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
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Базовая**
№ дисциплины по учебному плану:	**Б1.Б.03**
Трудоемкость в зачетных единицах:	**2 семестр - 5;** **3 семестр - 3;** **всего - 8**
Часов (всего) по учебному плану:	**288 часа**
Лекции	**2 семестр - 16 часов;**
Практические занятия	**2 семестр - 48 часа;** **3 семестр - 16 часов;** **всего - 64 часа**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**3 семестр - 18 часов;**
Самостоятельная работа	**2 семестр - 115,7 часов;** **3 семестр - 69,2 часа;** **всего - 184,9 часа**
в том числе на КП/КР	**3 семестр - 15,7 часов;**
Иная контактная работа	**3 семестр - 4 часа;**
включая: **Тестирование** **Домашнее задание** **Отчет** **Деловая игра** **Контрольная работа**	
Промежуточная аттестация:	
Зачет с оценкой **Защита курсовой работы** **Экзамен**	**2 семестр - 0,3 часа;** **3 семестр - 0,3 часа;** **3 семестр - 0,5 часа;** **всего - 1,1 часа**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(должность)	(подпись)	(расшифровка подписи)

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
(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 теоретических знаний и умений по организации системы менеджмента информационной безопасности в организациях на основе оценки рисков информационной безопасности, реализации и внедрения соответствующих механизмов контроля, распределения ролей и ответственности, обучения персонала, оперативной работы по осуществлению защитных мероприятий и мониторинга функционирования механизмов контроля

Задачи дисциплины

- Получение студентами 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;
- Обучение методам и технологиям работы с первичными руководящими документами и стандартами в сфере информационной безопасности и управления.

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-5 способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества		знать: - основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах;.
ПК-9 способностью проводить аудит информационной безопасности информационных систем и объектов информатизации		знать: - основные способы проведения аудита информационной безопасности информационных систем. уметь: - разрабатывать (участвовать в разработке) модели угроз безопасности современного объекта, в том числе с АСУ (АСУТП).
ПК-12 способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения		знать: - основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ.
ПК-13 способностью организовать управление информационной безопасностью		уметь: - применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документамиФСБ России, ФСТЭК России		знать: - методы управления СМИБ на основе методик управления рисками. уметь: - использовать методы анализа процессов для определения и моделирования актуальных угроз организации.
ПК-15 способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности		уметь: - проводить анализ существующих взглядов на объект исследований и оценке необходимости его совершенствования; - выполнять комплекс работ с целью обеспечения готовности производства предприятия - изготовителя к изготовлению и поставке вновь разработанных, модернизированных и/или переданных изделий с одного предприятия на другое в заданных объёмах производства.
ОК-1 способностью к абстрактному мышлению, анализу, синтезу		уметь: - использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

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

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 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	Концепция управления информационной безопасностью	162	2	16	-	48	-	-	-	-	-	98	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Концепция управления информационной безопасностью"
1.1	Введение в дисциплину	50		4	-	16	-	-	-	-	-	30	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
1.2	Разработка плана и концепции СМИБ	52		6	-	16	-	-	-	-	-	30	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Концепция управления информационной безопасностью" 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:
1.3	Политика информационной безопасности и технология её разработки	60		6	-	16	-	-	-	-	-	38	-	

														Подготовка к практическим занятиям: Изучение материала по разделу "Концепция управления информационной безопасностью" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Концепция управления информационной безопасностью"
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**180.0**		**16**	-	**48**	-	-	-	-	**0.3**	**98**	**17.7**	
	Итого за семестр	**180.0**		**16**	-	**48**	-		-		**0.3**	**115.7**		
2	Управление рисками информационной безопасности	36	3	-	-	16	-	-	-	-	-	20	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление рисками информационной безопасности" ***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 "Управление рисками 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
2.1	Понятие риск информационной безопасности	36		-	-	16	-	-	-	-	-	20	-	

														слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление рисками информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление рисками информационной безопасности" ***Изучение материалов литературных источников:*** [4], 9-19
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	36.0		-	-	-	16	-	4	-	0.3	15.7	-	
	Всего за семестр	**108.0**		**-**	**-**	**16**	**16**	**2**	**4**	**-**	**0.8**	**35.7**	**33.5**	
	Итого за семестр	**108.0**		**-**	**-**	**16**	**18**		**4**		**0.8**	**69.2**		
	ИТОГО	**288.0**	**-**	**16**	**-**	**64**	**18**		**4**		**1.1**	**184.9**		

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. Концепция управления информационной безопасностью

1.1. Введение в дисциплину

Термины и определения. Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ). Концепция управления информационной безопасностью на основе цикла Дёминга-Шухарта. Критерии управления информационной безопасностью..

1.2. Разработка плана и концепции СМИБ

Логистика процессов управления информационной безопасностью на основе стандартов. Система документооборота и её формализованное представление..

1.3. Политика информационной безопасности и технология её разработки

Частные политики информационной безопасности. Процедуры, регламенты и инструкции по информационной безопасности..

2. Управление рисками информационной безопасности

2.1. Понятие риск информационной безопасности

Методы описания рисков. Методики моделирования угроз и оценки рисков. Разработка плана по обработке рисков. Разработка положения о применимости. Аттестация хозяйствующих субъектов по требованиям СМИБ: этапы и их последовательность, необходимая документация и механизм процедуры сертификации системы управления информационной безопасностью. Практическая работа по управлению информационной безопасностью на модели хозяйствующего субъекта..

3.3. Темы практических занятий

1. 3. Разработка плана и концепции СМИБ;
2. 2. Концепция управления информационной безопасностью на основе цикла Дёминга-Шухарта. Критерии управления информационной безопасностью;
3. 10. Практическая работа по управлению информационной безопасностью на модели хозяйствующего субъекта;
4. 9. Аттестация хозяйствующих субъектов по требованиям СМИБ: этапы и их последовательность, необходимая документация и механизм процедуры сертификации системы управления информационной безопасностью;
5. 8. Разработка плана по обработке рисков. Разработка положения о применимости.;
6. 7. Понятие риск информационной безопасности. Методы описания рисков. Методики моделирования угроз и оценки рисков;
7. 6. Политика информационной безопасности и технология её разработки. Частные политики информационной безопасности. Процедуры, регламенты и инструкции по информационной безопасности;
8. 5. Система документооборота и её формализованное представление;
9. 4. Логистика процессов управления информационной безопасностью на основе стандартов;
10. 1. Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ).

3.4. Темы лабораторных работ

не предусмотрено

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 "Концепция управления информационной безопасностью"
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 рисками информационной безопасности"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Концепция управления информационной безопасностью"
2. Обсуждение материалов по кейсам раздела "Управление рисками информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Концепция управления информационной безопасностью"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление рисками информационной безопасности"

3.6 Тематика курсовых проектов/курсовых работ

3 Семестр

Курсовая работа (КР)

Темы:

- Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите ГИС.
- Методы и технологии защиты ГИС, содержащих биометрические данные больших объемов (свыше 100 000 чел).
- Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ.

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 13	Зачетная
Раздел курсового проекта	1, 2	3	4, 5	Защита курсового проекта
Объем раздела, %	60	20	20	-
Выполненный объем нарастающим итогом, %	60	80	100	-

Номер раздела	Раздел курсового проекта
1	Введение
2	Глава 1
3	Глава 2

4	Глава 3
5	Заключение

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	
Знать:				
основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах;	ПК-5(Компетенция)	+		Тестирование/Тест №1
основные способы проведения аудита информационной безопасности информационных систем	ПК-9(Компетенция)	+		Домашнее задание/Выполнение и защита контрольного задания № 1 Отчет/Выполнение и защита контрольного задания № 2
основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ	ПК-12(Компетенция)	+		Домашнее задание/Выполнение и защита контрольного задания № 3
методы управления СМИБ на основе методик управления рисками	ПК-14(Компетенция)		+	Домашнее задание/Выполнение и защита контрольного задания № 4 Деловая игра/Выполнение и защита контрольного задания № 5 Контрольная работа/Защита курсовой работы Тестирование/Тест №2
Уметь:				
разрабатывать (участвовать в разработке) модели угроз	ПК-9(Компетенция)	+		Тестирование/Тест №1

безопасности современного объекта, в том числе с АСУ (АСУТП)				
применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ	ПК-13(Компетенция)	+		Домашнее задание/Выполнение и защита контрольного задания № 1
использовать методы анализа процессов для определения и моделирования актуальных угроз организации	ПК-14(Компетенция)	+		Отчет/Выполнение и защита контрольного задания № 2
выполнять комплекс работ с целью обеспечения готовности производства предприятия - изготовителя к изготовлению и поставке вновь разработанных, модернизированных и/или переданных изделий с одного предприятия на другое в заданных объёмах производства	ПК-15(Компетенция)	+		Домашнее задание/Выполнение и защита контрольного задания № 3
проводить анализ существующих взглядов на объект исследований и оценке необходимости его совершенствования	ПК-15(Компетенция)		+	Домашнее задание/Выполнение и защита контрольного задания № 4 Тестирование/Тест №2
использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации	ОК-1(Компетенция)		+	Деловая игра/Выполнение и защита контрольного задания № 5 Контрольная работа/Защита курсовой работы

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

4.1. Текущий контроль успеваемости

2 семестр

Форма реализации: Защита задания

1. Выполнение и защита контрольного задания № 1 (Домашнее задание)

Форма реализации: Компьютерное задание

1. Выполнение и защита контрольного задания № 2 (Отчет)
2. Выполнение и защита контрольного задания № 3 (Домашнее задание)
3. Тест №1 (Тестирование)

3 семестр

Форма реализации: Выполнение задания

1. Защита курсовой работы (Контрольная работа)

Форма реализации: Защита задания

1. Выполнение и защита контрольного задания № 5 (Деловая игра)

Форма реализации: Компьютерное задание

1. Выполнение и защита контрольного задания № 4 (Домашнее задание)
2. Тест №2 (Тестирование)

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

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №2)

Оценка определяется по совокупности результатов текущего контроля успеваемости в в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

Экзамен (Семестр №3)

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

Курсовая работа (КР) (Семестр №3)

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 3 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. 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 .;
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. 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 .;
4. 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. **База данных Web of Science** - http://webofscience.com/
3. **База данных Scopus** - http://www.scopus.com
4. **Национальная электронная библиотека** - https://rusneb.ru/
5. **Портал открытых данных Российской Федерации** - https://data.gov.ru
6. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
7. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
8. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
9. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
10. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
11. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.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-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	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	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	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Управление информационной безопасностью

(название дисциплины)

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тест №1 (Тестирование)
КМ-2 Выполнение и защита контрольного задания № 1 (Домашнее задание)
КМ-3 Выполнение и защита контрольного задания № 2 (Отчет)
КМ-4 Выполнение и защита контрольного задания № 3 (Домашнее задание)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Концепция управления информационной безопасностью					
1.1	Введение в дисциплину		+	+		
1.2	Разработка плана и концепции СМИБ			+	+	
1.3	Политика информационной безопасности и технология её разработки				+	+
		Вес КМ, %:	25	25	25	25

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тест №2 (Тестирование)
КМ-2 Выполнение и защита контрольного задания № 4 (Домашнее задание)
КМ-3 Выполнение и защита контрольного задания № 5 (Деловая игра)
КМ-4 Защита курсовой работы (Контрольная работа)

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	Управление рисками информационной безопасности					
1.1	Понятие риск информационной безопасности		+	+	+	+
		Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Управление информационной безопасностью

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Соблюдение графика выполнения КР; качество оформления КР
КМ-2 Соблюдение графика выполнения КР; оценка выполнения разделов КР
КМ-3 Соблюдение графика выполнения КР; оценка выполнения разделов КР

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	13
1	Введение		+		
2	Глава 1		+		
3	Глава 2			+	
4	Глава 3				+
5	Заключение				+
		Вес КМ, %:	60	20	20