Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.18**
Трудоемкость в зачетных единицах:	**4 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**4 семестр - 20 часов;**
Практические занятия	**4 семестр - 24 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**4 семестр - 2 часа;**
Самостоятельная работа	**4 семестр - 133,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет** **Доклад** **Домашнее задание** **Решение задач**	
Промежуточная аттестация:	
Экзамен	**4 семестр - 0,5 часа;**

Москва 2023

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: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(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 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**
ОПК-1 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-1$_{ОПК-1}$ Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	знать: - критерии мотивации к выполнению профессиональной деятельности. уметь: - понимать социальную значимость своей будущей профессии; - выполнять профессиональную деятельность в области обеспечения информационной безопасности.
ОПК-1 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	знать: - состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации.
ОПК-4.1 способен проводить организационные	ИД-1$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры,	знать: - нормативные методические документы федеральной службы безопасности Российской Федерации,

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
мероприятия по обеспечению безопасности информации в автоматизированных системах	реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	Федеральной службы по техническому и экспортному контролю в данной области. уметь: - формировать различные модели контроля конфиденциальности и целостности.
ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-2$_{ОПК-6}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	знать: - источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию. уметь: - применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, 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 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	Основы теории обеспечения информационной безопасности	58	4	6	-	12	-	-	-	-	-	40	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы теории обеспечения информационной безопасности"
1.1	Вводная тема	7		1	-	2	-	-	-	-	-	4	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка вопросов семинарских занятий ***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. ***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:
1.2	Тема 1. Информация, как наиболее ценный ресурс современного общества	7		1	-	2	-	-	-	-	-	4	-	
1.3	Тема 2. Понятие угрозы безопасности информации	7		1	-	2	-	-	-	-	-	4	-	
1.4	Тема 3. Понятие уязвимости в информационной безопасности	11		1	-	2	-	-	-	-	-	8	-	
1.5	Тема 4. Понятие нарушителя и классификационные признаки нарушителей ИБ	7		1	-	2	-	-	-	-	-	4	-	
1.6	Тема 5. Модель угроз: понятие, цель разработки, выполняемые задачи	19		1	-	2	-	-	-	-	-	16	-	

														1.Порядок оценки ценности информации на основе анализа рисков информационной безопасности. 2.История возникновения тайны информации. Виды тайны информации, определяемые современным законодательством РФ. 3.Цель, назначение, порядок использования информационного ресурса «Банк данных угроз информационной безопасности», расположенного на официальном интернет-сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК России). 4. Цель, назначение, порядок использования информационного ресурса «Банк данных угроз информационной безопасности (Раздел «Уязвимости»), расположенного на официальном интернет-сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК России) 5. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли. Методический документ: общая характеристика, назначение, локализация (в чьих интересах разработан), содержание общее и детально модели нарушителя 6. Общая информация и особенности, отражаемые в Модели угроз на основе анализа следующих примеров: ●Модель угроз типовой медицинской информационной системы (МИС) типового лечебно-профилактического учреждения (ЛПУ), разработана департаментом информатизации Министерства здравоохранения и социального развития ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основы теории обеспечения информационной безопасности" подготовка к выполнению заданий на практических занятиях

														Самостоятельное изучение теоретического материала: Изучение дополнительного материала по разделу "Основы теории обеспечения информационной безопасности" ***Изучение материалов литературных источников:*** [2], 1-184 [4], 1-50 [6], 192-200
2	Методологические основы защиты информации	86		14	-	12	-	-	-	-	-	60	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Методологические основы защиты информации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка вопросов семинаров ***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. ***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.Неформальные модели безопасности.
2.1	Тема 6. Понятие, общие положения, модели безопасности. Виды Политик безопасности	11		2	-	1	-	-	-	-	-	8	-	
2.2	Тема 7. Модель ХРУ (HRU	11		2	-	1	-	-	-	-	-	8	-	
2.3	Тема 8. Мандатная Модель целостности Биба (БМ)	12		2	-	2	-	-	-	-	-	8	-	
2.4	Тема 9. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации	14		2	-	2	-	-	-	-	-	10	-	
2.5	Тема 10. Анализ причин и методов НСД к информации	12		2	-	2	-	-	-	-	-	8	-	
2.6	Тема 11. Характеристика методов и средств защиты информации	12		2	-	2	-	-	-	-	-	8	-	
2.7	Тема 12. Методологические	14		2	-	2	-	-	-	-	-	10	-	

	подходы к защите информации и принципы её организации													Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей 2. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство 3. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности 4. Краткая характеристика государственной системы защиты информации Российской Федерации. Анализ ее структуры, задач и полномочий 5. Общее содержание и анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Методологические основы защиты информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Методологические основы защиты информации" ***Изучение материалов литературных источников:*** [1], 30-150 [3], 1-280 [5], 152-192
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**20**	**-**	**24**	**-**	**2**	**-**	**-**	**0.5**	**100**	**33.5**	
	Итого за семестр	**180.0**		**20**	**-**	**24**	**2**		**-**		**0.5**	**133.5**		

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. 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 модел.

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

1. 1.Место и роль дисциплины «Теория информационной безопасности» в формировании специалиста в области информационной безопасности;
2. 18.Проектирование систем защиты информации;
3. 17.Структура системы защиты информации, назначение составных частей системы;
4. 16.Характеристика средств защиты информации;
5. 15.Характеристика методов защиты информации;
6. 14.Теоретические основы защиты информации от несанкционированного доступа (НСД);
7. 13.Теоретические основы защиты информации;
8. 12.Формализованные модели контроля целостности информации;
9. 11.Формализованные модели контроля конфиденциальности информации;
10. 10. Моделирование безопасности информации на основе Политики безопасности;
11. 9.Системный подход к моделированию угроз безопасности информации;
12. 8.Моделирование действий нарушителя информационной безопасности;
13. 7.Разработка «Модели угроз безопасности информации организации «Х»;
14. 6.Разработка модели угроз для информационной системы предприятия (организации);
15. 5.Анализ общедоступной базы уязвимостей, относящейся к ИБ, поддерживаемых различными профильными организациями и вендорами;
16. 4.Уязвимости информационных (автоматизированных) систем;
17. 3.Угрозы безопасности информации;
18. 2.Информация как объект защиты;
19. 19.Параметры защищаемой информации. Анализ и оценка факторов, влияющих на требуемый уровень защиты;
20. 20.Сущность и содержание основных направлений обеспечения информационной безопасности. Организация и обеспечение правовой, организационной и инженерно-технической защиты информации.

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:				
критерии мотивации к выполнению профессиональной деятельности	ИД-1$_{ОПК-1}$	+		Отчет/Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности.
состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации	ИД-2$_{ОПК-1}$	+		Домашнее задание/Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей
нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области	ИД-1$_{ОПК-4.1}$		+	Доклад/Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»
источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию	ИД-2$_{ОПК-6}$	+		Домашнее задание/Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х».
Уметь:				
выполнять профессиональную деятельность в области обеспечения информационной безопасности	ИД-1$_{ОПК-1}$		+	Доклад/Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»
понимать социальную значимость своей будущей профессии	ИД-1$_{ОПК-1}$	+		Отчет/Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности.
формировать различные модели контроля конфиденциальности и целостности	ИД-1$_{ОПК-4.1}$	+	+	Решение задач/Контрольное задание № 1. Разработка матрицы доступа к защищаемой информации Отчет/Практическое задание № 3. Основная теорема

				безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. Отчет/Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности
применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода	ИД-2$_{ОПК-6}$	+	+	Отчет/Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей.

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

4.1. Текущий контроль успеваемости

4 семестр

Форма реализации: Выполнение задания

1. Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей (Домашнее задание)
2. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х». (Домашнее задание)
3. Контрольное задание № 1. Разработка матрицы доступа к защищаемой информации (Решение задач)
4. Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности. (Отчет)
5. Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. (Отчет)
6. Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. (Отчет)
7. Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности (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)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №4)

В диплом выставляется оценка за 4 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
2. Малюк, А. А. Теория защиты информации / А. А. Малюк . – М. : Горячая Линия-Телеком, 2012 . – 184 с. - ISBN 978-5-9912-0246-6 .;

3. 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 .;
4. 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 .;
5. 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 .;
6. Малюк А. А., Полянская О. Ю., Алексеева И. Ю.- "Этика в сфере информационных технологий", Издательство: "Горячая линия-Телеком", Москва, 2016 - (344 с.) https://e.lanbook.com/book/111076.

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. **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	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	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	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
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	А-317, 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

Теория информационной безопасности

(название дисциплины)

4 семестр

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

КМ-1 Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности. (Отчет)

КМ-1 Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей (Домашнее задание)

КМ-2 Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х». (Домашнее задание)

КМ-2 Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. (Отчет)

КМ-3 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-3 Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. (Отчет)

КМ-4 Контрольное задание № 1. Разработка матрицы доступа к защищаемой информации (Решение задач)

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

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-4	КМ-4
		Неделя КМ:	4	4	8	8	12	12	15	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. Виды Политик 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, %:	10	15	15	10	15	10	15	10