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

Направление подготовки/специальность: 38.03.02 Менеджмент

Наименование образовательной программы: Менеджмент предприятий и организаций

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 4 «Факультативы»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.01**
Трудоемкость в зачетных единицах:	**3 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**3 семестр - 16 часов;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**3 семестр - 55,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет** **Доклад**	
Промежуточная аттестация:	
Зачет	**3 семестр - 0,3 часа;**

Москва 2026

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: Сотниченко Е. Идентификатор: R4dba8757-SotnichenkoY-c3f9793	Е. Сотниченко
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Кетоева Н.Л. Идентификатор: R56dba1ba-KetoyevaNL-5403d8c5	Н.Л. Кетоева

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование системы знаний и навыков по теоретическим основам информационной безопасности, анализу информационных ресурсов, анализу угроз защищаемой информации, определению методов и средств защиты информации..

Задачи дисциплины

- на основе изучения понятийного аппарата в области информационной безопасности и защиты информации раскрыть теоретическую содержательную часть предметной области дисциплины;
- на основе системного подхода к изучению теоретического материала дисциплины сформировать состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также ее собственникам и обладателям;
- сформировать готовность и способность студентов к реализации профессиональной деятельности в условиях воздействия угроз информационной безопасности;
- сформировать у студентов системный подход к обеспечению информационной безопасности предприятия (организации);
- выработать у студентов практические навыки правильного оформления 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**
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1$_{УК-1}$ Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи	знать: - источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию; - состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации; - критерии мотивации к выполнению профессиональной деятельности; - нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области. уметь: - способностью формирования различных моделей контроля конфиденциальности и целостности; - применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода; - выполнять профессиональную деятельность в области обеспечения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Менеджмент предприятий и организаций (далее – ОПОП), направления подготовки 38.03.02 Менеджмент, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 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	Основы теории обеспечения информационной безопасности	25	3	6	-	-	-	-	-	-	-	19	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы теории обеспечения информационной безопасности"
1.1	Вводная тема.	4		1	-	-	-	-	-	-	-	3	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Основы теории обеспечения информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.
1.2	Тема 1. Информация, как наиболее ценный ресурс современного общества.	4		1	-	-	-	-	-	-	-	3	-	
1.3	Тема 2. Понятие угрозы безопасности информации.	4		1	-	-	-	-	-	-	-	3	-	
1.4	Тема 3. Понятие уязвимости в информационной безопасности.	4		1	-	-	-	-	-	-	-	3	-	
1.5	Тема 4. Понятие нарушителя и классификационные признаки нарушителей ИБ.	4		1	-	-	-	-	-	-	-	3	-	***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: ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу
1.6	Тема 5. Модель угроз: понятие, цель разработки, выполняемые задачи.	5		1	-	-	-	-	-	-	-	4	-	

														"Основы теории обеспечения информационной безопасности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основы теории обеспечения информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Изучение материалов литературных источников:*** [4], 10-23
2	Методологические основы защиты информации	46.7		10	-	-	-	-	-	-	-	36.7	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Методологические основы защиты информации" подготовка к выполнению заданий на практических занятиях ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Методологические основы защиты информации" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Методологические основы защиты информации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
2.1	Тема 6. Понятие, общие положения, модели безопасности	6		1	-	-	-	-	-	-	-	5	-	
2.2	Тема 7. Модель ХРУ (HRU).	7		2	-	-	-	-	-	-	-	5	-	
2.3	Тема 8. Мандатная Модель целостности Биба (БМ).	7		2	-	-	-	-	-	-	-	5	-	
2.4	Тема 9. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации.	6		1	-	-	-	-	-	-	-	5	-	
2.5	Тема 10. Анализ причин и методов НСД к информации.	5		1	-	-	-	-	-	-	-	4	-	
2.6	Тема 11. Характеристика методов и средств защиты информации.	4		2	-	-	-	-	-	-	-	2	-	
2.7	Тема 12.	11.7		1	-	-	-	-	-	-	-	10.7	-	

	Методологические подходы к защите информации и принципы её организации.													***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Методологические основы защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Изучение материалов литературных источников:*** [4], 24-43
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**72.0**		**16**	**-**	**-**	**-**	**-**	**-**	**-**	**0.3**	**55.7**	**-**	
	Итого за семестр	**72.0**		**16**	**-**	**-**	**-**		**-**		**0.3**	**55.7**		

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. Основы теории обеспечения информационной безопасности

1.1. Вводная тема.

Введение в дисциплину «Теория информационной безопасности». План изучения дисциплины. Основные понятия и определения. Цель и содержание учебной дисциплины, общая структура и характеристика ее составляющих; взаимосвязь учебной дисциплины с другими дисциплинами специальности, её место и роль в формировании специалиста в области информационной безопасности; общие рекомендации по изучению дисциплины, актуальные проблемы информационной безопасности в РФ, рекомендуемая литература..

1.2. Тема 1. Информация, как наиболее ценный ресурс современного общества.

Понятие ценности информации, свойства информации, определяющие ее ценность. Методы определения ценности информации (личной, корпоративной и государственной). Понятие тайны информации и современное состояние тайны информации в РФ. Виды доступа к информации. Организация доступа к общедоступной информации в РФ. Информация ограниченного доступа. Несанкционированный доступ к информации. Проблемы информационной войны и информационной безопасности в сфере государственного и муниципального управления. Классификация защищаемой информации по собственникам и обладателям..

1.3. Тема 2. Понятие угрозы безопасности информации.

Основы классификации угроз. Классификация угроз по характеру воздействия. Классификация угроз по расположению источника угроз. Классификация угроз по составляющим ИБ. Классификация угроз по компонентам ИС. Моделирование и разработка модели угроз..

1.4. Тема 3. Понятие уязвимости в информационной безопасности.

Природа возникновения уязвимостей. Понятие уязвимости и природа (причины) возникновения уязвимостей в ИС. Классификация уязвимостей по типу. Классификация уязвимостей по компоненту, содержащему уязвимость. Классификация уязвимостей по этапам жизненного цикла. Классификация уязвимостей по преднамеренности внесения. Классификация уязвимостей по месту уязвимости в ИС. Основы практической работы с базами уязвимостей(информацией об уязвимостях)..

1.5. Тема 4. Понятие нарушителя и классификационные признаки нарушителей ИБ.

Общая характеристика внутренних и внешних нарушителей. Классификация нарушителей по используемым средствам и методам. Классификация уязвимостей по уровню подготовки (квалификации). Характеристика основных групп нарушителей. Общая характеристика модели нарушителя: понятие, назначение и цели её разработки. Структура модели нарушителя: основные разделы и содержание..

1.6. Тема 5. Модель угроз: понятие, цель разработки, выполняемые задачи.

Требования к разработке Модели угроз. Содержание Модели угроз безопасности. Последовательность работ по моделированию угроз. Методика определения актуальных угроз безопасности информации в информационной системе. Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба..

2. Методологические основы защиты информации

2.1. Тема 6. Понятие, общие положения, модели безопасности

Виды Политик безопасности. Модели Политик безопасности. Формальное и неформальное выражение Политики безопасности. Классификация и содержание основных моделей безопасности. Понятие и сущность Политики безопасности. Дуализм политики. Общая характеристика дискреционной Политики безопасности. Общая характеристика мандатной Политики безопасности. Общая характеристика Политик безопасности информационных потоков, ролевого доступа и изолированной программной среды. Классификация моделей безопасности. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели..

2.2. Тема 7. Модель ХРУ (HRU).

Постановка задачи моделирования. Модель ХРУ (HRU), исходные данные модели. Модель ХРУ (HRU), управление доступом. Модель БЛ (BL). Подходы к моделированию. Модель БЛ (BL), исходные данные. Модель БЛ (BL), характеристика безопасного состояния системы. Основная теорема безопасности Белла – Лападулы (БЛМ), постановка задачи, формулировка и доказательство..

2.3. Тема 8. Мандатная Модель целостности Биба (БМ).

Постановка задачи моделирования. Модели понижения уровня субъекта и объекта. Случаи необходимости моделей. Объединение моделей. Цели и порядок объединения. Постановка и общее описание модели Кларка – Вильсона (КВМ). Интерпретация правил КВМ. Поддержка принципов контроля целостности правилами КВМ. Сравнительный анализ БЛМ – БМ. Общее и основные различия в различных моделях. Возможность создания различных моделей контроля конфиденциальности и целостности..

2.4. Тема 9. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации.

Оценка взглядов субъектов информационных отношений на обеспечение доступности и целостности информации. Оценка взглядов субъектов информационных отношений на обеспечение безопасности информации. Сравнительный анализ методов организации работ по защите информационных активов. Характеристика государственной системы защиты информации Российской Федерации. Анализ ее структуры, задач и полномочий..

2.5. Тема 10. Анализ причин и методов НСД к информации.

Методы защиты информации от НСД. Анализ комплекса мероприятий защиты информации от НСД . Содержание основных мероприятий защиты информации от НСД. Общее содержание и анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»..

2.6. Тема 11. Характеристика методов и средств защиты информации.

Методы защиты информации и их характеристика. Скрытие. Ранжирование. Дезинформация. Страхование. Морально-нравственные методы. Учет. Кодирование. Шифрование. Средства защиты информации и их характеристика. Средства защиты информации..

2.7. Тема 12. Методологические подходы к защите информации и принципы её организации.

Направления обеспечения информационной безопасности. Сущность и содержание основных направлений обеспечения информационной безопасности. Организация и обеспечение правовой, организационной и технической защиты информации. Основные и

вспомогательные виды обеспечения защиты информации. Сущность, значение и состав всех видов обеспечения защиты информации..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основы теории обеспечения информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Методологические основы защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы теории обеспечения информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методологические основы защиты информации"

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	
Знать:				
нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области	ИД-1$_{УК-1}$		+	Доклад/Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»
критерии мотивации к выполнению профессиональной деятельности	ИД-1$_{УК-1}$	+		Отчет/Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей
состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации	ИД-1$_{УК-1}$	+		Отчет/Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей
источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию	ИД-1$_{УК-1}$	+		Отчет/Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х»
Уметь:				
выполнять профессиональную деятельность в области обеспечения информационной безопасности	ИД-1$_{УК-1}$		+	Доклад/Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»
применять теоретические знания в области информационной безопасности на основе	ИД-1$_{УК-1}$	+	+	Отчет/Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация,

системного анализа и системного подхода				ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х»
способностью формирования различных моделей контроля конфиденциальности и целостности	ИД-1$_{УК-1}$	+	+	Отчет/Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Выполнение задания

1. Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет)
2. Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х» (Отчет)

Форма реализации: Выступление (доклад)

1. Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)

Форма реализации: Защита задания

1. Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №3)

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. Введение в информационную безопасность : учебное пособие для вузов по направлениям и специальностям, не входящим в направление подготовки "Информационная безопасность" / А. А. Малюк, и др. ; Ред. В. С. Горбатов. – М. : Горячая Линия-Телеком, 2011. – 288 с. – ISBN 978-5-9912-0160-5.;
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов по специальностям 090300 "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению 090900 "Информационная безопасность" / П. Н. Девянин. – М. : Горячая Линия-Телеком, 2011. – 320 с. – ISBN 978-5-9912-0147-6.;

3. Малюк, А. А. Теория защиты информации / А. А. Малюк. – М. : Горячая Линия-Телеком, 2012. – 184 с. – ISBN 978-5-9912-0246-6.;
4. А. Абденов, Г. Дронова, В. Трушин- "Современные системы управления информационной безопасностью", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2017 - (48 с.)
https://biblioclub.ru/index.php?page=book&id=574594.

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. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **Национальная электронная библиотека** - https://rusneb.ru/
8. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
9. **Журнал Science** - https://www.sciencemag.org/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
12. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-526, Компьютерный класс ИВЦ	стол, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	К-526, Компьютерный класс ИВЦ	стол, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	К-526, Компьютерный класс ИВЦ	стол, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная, компьютер персональный, кондиционер
Помещения для самостоятельной работы	НТБ-302, Читальный зал отдела обслуживания учебной литературой	стул, стол письменный, компьютерная сеть с выходом в Интернет, компьютер персональный
	НТБ-303, Лекционная	стол компьютерный, стул, стол

	аудитория	письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	К-203а, Кабинет сотрудников каф. "БИТ"	стол, стол компьютерный, стул, шкаф для документов, шкаф для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, кондиционер
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

Теория информационной безопасности

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет)

КМ-2 Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х» (Отчет)

КМ-3 Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности (Отчет)

КМ-4 Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Основы теории обеспечения информационной безопасности					
1.1	Вводная тема.		+			
1.2	Тема 1. Информация, как наиболее ценный ресурс современного общества.		+			
1.3	Тема 2. Понятие угрозы безопасности информации.		+	+		
1.4	Тема 3. Понятие уязвимости в информационной безопасности.		+	+		
1.5	Тема 4. Понятие нарушителя и классификационные признаки нарушителей ИБ.		+	+		
1.6	Тема 5. Модель угроз: понятие, цель разработки, выполняемые задачи.			+	+	
2	Методологические основы защиты информации					
2.1	Тема 6. Понятие, общие положения, модели безопасности			+	+	
2.2	Тема 7. Модель ХРУ (HRU).				+	
2.3	Тема 8. Мандатная Модель целостности Биба (БМ).				+	

2.4	Тема 9. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации.				+
2.5	Тема 10. Анализ причин и методов НСД к информации.				+
2.6	Тема 11. Характеристика методов и средств защиты информации.				+
2.7	Тема 12. Методологические подходы к защите информации и принципы её организации.				+
	Вес КМ, %:	25	25	25	25