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:	**Базовая**
№ дисциплины по учебному плану:	**Б1.Б.02**
Трудоемкость в зачетных единицах:	**2 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**2 семестр - 16 часов;**
Практические занятия	**2 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**2 семестр - 2 часа;**
Самостоятельная работа	**2 семестр - 181,5 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 2020

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
(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 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 способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности		уметь: - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.
ПК-2 способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности		знать: - методику разработки систем обеспечения информационной без-опасности. уметь: - разрабатывать системы обеспечения информационной безопасности.
ПК-6 способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок		уметь: - производить анализ и систематизацию научно-технической информации по теме исследования.
ПК-9 способностью проводить аудит информационной		уметь: - организовывать на субъекте критической информационной инфраструктуры систему мониторинга

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
безопасности информационных систем и объектов информатизации		и аудита состояния защищенности значимых объектов, в том числе с АСУ (АСУ ТП).
ПК-16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности		уметь: - разрабатывать документы при создании системы информационной безопасности объекта.
ОК-2 способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения		знать: - требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации и технологиям защиты информации.

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 6 зачетных единиц, 216 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Система менеджмента информационной безопасности объектов	60.0	2	4.0	-	4.0	-	-	-	-	-	52	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Система менеджмента информационной безопасности объектов"
1.1	Тема 1. Система менеджмента информационной безопасности.	9.0		0.5	-	0.5	-	-	-	-	-	8	-	***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], 1-98 [4], 47-76
1.2	Тема 2. Менеджмент информационной безопасности на уровне предприятия.	9.0		0.5	-	0.5	-	-	-	-	-	8	-	
1.3	Тема 3. Управление обеспечением информационной безопасности организации.	9.0		0.5	-	0.5	-	-	-	-	-	8	-	
1.4	Тема 4. Система управления информационной безопасностью.	9.0		0.5	-	0.5	-	-	-	-	-	8	-	
1.5	Тема 5. Процессный подход в рамках управления ИБ.	12		1	-	1	-	-	-	-	-	10	-	
1.6	Тема 6. Работа с процессами СУИБ организации.	12		1	-	1	-	-	-	-	-	10	-	
2	Разработка СМИБ	60		6	-	6	-	-	-	-	-	48	-	***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.	20		2	-	2	-	-	-	-	-	16	-	***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:*** [3], 1-352
2.2	Тема 8. Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0.	20		2	-	2	-	-	-	-	-	16	-	
2.3	Тема 9. Моделирование системы менеджмента информационной безопасности организации с использованием технологии IDEF0.	20		2	-	2	-	-	-	-	-	16	-	
3	Проектирование СМИБ объектов с критической информационной инфраструктурой	60		6	-	6	-	-	-	-	-	48	-	***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	20		2	-	2	-	-	-	-	-	16	-	***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.	20		2	-	2	-	-	-	-	-	16	-	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], 37-77
3.3	Тема 12. Разработка проектной, рабочей и эксплуатационной документации на СМИБ.	20		2	-	2	-	-	-	-	-	16	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**216.0**		**16.0**	**-**	**16.0**	**-**	**2**	**-**	**-**	**0.5**	**148**	**33.5**	
	Итого за семестр	**216.0**		**16.0**	**-**	**16.0**	**2**		**-**		**0.5**	**181.5**		

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. 1. Анализ требований по организации и технологиям защиты информации на значимых объектах критической информационной инфраструктуры. Особенности формирования требований, предъявляемых к процессам защиты информации на значимых объектах крити-ческой информационной инфраструктуры АСУ и АСУ ТП;
2. 2. Требования современных руководящих и других нормативных документов по организации и технологиям защиты информации;
3. 3. Принципы и технология выбора средств и технологий защиты информации из официальных перечней;
4. 4. Классификация технологий обеспечения ИБ: системы обнаружения вторжений, системы защиты от НСД, системы антивирусного программного обеспечения, системы про-активной защиты информации в корпоративных системах, системы аудита информационной безопасности;
5. 5. Практическое применение технологий обеспечения безопасности современных высокотехнологичных объектов, в том числе с использованием АСУ и АСУТП;
6. 6. Анализ и построение модели угроз безопасности объекта на основе требований, предъявляемых к процессам защиты информации на значимых объектах с критической ин-формационной инфраструктурой АСУ и АСУ ТП;
7. 7. Изучение и анализ возможностей основных технологий обеспечения ИБ при их применении на объектах с критической информационной инфраструктурой АСУ и АСУ ТП;
8. 8. Разработка комплекса нормативно-распорядительной документации по созданию и обеспечению функционирования системы информационной безопасности значимого объекта критической информационной инфраструктуры, в том числе объектов АСУ и АСУ ТП.

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	ПК-2(Компетенция)	+			Коллоквиум/Документирование и описание процесса СУИБ. Коллоквиум Коллоквиум/Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум
требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации и технологиям защиты информации	ОК-2(Компетенция)	+			Коллоквиум/Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия
Уметь:					
осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	ОПК-2(Компетенция)	+			Коллоквиум/Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия
разрабатывать системы обеспечения информационной безопасности	ПК-2(Компетенция)		+		Отчет/Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0
производить анализ и систематизацию научно-технической информации по теме исследования	ПК-6(Компетенция)	+			Коллоквиум/Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум
организовывать на субъекте критической информационной	ПК-9(Компетенция)			+	Отчет/Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с

инфраструктуры систему мониторинга и аудита состояния защищенности значимых объектов, в том числе с АСУ (АСУ ТП)					использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ
разрабатывать документы при создании системы информационной безопасности объекта	ПК-16(Компетенция)		+	+	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 (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. Клейменов, С. А. Администрирование в информационных системах : учебное пособие для вузов по специальности "Информационные системы и технологии" / С. А. Клейменов, В. П. Мельников, А. М. Петраков ; Ред. В. П. Мельников . – М. : Академия, 2008 . – 272 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4708-9 .;
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника"

/ П. Б. Хорев . – М. : Форум, 2013 . – 352 с. – (Высшее образование) . - ISBN 978-5-91134-353-8 .;
4. 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. 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. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
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. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
12. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
13. **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-509, Учебная аудитория	парта со скамьей, 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-509, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-509, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для	НТБ-303,	стол компьютерный, стул, стол

самостоятельной работы	Компьютерный читальный зал	письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-509, 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

Технологии обеспечения информационной безопасности объектов

(название дисциплины)

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

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

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

КМ-3 Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум (Коллоквиум)

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-2	КМ-2	КМ-3	КМ-3	КМ-4
		Неделя КМ:	4	8	8	12	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, %:	25	10	15	15	10	25