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
ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.06**
Трудоемкость в зачетных единицах:	**2 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**2 семестр - 32 часа;**
Практические занятия	**2 семестр - 64 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**2 семестр - 2 часа;**
Самостоятельная работа	**2 семестр - 81,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Коллоквиум** **Отчет**	
Промежуточная аттестация:	
Экзамен	**2 семестр - 0,5 часа;**

Москва 2024

ПРОГРАММУ СОСТАВИЛ:

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

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование знаний и умений по применению технологий обеспечения информационной безопасности сложных социотехнических объектов и систем на основе применения отечественных и международных стандартов, руководящих документов и методик по обеспечению информационной безопасности хозяйствующих субъектов

Задачи дисциплины

- изучение требований нормативных документов по организации управления информационной безопасностью организации;
- изучение методологии моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0;
- овладение технологией проектирования системы менеджмента информационной безопасности и документарного оформления процесса разработки организационно-распорядительной документации по организации обеспечения информационной безопасности объекта критической информационной инфраструктуры.

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-2 Способен разрабатывать технический проект системы (подсистемы, компонента системы) обеспечения информационной безопасности	ИД-1$_{ОПК-2}$ Анализирует угрозы информационной безопасности объектов и разрабатывать методы противодействия им	знать: - требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации защиты информации; - методику разработки систем обеспечения информационной безопасности. уметь: - производить анализ угроз информационной безопасности объектов; - разрабатывать системы менеджмента информационной безопасности.
ОПК-3 Способен разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности	ИД-2$_{ОПК-3}$ Разрабатывает проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, в том числе и на объектах энергетики с критической информационной инфраструктурой,	знать: - технологию разработки документов при создании системы менеджмента информационной безопасности объекта. уметь: - – разрабатывать проекты организационно-распорядительных документов по информационной безопасности на объектах энергетики с критической информационной инфраструктурой.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
	использующих АСУ ТП	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

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

Базируется на уровне высшего образования (бакалавриат, специалитет).

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Система менеджмента информационной безопасности объектов	68	2	16	-	28	-	-	-	-	-	24	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Система менеджмента информационной безопасности объектов"
1.1	Тема 1. Система менеджмента информационной безопасности.	12		2	-	6	-	-	-	-	-	4	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Система менеджмента информационной безопасности объектов" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Система менеджмента информационной безопасности объектов" ***Изучение материалов литературных источников:*** [1], 1-50 [3], 47-76
1.2	Тема 2. Менеджмент информационной безопасности на уровне предприятия.	16		4	-	6	-	-	-	-	-	6	-	
1.3	Тема 3. Управление обеспечением информационной безопасности организации.	14		2	-	6	-	-	-	-	-	6	-	
1.4	Тема 4. Система управления информационной безопасностью.	6		2	-	2	-	-	-	-	-	2	-	
1.5	Тема 5. Процессный подход в рамках управления ИБ.	6		2	-	2	-	-	-	-	-	2	-	
1.6	Тема 6. Работа с процессами СУИБ организации.	14		4	-	6	-	-	-	-	-	4	-	
2	Разработка СМИБ	38		8	-	18	-	-	-	-	-	12	-	***Подготовка к текущему контролю:***

	объектов с использованием методологии IDEF													Повторение материала по разделу "Разработка СМИБ объектов с использованием методологии IDEF"
2.1	Тема 7. Стратегии построения и внедрения СУИБ.	12		2	-	6	-	-	-	-	-	4	-	***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 к практическим занятиям:*** Изучение материала по разделу "Разработка СМИБ объектов с использованием методологии IDEF" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Разработка СМИБ объектов с использованием методологии IDEF" ***Изучение материалов литературных источников:*** [1], 51-98
2.2	Тема 8. Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0.	12		2	-	6	-	-	-	-	-	4	-	
2.3	Тема 9. Моделирование системы менеджмента информационной безопасности организации с использованием технологии IDEF0.	14		4	-	6	-	-	-	-	-	4	-	
3	Проектирование СМИБ объектов с критической информационной инфраструктурой	38		8	-	18	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Проектирование СМИБ объектов с критической информационной инфраструктурой"
3.1	Тема 10. Проектирование системы менеджмента информационной безопасности для объектов КИИ различной категории значимости с	8		2	-	4	-	-	-	-	-	2	-	***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

	использованием технологии IDEF0.													предлагаются следующие варианты: ***Подготовка к практическим занятиям:***
3.2	Тема 11. Разработка организационно-распорядительной документации для объектов КИИ (значимых и незначимых) с использованием технологии IDEF0.	12		2	-	6	-	-	-	-	-	4	-	Изучение материала по разделу "Проектирование СМИБ объектов с критической информационной инфраструктурой" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Проектирование СМИБ объектов с критической информационной инфраструктурой" ***Изучение материалов литературных источников:*** [2], 10-100
3.3	Тема 12. Разработка проектной, рабочей и эксплуатационной документации на СМИБ.	18		4	-	8	-	-	-	-	-	6	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**32**	**-**	**64**	**-**	**2**	**-**	**-**	**0.5**	**48**	**33.5**	
	Итого за семестр	**180.0**		**32**	**-**	**64**	**2**		**-**		**0.5**	**81.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Система менеджмента информационной безопасности объектов

1.1. Тема 1. Система менеджмента информационной безопасности.

Модель управления информационной безопасностью. Анализ и управление рисками. Цикл управления рисками. Методы оценки рисков. Выбор мер безопасности. Порядок использования политик, стандартов и руководств..

1.2. Тема 2. Менеджмент информационной безопасности на уровне предприятия.

Предпосылки развития менеджмента в сфере информационной безопасности на уровне предприятий. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия. Формирование политики информационной безопасности на предприятии..

1.3. Тема 3. Управление обеспечением информационной безопасности организации.

Специфические черты организации информационной безопасности. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации..

1.4. Тема 4. Система управления информационной безопасностью.

Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Документальное обеспечение СУИБ. Политика СУИБ. Поддержка СУИБ со стороны руководства организации..

1.5. Тема 5. Процессный подход в рамках управления ИБ.

Процессы цикла PDCA в применении к процессам СУИБ. Планирование СУИБ. Реализация СУИБ. Проверка СУИБ. Совершенствование СУИБ..

1.6. Тема 6. Работа с процессами СУИБ организации.

Задание процесса СУИБ. Идентификация процессов СУИБ организации. Документирование и описание процесса СУИБ. Мониторинг и измерение параметров процесса СУИБ..

2. Разработка СМИБ объектов с использованием методологии IDEF

2.1. Тема 7. Стратегии построения и внедрения СУИБ.

Подходы построения СУИБ. Построение и внедрение СУИБ в целом..

2.2. Тема 8. Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0.

Постановка задачи. Методы исследования..

2.3. Тема 9. Моделирование системы менеджмента информационной безопасности организации с использованием технологии IDEF0.

Описание модели системы менеджмента информационной безопасности. Структура системы менеджмента информационной безопасности. Этапы внедрения системы менеджмента информационной безопасности в организации..

3. Проектирование СМИБ объектов с критической информационной инфраструктурой

3.1. Тема 10. Проектирование системы менеджмента информационной безопасности для объектов КИИ различной категории значимости с использованием технологии IDEF0.

Обследование объектов КИИ. Формирование требований, с учетом международных стандартов и лучших практик и разработка технических заданий.

3.2. Тема 11. Разработка организационно-распорядительной документации для объектов КИИ (значимых и незначимых) с использованием технологии IDEF0.

Моделирование порядка разработки организационно-распорядительной документации для объектов КИИ (значимых и незначимых)..

3.3. Тема 12. Разработка проектной, рабочей и эксплуатационной документации на СМИБ.

Моделирование комплексного решения разработки СМИБ объектов КИИ с использованием технологии IDEF0..

3.3. Темы практических занятий

1. 21.Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ;
2. 10.Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ;
3. 2.Цикл управления рисками. Методы оценки рисков;
4. 3.Выбор мер безопасности. Порядок использования политик, стандартов и руководств.;
5. 4. Предпосылки развития менеджмента в сфере информационной безопасности на уровне предприятий;
6. 5.Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия;
7. 6.Формирование политики информационной безопасности на предприятии;
8. 8.Деятельность по обеспечению ИБ организации как процесс;
9. 20. Применение технологии IDEF0 для разработки функциональной модели создания организационно-распорядительной документации для объектов КИИ (значимых и незначимых);
10. 12.Задание процесса СУИБ. Идентификация процессов СУИБ организации;
11. 13.Документирование и описание процесса СУИБ;
12. 14.Мониторинг и измерение параметров процесса СУИБ;
13. 15.Подходы построения СУИБ. Построение и внедрение СУИБ в целом;
14. 16.Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0;
15. 17.Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0;
16. 18.Моделирование этапов внедрения системы менеджмента информационной безопасности в организации с использованием технологии IDEF0;
17. 9.Управление ИБ информационно-телекоммуникационных технологий организации;
18. 7. Специфические черты организации информационной безопасности;
19. 1.Модель управления информационной безопасностью. Анализ и управление рисками;
20. 11. Планирование, реализация, проверка и совершенствование СУИБ;
21. 19. Применение технологии IDEF0 для проектирования системы менеджмента

информационной безопасности для объектов КИИ различной категории значимости.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Система менеджмента информационной безопасности объектов"
2. Обсуждение материалов по кейсам раздела "Разработка СМИБ объектов с использованием методологии IDEF"
3. Обсуждение материалов по кейсам раздела "Проектирование СМИБ объектов с критической информационной инфраструктурой"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Система менеджмента информационной безопасности объектов"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Разработка СМИБ объектов с использованием методологии IDEF"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Проектирование СМИБ объектов с критической информационной инфраструктурой"

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	
Знать:					
методику разработки систем обеспечения информационной безопасности	ИД-1$_{ОПК-2}$	+			/Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум
требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации защиты информации	ИД-1$_{ОПК-2}$	+			Коллоквиум/Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия
технологию разработки документов при создании системы менеджмента информационной безопасности объекта	ИД-2$_{ОПК-3}$	+			Коллоквиум/Документирование и описание процесса СУИБ. Коллоквиум
Уметь:					
разрабатывать системы менеджмента информационной безопасности	ИД-1$_{ОПК-2}$		+		Отчет/Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0
производить анализ угроз информационной безопасности объектов	ИД-1$_{ОПК-2}$	+			Коллоквиум/Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум
– разрабатывать проекты организационно-распорядительных документов по информационной безопасности на объектах энергетики с критической информационной инфраструктурой	ИД-2$_{ОПК-3}$			+	Отчет/Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ

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: Выполнение задания

1. Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0 (Отчет)
2. Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ (Отчет)

Форма реализации: Выступление (доклад)

1. Документирование и описание процесса СУИБ. Коллоквиум (Коллоквиум)
2. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия (Коллоквиум)
3. Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум (Коллоквиум)
4. Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум ()

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №2)

В диплом выставляется оценка за 2 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. 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. В. Г. Тимирясов, Т. В. Тишкина, Л. М. Рабинович- "Система менеджмента предприятия: оценка эффективности", Издательство: "Познание (Институт ЭУП)", Казань, 2009 - (184 с.) https://biblioclub.ru/index.php?page=book&id=257494.

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

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
8. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
9. **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, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Учебные аудитории для проведения промежуточной аттестации	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в

		Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Технологии обеспечения информационной безопасности объектов

(название дисциплины)

2 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум (Коллоквиум)

КМ-1 Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия (Коллоквиум)

КМ-2 Документирование и описание процесса СУИБ. Коллоквиум (Коллоквиум)

КМ-2 Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум

КМ-3 Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0 (Отчет)

КМ-4 Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ (Отчет)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	4	8	8	12	15
1	Система менеджмента информационной безопасности объектов							
1.1	Тема 1. Система менеджмента информационной безопасности.			+				
1.2	Тема 2. Менеджмент информационной безопасности на уровне предприятия.			+				
1.3	Тема 3. Управление обеспечением информационной безопасности организации.		+					
1.4	Тема 4. Система управления информационной безопасностью.		+					
1.5	Тема 5. Процессный подход в рамках управления ИБ.					+		
1.6	Тема 6. Работа с процессами СУИБ организации.				+	+		
2	Разработка СМИБ объектов с использованием методологии IDEF							
2.1	Тема 7. Стратегии построения и внедрения СУИБ.						+	
2.2	Тема 8. Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0.						+	

2.3	Тема 9. Моделирование системы менеджмента информационной безопасности организации с использованием технологии IDEF0.					+	
3	Проектирование СМИБ объектов с критической информационной инфраструктурой						
3.1	Тема 10. Проектирование системы менеджмента информационной безопасности для объектов КИИ различной категории значимости с использованием технологии IDEF0.						+
3.2	Тема 11. Разработка организационно-распорядительной документации для объектов КИИ (значимых и незначимых) с использованием технологии IDEF0.						+
3.3	Тема 12. Разработка проектной, рабочей и эксплуатационной документации на СМИБ.						+
	Вес КМ, %:	15	10	15	10	25	25