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

Направление подготовки/специальность: 09.04.03 Прикладная информатика

Наименование образовательной программы: Информационные системы и технологии поддержки цифровой экономики

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОРПОРАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.10**
Трудоемкость в зачетных единицах:	**1 семестр - 8;**
Часов (всего) по учебному плану:	**288 часа**
Лекции	**1 семестр - 16 часов;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**1 семестр - 32 часа;**
Консультации	**1 семестр - 18 часов;**
Самостоятельная работа	**1 семестр - 217,2 часов;**
в том числе на КП/КР	**1 семестр - 0,7 часа;**
Иная контактная работа	**1 семестр - 4 часа;**
включая: **Контрольная работа** **Тестирование**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**1 семестр - 0,3 часа;** **1 семестр - 0,5 часа;** **всего - 0,8 часа**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Унижаев Н.В. Идентификатор: Rb43f42d6-UnizhayevNV-2454ef20	Н.В. Унижаев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крепков И.М. Идентификатор: R04da5bdb-KrepkovIM-33fe3095	И.М. Крепков
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: совершенствовании способностей и умений разработки стратегии информационной безопасностью корпорации

Задачи дисциплины

- изучение теоретических основ обеспечения информационной безопасности корпорации;
- формирование компетенций, связанных с защитой информации в условиях современного информационного противоборства;
- приобретение навыков практического использования результатов учебной деятельности.

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-8 Способен осуществлять эффективное управление разработкой программных средств и проектов, в том числе с использованием современных цифровых технологий	ИД-1$_{ОПК-8}$ Применяет знания по архитектуре информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов	знать: - федеральное законодательство и стандарты, регламентирующее информационную безопасность; - цели, функции и принципы информационной безопасности. уметь: - искать уязвимости информационной системы организации; - строить систему защиты информации на основе принципов информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Информационные системы и технологии поддержки цифровой экономики (далее – ОПОП), направления подготовки 09.04.03 Прикладная информатика, 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 8 зачетных единиц, 288 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	Современные проблемы информационной безопасности	49	1	3	10	-	-	-	-	-	-	36	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Современные проблемы информационной безопасности" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Современные проблемы информационной безопасности" ***Подготовка к лабораторной работе:*** 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 "Современные проблемы информационной безопасности" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Современные проблемы информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и
1.1	Тема 1. Введение в информационную безопасность	17		1	4	-	-	-	-	-	-	12	-	
1.2	Тема 2. Основные термины информационной безопасности	17		1	4	-	-	-	-	-	-	12	-	
1.3	Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.	15		1	2	-	-	-	-	-	-	12	-	

														разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<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: Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью. ***<u>Подготовка курсовой работы:</u>*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. ***<u>Изучение материалов литературных источников:</u>*** [1], 16-63 [5], 12-84 [7], 36-113 [10], 36-75 [13], 12-37

2	Управление системой информационной безопасности	61		5	8	-	-	-	-	-	-	48	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление системой информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью. ***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: Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры. ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Управление системой информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных
2.1	Тема 4. Место системы информационной безопасности организации	15		1	2	-	-	-	-	-	-	12	-	
2.2	Тема 5. Доктрина информационной безопасности Российской Федерации	16		2	2	-	-	-	-	-	-	12	-	
2.3	Тема 6. Модель информационной безопасности организации.	30		2	4	-	-	-	-	-	-	24	-	

														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 системой информационной безопасности" ***Подготовка к лабораторной работе:*** 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 системой информационной безопасности" материалу. ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление системой информационной безопасности" ***Изучение материалов литературных источников:*** [5], 113-167 [10], 12-73 [13], 17-73
3	Меры обеспечения информационной безопасности	64		5	8	-	-	-	-	-	-	51	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Меры обеспечения информационной безопасности" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов
3.1	Тема 7. Особенности информационной безопасности критической информационной инфраструктуры	22		2	2	-	-	-	-	-	-	18	-	
3.2	Тема 8. Криптографические	23		1	4	-	-	-	-	-	-	18	-	

	методы обеспечения информационной безопасности													обработки результатов по изученному в разделе "Меры обеспечения информационной безопасности" материалу.
3.3	Тема 9. Организация защиты от вредоносных программ (вирусов)	19		2	2	-	-	-	-	-	-	15	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Меры обеспечения информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***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: Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов. ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры. ***Самостоятельное изучение теоретического материала:*** Изучение

														дополнительного материала по разделу "Меры обеспечения информационной безопасности" ***<u>Изучение материалов литературных источников:</u>*** [3], 25-94 [6], 47-94 [7], 115-167 [8], 25-94 [9], 37-84 [12], 56-73 [13], 67-90 [15], 46-93
4	Политики информационной безопасности	57		3	6	-	-	-	-	-	-	48	-	***<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: Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности. ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Политики информационной безопасности" ***<u>Подготовка курсовой работы:</u>*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: Методы и варианты организации защиты от вредоносных программ (вирусов). Классификация вирусов. Система защиты от
4.1	Тема 10. Особенности защиты персональных данных	29		1	4	-	-	-	-	-	-	24	-	
4.2	Тема 11. Политика информационной безопасности	28		2	2	-	-	-	-	-	-	24	-	

														вирусов. ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Политики информационной безопасности" 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 "Политики информационной безопасности" ***Подготовка к лабораторной работе:*** 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 "Политики информационной безопасности" материалу. ***Изучение материалов литературных источников:*** [2], 12-76 [4], 37-94 [11], 64-94 [14], 14-76
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	21.0		-	-	-	16	-	4	-	0.3	0.7	-	
	Всего за семестр	**288.0**		**16**	**32**	**-**	**16**	**2**	**4**	**-**	**0.8**	**183.7**	**33.5**	
	Итого за семестр	**288.0**		**16**	**32**	**-**	**18**		**4**		**0.8**	**217.2**		

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. Современные проблемы информационной безопасности

1.1. Тема 1. Введение в информационную безопасность

Введение в управление информационной безопасностью. Место информационной безопасности в экономических процессах. Выявление причин и следствий нарушения информационной безопасности. Проблемы, связанные с сотрудниками и техническими ресурсами..

1.2. Тема 2. Основные термины информационной безопасности

Термины информационной безопасности, регламентированные федеральным законодательством и стандартами. Особенности использования терминологии..

1.3. Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.

Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью..

2. Управление системой информационной безопасности

2.1. Тема 4. Место системы информационной безопасности организации

Место системы информационной безопасности организации в системе безопасности Российской Федерации..

2.2. Тема 5. Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере..

2.3. Тема 6. Модель информационной безопасности организации.

Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью..

3. Меры обеспечения информационной безопасности

3.1. Тема 7. Особенности информационной безопасности критической информационной инфраструктуры

Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры..

3.2. Тема 8. Криптографические методы обеспечения информационной безопасности

Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов..

3.3. Тема 9. Организация защиты от вредоносных программ (вирусов)

Методы и варианты организации защиты от вредоносных программ (вирусов). Классификация вирусов. Система защиты от вирусов..

4. Политики информационной безопасности

4.1. Тема 10. Особенности защиты персональных данных

Особенности защиты персональных данных. Требования федерального законодательства. Классификация информационных систем персональных данных..

4.2. Тема 11. Политика информационной безопасности

Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Модель информационной безопасности организации;
2. Современные проблемы информационной безопасности. Введение в управление информационной безопасностью;
3. Документы, регламентирующие процесс управления информационной безопасностью.;
4. Система защиты компьютера с использованием паролей;
5. Вредоносные программы и защита от них. Организация защиты от вредоносных программ (вирусов);
6. Особенности защиты персональных данных. Требования федерального законодательства. Особенности защиты персональных данных;
7. Проведение анализа рисков;
8. Организационные меры защиты информации;
9. Каналы доступа к информации;
10. Политика информационной безопасности. Управление политикой безопасности;
11. Криптографические методы обеспечения информационной безопасности;
12. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Современные проблемы информационной безопасности"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Управление системой информационной безопасности"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Меры обеспечения информационной безопасности"

4. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Политики информационной безопасности"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Современные проблемы информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Управление системой информационной безопасности"
3. Обсуждение материалов по кейсам раздела "Меры обеспечения информационной безопасности"
4. Обсуждение материалов по кейсам раздела "Политики информационной безопасности"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Современные проблемы информационной безопасности"
2. Консультации проводятся по разделу "Управление системой информационной безопасности"
3. Консультации проводятся по разделу "Меры обеспечения информационной безопасности"
4. Консультации проводятся по разделу "Политики информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Современные проблемы информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление системой информационной безопасности"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Меры обеспечения информационной безопасности"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Политики информационной безопасности"

3.6 Тематика курсовых проектов/курсовых работ

1 Семестр

Курсовая работа (КР)
Темы:
- - Совершенствование системы информационной безопасности корпорации «Наименова-ние» - Создание системы информационной безопасности новой корпорации - Поиск уязвимостей информационной безопасности корпорации «Наименование» - Оценка эффективности информационной безопасности корпорации «Наименование» - Моделирование процессов, связанных с информационной безопасности корпорации «Наименование» - Поиск уязвимостей информационной безопасности в документообороте корпорации «Наименование» - Моделирование рисков информационной безопасности корпорации «Наименование» - Создание механизма формирования угроз информационной безопасности корпорации «Наименование» - Реинжиниринг информационной системы персональных данных корпорации «Наимено-вание» - Моделирование процессов, связанных с обеспечением защиты персональных данных корпорации «Наименование» - Моделирование рисков утечки персональных данных корпорации «Наименование» - Предложения по формированию плана совершенствования знаний персонала по инфор-

мационной безопасности корпорации - Рекомендации по действиям сотрудников корпорации при проверке информационной безопасности органами государственной власти - Расчет затрат на информационную безопасность. Предложения по сбалансированности затрат на информационной безопасности корпорации «Наименование» - Анализ способов противодействия угрозам информационной безопасности корпорации «Наименование» - Предложения по совершенствованию программно-технических способов обеспечения информационной безопасности корпорации «Наименование» - Предложения по совершенствованию нормативно-правовой и научной базы необходи-мой для обеспечения информационной безопасности корпорации «Наименование» - Предложения по совершенствованию структуры и задач корпорации «Наименование», обеспечивающих информационную безопасность. - Предложения по совершенствованию организационно-технических мер корпорации «Наименование»

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 15	Зачетная
Раздел курсового проекта	1	2	3	4	Защита курсового проекта
Объем раздела, %	25	25	25	25	-
Выполненный объем нарастающим итогом, %	25	50	75	100	-

Номер раздела	Раздел курсового проекта
1	Анализ информационной безопасности корпорации
2	Предложения по оптимизации информационной безопасности корпорации
3	Разработка плана совершенствования информационной безопасности
4	Оформление курсовой работы и подготовка к защите

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:						
цели, функции и принципы информационной безопасности	ИД-1$_{ОПК-8}$			+		Контрольная работа/КМ-3.
федеральное законодательство и стандарты, регламентирующее информационную безопасность	ИД-1$_{ОПК-8}$	+				Контрольная работа/КМ-1.
Уметь:						
строить систему защиты информации на основе принципов информационной безопасности	ИД-1$_{ОПК-8}$		+			Тестирование/КМ-2.
искать уязвимости информационной системы организации	ИД-1$_{ОПК-8}$				+	Тестирование/КМ-4.

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: Компьютерное задание

1. КМ-1. (Контрольная работа)
2. КМ-2. (Тестирование)
3. КМ-3. (Контрольная работа)
4. КМ-4. (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №1)

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ» Правила выставления итоговой оценки по курсу 1 семестр Экзамен. Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для магистров НИУ «МЭИ» на основании семестровой и экзаменационной составляющих. 1 семестр Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ». В приложение к диплому выносится оценка за 1 семестр и за курсовую работу.

Курсовая работа (КР) (Семестр №1)

Процедура проведения соответствует требованиям руководящих документов НИУ «МЭИ» 1 семестр Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ». В приложение к диплому выносится оценка за 1 семестр и за курсовую работу.

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. 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 .;
2. Минзов, А. С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса : учебно-методическое пособие / А. С. Минзов, Л. М. Кунбутаев, Нац. исслед. ун-т "МЭИ", Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : ВНИИгеосистем, 2011 . – 84 с. - ISBN 978-5-8481-0083-9 .;
3. 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 .;
4. 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 .;
5. Унижаев, Н. В. Управление экономической безопасностью организации : (создание и реинжиниринг системы безопасности, практика применения) / Н. В. Унижаев, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – М. : ВНИИгеосистем, 2018 . – 448 с. - ISBN 978-5-8481-0227-7 .
http://elib.mpei.ru/elib/view.php?id=10178;
6. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие для среднего профессионального образования / А. В. Васильков, И. А. Васильков . – М. : Форум, 2010 . – 368 с. – (Профессиональное образование) . - ISBN 978-5-91134-360-6 .;
7. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для вузов по специальности 075400 "Комплексная защита объектов информации" / А. А. Малюк . – М. : Горячая Линия-Телеком, 2004 . – 280 с. - ISBN 5-935171-97-X .;
8. Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза : монография / А. А. Смирнов . – М. : ЮНИТИ-ДАНА : Закон и право, 2012 . – 159 с. – (Научные издания для юристов) . - ISBN 978-5-238-02259-8 .;
9. А. А. Шунейко, И. А. Авдеенко- "Информационная безопасность человека", Издательство: "Владос", Москва, 2018 - (177 с.)
https://biblioclub.ru/index.php?page=book&id=573372;
10. В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской- "Введение в информационную безопасность и защиту информации", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2017 - (132 с.)
https://biblioclub.ru/index.php?page=book&id=575113;
11. В. Я. Ищейнов- "Информационная безопасность и защита информации: теория и практика", Издательство: "Директ-Медиа", Москва, Берлин, 2020 - (271 с.)
https://biblioclub.ru/index.php?page=book&id=571485;
12. Е. А. Басыня- "Системное администрирование и информационная безопасность", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2018 - (79 с.)
https://biblioclub.ru/index.php?page=book&id=575325;
13. О.А. Яшутина- "Обеспечение информационной безопасности с помощью антивируса Касперского. Лекция 2. Локальное использование Антивируса Касперского 6.0. Презентация", Издательство: "Национальный Открытый Университет «ИНТУИТ»", Москва, 2014 - (3 с.)
http://biblioclub.ru/index.php?page=book&id=239491;
14. В. Ю. Дронов- "Международные и отечественные стандарты по информационной безопасности", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2016 - (34 с.)
https://biblioclub.ru/index.php?page=book&id=575373;
15. Е. Н. Малыгин, В. А. Немтинов, С. Я. Егоров, В. Г. Мокрозуб, В. Г. Однолько- "Информационные и процедурные модели синтеза экологически безопасных технологических процессов химико-термической обработки изделий из металлов", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов,

2012 - (109 с.)
https://biblioclub.ru/index.php?page=book&id=277811.

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. Расписание учебных занятий;
6. Acrobat Reader;
7. MySQL;
8. Libre Office;
9. 7-zip;
10. Bison.

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. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данный Association for Computing Machinery Digital Library** - https://dl.acm.org/about/content
9. **База данных Computers & Applied Sciences Complete (CASC)** - http://search.ebscohost.com
10. **Журналы Institute of Physics (IOP), Великобритания** - https://iopscience.iop.org/
11. **Журналы по химии Thieme Chemistry Package компании Georg Thieme Verlag KG** - https://www.thieme-connect.com/products/all/home.html
12. **Портал открытых данных Российской Федерации** - https://data.gov.ru
13. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
14. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
15. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
16. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
17. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-503, Учебная лаборатория "Киберполигон SOFTLINE"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер

	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-503, Учебная лаборатория "Киберполигон SOFTLINE"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения лабораторных занятий	М-503, Учебная лаборатория "Киберполигон SOFTLINE"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-503, Учебная лаборатория "Киберполигон SOFTLINE"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
	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
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-521, Хозяйственное помещение кафедры МЭП	стеллаж, хозяйственный инвентарь, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Управление информационной безопасностью корпорации

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 КМ-1. (Контрольная работа)
КМ-2 КМ-2. (Тестирование)
КМ-3 КМ-3. (Контрольная работа)
КМ-4 КМ-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	Современные проблемы информационной безопасности					
1.1	Тема 1. Введение в информационную безопасность		+			
1.2	Тема 2. Основные термины информационной безопасности		+			
1.3	Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.		+			
2	Управление системой информационной безопасности					
2.1	Тема 4. Место системы информационной безопасности организации			+		
2.2	Тема 5. Доктрина информационной безопасности Российской Федерации			+		
2.3	Тема 6. Модель информационной безопасности организации.			+		
3	Меры обеспечения информационной безопасности					
3.1	Тема 7. Особенности информационной безопасности критической информационной инфраструктуры				+	
3.2	Тема 8. Криптографические методы обеспечения информационной безопасности				+	
3.3	Тема 9. Организация защиты от вредоносных программ (вирусов)				+	
4	Политики информационной безопасности					
4.1	Тема 10. Особенности защиты персональных данных					+

4.2	Тема 11. Политика информационной безопасности				+
	Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Управление информационной безопасностью корпорации

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 КМ-1. соблюдение графика выполнения КР
КМ-2 КМ-2. соблюдение графика выполнения КР
КМ-3 КМ-3. соблюдение графика выполнения КР
КМ-4 КМ-4.соблюдение графика выполнения КР и качество оформления КР

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Анализ информационной безопасности корпорации		+			
2	Предложения по оптимизации информационной безопасности корпорации			+		
3	Разработка плана совершенствования информационной безопасности				+	
4	Оформление курсовой работы и подготовка к защите					+
Вес КМ, %:			25	25	25	25