД-2$_{ОПК-10}$			+		Отчет/Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000
технологии сбора исходных данных для проектирования СМИБ	ИД-1$_{ОПК-12}$	+				Отчет/Задание 3. Моделирование процессов управления рисками в различных концепциях
методы технико-экономического обоснования проектов по информационной безопасности с использованием моделей рисков	ИД-1$_{ОПК-12}$				+	Отчет/Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0
Уметь:						
применять информационные технологии искусственного интеллекта для решения задач информационной безопасности при оценке рисков, классификации событий безопасности и обосновании управленческих решений	ИД-2$_{ОПК-4.1}$		+	+		Отчет/Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000

моделировать системы управления информационной безопасностью	ИД-2$_{ОПК-6}$		+	+		Отчет/Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0
выполнять процессы разработки основных планирующих документов и политик безопасности	ИД-3$_{ОПК-6}$		+	+		Отчет/Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0
выполнять комплекс мер по обеспечению информационной безопасности	ИД-2$_{ОПК-10}$			+	+	Отчет/Задание 3. Моделирование процессов управления рисками в различных концепциях
моделировать риски информационной безопасности на основе анализа и классификации активов, уязвимостей и угроз	ИД-1$_{ОПК-12}$				+	Деловая игра/Контрольные задания 1-6. 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

9 семестр

Форма реализации: Выполнение задания

1. Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет)
2. Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет)

Форма реализации: Защита задания

1. Контрольные задания 1-6. Деловая игра (Деловая игра)

Форма реализации: Письменная работа

1. Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000 (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №9)

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 9 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Система менеджмента информационной безопасности ГОСТ Р ИСО/МЭК 27001-2006 (проекты документов) : [учебно-методическое пособие] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Р. А. Сюбаев, М-во образования и науки Рос. Федерации, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИгеосистем, 2019 . – 98 с. - Авт. указаны на обороте тит. л. - ISBN 978-5-8481-0234-5 .;
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
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	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 лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	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
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура,

		кондиционер, телевизор
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

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

(название дисциплины)

9 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Задание 1. Термины и определения стандарта ГОСТ ИСО/МЭК 27000 (Отчет)
КМ-2 Задание 2. Моделирование процессов управления СМИБ в стандарте IDEF0 (Отчет)
КМ-3 Задание 3. Моделирование процессов управления рисками в различных концепциях (Отчет)
КМ-4 Контрольные задания 1-6. Деловая игра (Деловая игра)

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	Вводный раздел					
1.1	Введение в курс. Термины и определения		+		+	
2	Система менеджмента					
2.1	Система менеджмента информационной безопасности на основе ГОСТ Р ИСО/МЭК 27001-2008		+	+		
3	Управление информационной безопасностью					
3.1	Управление информационной безопасностью на основе практических правил по защите информации (ГОСТ Р ИСО/МЭК 27002)		+	+	+	
4	Разработка системы менеджмента информационной безопасности					
4.1	Разработка СМИБ на примере АКБ (деловая игра)			+	+	+
		Вес КМ, %:	25	25	25	25