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

Направление подготовки/специальность: 27.04.04 Управление в технических системах

Наименование образовательной программы: Интеллектуальные технологии управления в технических системах, обработка и анализ данных

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.04**
Трудоемкость в зачетных единицах:	**2 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**2 семестр - 16 часов;**
Практические занятия	**2 семестр - 16 часов;**
Лабораторные работы	**2 семестр - 16 часов;**
Консультации	**2 семестр - 2 часа;**
Самостоятельная работа	**2 семестр - 129,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Лабораторная работа**	
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: Елисеев В.Л. Идентификатор: R37a37292-YeliseevVL-9b2e3978	В.Л. Елисеев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бобряков А.В. Идентификатор: R2c90f415-BobriakovAV-70dec1fa	А.В. Бобряков
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бобряков А.В. Идентификатор: R2c90f415-BobriakovAV-70dec1fa	А.В. Бобряков

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение основных подходов и методов, обеспечивающих информационную безопасность компьютерных систем, включая системы криптографической защиты данных, средства разграничения доступа, защиты компьютеров и информационных систем.

Задачи дисциплины

- определение основных рисков, изучение подходов по их моделированию и устранению, целей и задач информационной безопасности;;
- освоение базовых понятий и классификации задач информационной безопасности компьютерных систем;;
- изучение симметричных и ассиметричных алгоритмов шифрования и аутентификации данных;;
- приобретение навыков использования криптографических и других систем для защиты данных и информационных систем..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-2 Способен разрабатывать и применять информационные системы обработки и анализа данных для автоматизации процессов управления в сложных технических и организационно-технических системах	ИД-1$_{ПК-2}$ Демонстрирует умение организовывать экспериментальные исследования и сбор экспертной информации, проводить анализ и предварительную обработку данных с применением автоматизированных информационных систем, выбирать обоснованные способы обеспечения защиты данных	знать: - назначение и общие принципы использования криптографических алгоритмов.; - основные подходы к решению задач информационной безопасности;. уметь: - выбирать комплекс мер для защиты информации и информационных систем..
ПК-2 Способен разрабатывать и применять информационные системы обработки и анализа данных для автоматизации процессов управления в сложных технических и организационно-технических системах	ИД-2$_{ПК-2}$ Может разрабатывать информационные и информационно-аналитические системы автоматизации процессов управления в сложных технических и организационно-технических системах	знать: - возможности и ограничения средств защиты информации и информационных систем.. уметь: - настраивать и использовать средства защиты информации и информационных систем..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Интеллектуальные технологии управления в технических системах, обработка и анализ данных (далее – ОПОП), направления подготовки 27.04.04 Управление в технических системах, 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	Основы информационной безопасности	24.0	2	2.0	4	2.0	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы информационной безопасности"
1.1	Введение в информационную безопасность (ИБ).	6.0		0.5	1	0.5	-	-	-	-	-	4	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Основы информационной безопасности" материалу. ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основы информационной безопасности" ***Изучение материалов литературных источников:*** [1], стр. 8-34, 195-202 [4], стр. 39-52 [5], стр. 106-133 [6], стр. 5-27
1.2	Правовые аспекты и преступления в сфере ИБ.	6.0		0.5	1	0.5	-	-	-	-	-	4	-	
1.3	Стандарты и рекомендации в сфере ИБ.	6.0		0.5	1	0.5	-	-	-	-	-	4	-	
1.4	Управление доступом.	6.0		0.5	1	0.5	-	-	-	-	-	4	-	
2	Основы криптографии и симметричные криптосистемы	26		4	-	4	-	-	-	-	-	18	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы криптографии и симметричные криптосистемы" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу
2.1	. Введение в криптографию.	6		1	-	1	-	-	-	-	-	4	-	
2.2	Блочные шифры и сеть Фейстеля.	7		1	-	1	-	-	-	-	-	5	-	

2.3	SP-сети.	7		1	-	1	-	-	-	-	-	5	-	"Основы криптографии и симметричные криптосистемы" ***<u>Изучение материалов литературных источников:</u>*** [1], стр. 35-66, 79-84 [2], стр. 241-249
2.4	Односторонние функции.	6		1	-	1	-	-	-	-	-	4	-	
3	Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей	28		4	4	4	-	-	-	-	-	16	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей"
3.1	Свойства симметричной криптографии.	10		2	1	1	-	-	-	-	-	6	-	***<u>Подготовка к лабораторной работе:</u>*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей" материалу. ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей" ***<u>Изучение материалов литературных источников:</u>*** [1], стр. 67-78, 85-92
3.2	Протокол распределения ключей Диффи-Хеллмана.	10		1	2	1	-	-	-	-	-	6	-	
3.3	Инфраструктура открытых ключей (PKI).	8		1	1	2	-	-	-	-	-	4	-	
4	Защита информации при сетевом взаимодействии	24		2	4	-	-	-	-	-	-	18	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Защита информации при сетевом взаимодействии"
4.1	Уровни защиты данных при их передаче по сети.	12		1	2	-	-	-	-	-	-	9	-	***<u>Подготовка к лабораторной работе:</u>*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита информации при сетевом
4.2	Протокол IPsec.	12		1	2	-	-	-	-	-	-	9	-	

														взаимодействии" материалу. ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Защита информации при сетевом взаимодействии" ***Изучение материалов литературных источников:*** [1], стр. 96-116
5	Средства защиты информационных и коммуникационных систем	22		2	-	4	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Средства защиты информационных и коммуникационных систем"
5.1	Объекты защиты информационных и коммуникационных систем.	11		1	-	2	-	-	-	-	-	8	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Средства защиты информационных и коммуникационных систем" материалу. ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Средства защиты информационных и коммуникационных систем" ***Изучение материалов литературных источников:*** [1], стр. 117-120, 243-277, 309-318
5.2	Технологии злоумышленников и уязвимости.	11		1	-	2	-	-	-	-	-	8	-	
6	Новые технологии информационной безопасности	20		2	4	2	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Новые технологии информационной безопасности"
6.1	Облегченная криптография.	20		2	4	2	-	-	-	-	-	12	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Новые технологии информационной безопасности" ***Изучение материалов литературных источников:***

														[2], стр. 235-240 [3], стр. 173-226
	Экзамен	36.00		-	-	-	-	2	-	-	0.5	-	33.50	
	Всего за семестр	**180.00**		**16.0**	**16**	**16.0**	**-**	**2**	**-**	**-**	**0.5**	**96**	**33.50**	
	Итого за семестр	**180.00**		**16.0**	**16**	**16.0**	**2**		**-**		**0.5**	**129.50**		

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 информационной безопасности

1.1. Введение в информационную безопасность (ИБ).

Основная задача информационной безопасности. Термины. Экономическая модель информационной безопасности. Угрозы и направления защиты информации..

1.2. Правовые аспекты и преступления в сфере ИБ.

Законы, регулирующие сферу ИБ в России. Регуляторы и их нормативные акты..

1.3. Стандарты и рекомендации в сфере ИБ.

Классификация систем криптографической защиты информации (СКЗИ) в России. Стандарт СКЗИ США FIPS 140-2. Общие критерии ISO/IEC-15408..

1.4. Управление доступом.

Идентификация. Методы аутентификации. Защита от несанкционированного доступа. Модели авторизации. Модели безопасности и примеры их реализации в современных операционных системах..

2. Основы криптографии и симметричные криптосистемы

2.1. . Введение в криптографию.

Основные понятия. Исторические шифры. Шифры замены и их свойства. Шифры перестановки. Блочные и поточные шифры. Шифр Вернама. Современные СКЗИ и требования, предъявляемые к ним. Общие принципы симметричной и асимметричной криптографической системы..

2.2. Блочные шифры и сеть Фейстеля.

Шифры DES и 3DES. Режимы работы блочного шифра. Шифр «Магма»..

2.3. SP-сети.

Введение в поля Галуа. Шифры AES и «Кузнечик». Понятие о криптоанализе и атаки на криптографическую систему..

2.4. Односторонние функции.

Криптографические хэш-функции. Контроль целостности и имитозащита. Режимы шифрования с имитозащитой (AEAD) на примере GCM..

3. Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей

3.1. Свойства симметричной криптографии.

Принцип обеспечения секретности асимметричной криптографии. Модульная арифметика и основные теоретические результаты, лежащие в основе асимметричных криптографических алгоритмов..

3.2. Протокол распределения ключей Диффи-Хеллмана.

Пример согласования ключей по протоколу Диффи-Хеллмана. Атака «Человек посередине». Криптосистема RSA и практические аспекты её реализации. Другие

асимметричные криптографические системы: Эль-Гамаля, на эллиптических кривых. Квантовый алгоритм Шора. Постквантовая криптография. Электронная подпись и её виды с точки зрения законодательства в России..

3.3. Инфраструктура открытых ключей (PKI).

Назначение и архитектура. Субъекты, объекты и основные компоненты PKI. Сертификаты, их жизненный цикл и цепочка доверия. Программные и аппаратные средства поддержки PKI. Стандарт X.509. Форматы данных объектов PKI. Примеры применения сертификатов..

4. Защита информации при сетевом взаимодействии

4.1. Уровни защиты данных при их передаче по сети.

Криптографическая защита и протоколы, её реализующие. Протокол TLS/SSL, его назначение и принципы применения. Установление защищенного соединения. Протокол HTTPS, особенности его применения. Легальный MitM. Certificate Pinning и его применение..

4.2. Протокол IPsec.

Формат пакета IPsec. Протоколы AH, ESP. Туннельный и транспортный режимы. Протокол IKE, ассоциация защиты и фазы установления соединения IPsec..

5. Средства защиты информационных и коммуникационных систем

5.1. Объекты защиты информационных и коммуникационных систем.

Задача защиты компьютерной инфраструктуры. Модель угроз и нарушителя. Назначение и основные возможности средств защиты информационных и коммуникационных систем. Технологии защиты на уровне отдельного компьютера. Антивирус. Персональный межсетевой экран. Сложности с защитой отдельного компьютера. Технологии защиты на уровне корпоративной сети. Защита на уровне государства. Система ГосСОПКА. Периметровый подход к организации защиты, его сфера применения и известные ограничения..

5.2. Технологии злоумышленников и уязвимости.

Безопасность компьютерных систем. Цели и методы компьютерных злоумышленников. Классификация уязвимостей. Реестры уязвимостей и компьютерных атак. Распространенные виды компьютерных атак..

6. Новые технологии информационной безопасности

6.1. Облегченная криптография.

Квантовое распределение ключей. Протокол BB84. Критерии секретности квантового распределения ключей. Криптографические методы в технологиях распределенного реестра. Интеллектуальные методы выявления компьютерных инцидентов..

3.3. Темы практических занятий

1. Новые технологии информационной безопасности;
2. Защита информации при сетевом взаимодействии;
3. Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей;
4. Основы криптографии и симметричные криптосистемы;

5. Основы информационной безопасности.

3.4. Темы лабораторных работ

1. Социальная инженерия и конкурентная разведка;
2. Анализ защищенности Web-сайта;
3. Защита сетевого соединения;
4. Управление локальным и удаленным доступом.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основы информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Основы криптографии и симметричные криптосистемы"
3. Обсуждение материалов по кейсам раздела "Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей"
4. Обсуждение материалов по кейсам раздела "Защита информации при сетевом взаимодействии"
5. Обсуждение материалов по кейсам раздела "Средства защиты информационных и коммуникационных систем"
6. Обсуждение материалов по кейсам раздела "Новые технологии информационной безопасности"

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	4	5	6	
Знать:								
основные подходы к решению задач информационной безопасности;	ИД-1$_{ПК-2}$			+	+			Лабораторная работа/Лабораторная работа № 4 Тестирование/Тест № 3
назначение и общие принципы использования криптографических алгоритмов.	ИД-1$_{ПК-2}$	+	+	+			+	Тестирование/Тест № 1 Тестирование/Тест № 2
возможности и ограничения средств защиты информации и информационных систем.	ИД-2$_{ПК-2}$		+	+	+	+		Лабораторная работа/Лабораторная работа № 3 Тестирование/Тест № 4
Уметь:								
выбирать комплекс мер для защиты информации и информационных систем.	ИД-1$_{ПК-2}$	+	+		+	+		Лабораторная работа/Лабораторная работа № 1 Лабораторная работа/Лабораторная работа № 3 Тестирование/Тест № 1 Тестирование/Тест № 4
настраивать и использовать средства защиты информации и информационных систем.	ИД-2$_{ПК-2}$	+						Лабораторная работа/Лабораторная работа № 2 Лабораторная работа/Лабораторная работа № 4 Тестирование/Тест № 2 Тестирование/Тест № 3

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: Билеты (письменный опрос)

1. Тест № 1 (Тестирование)
2. Тест № 2 (Тестирование)
3. Тест № 3 (Тестирование)
4. Тест № 4 (Тестирование)

Форма реализации: Компьютерное задание

1. Лабораторная работа № 1 (Лабораторная работа)
2. Лабораторная работа № 2 (Лабораторная работа)
3. Лабораторная работа № 3 (Лабораторная работа)
4. Лабораторная работа № 4 (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №2)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

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. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров, С-Петерб. политехнич. ун-т Петра Великого. ПОЛИТЕХ . – М. : Юрайт, 2017 . – 321 с. – (Университеты России) . - ISBN 978-5-534-00258-4 .;
2. Авдошин, С. М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин . – М. : ДМК Пресс, 2017 . – 352 с. - ISBN 978-5-97060-408-3 .;
3. Альбов, А. С. Квантовая криптография / А. С. Альбов . – СПб. : Страта, 2018 . – 248 с. – (Просто) . - Автор идеи и науч. ред. серии Сергей Деменок . - ISBN 978-5-906150-35-6 .;
4. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев . – 3-е изд . – Москва : Изд-во МГТУ им. Н.Э. Баумана, 2021 . – 250 с. - ISBN 978-5-7038-5541-6 .;
5. Войтов, Н. М. Основы работы с Linux : учебный курс / Н. М. Войтов . – М. : ДМК, 2016 . – 216 с. - ISBN 978-5-94074-380-2 .;
6. А. В. Артемов- "Информационная безопасность: курс лекций", Издательство: "Межрегиональная академия безопасности и выживания", Орел, 2014 - (257 с.) https://biblioclub.ru/index.php?page=book&id=428605.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. OpenVPN;
2. ОС Linux.

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. **Национальная электронная библиотека** - https://rusneb.ru/
7. **База данных IEL издательства IEEE (Institute of Electrical and Electronics Engineers, Inc.)** - https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Портал открытых данных Российской Федерации** - https://data.gov.ru
10. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
11. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
12. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
13. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
14. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
15. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
16. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
17. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
18. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
19. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-307, Учебная аудитория	стол преподавателя, стол учебный, стул, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	М-307, Учебная аудитория	стол преподавателя, стол учебный, стул, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер

Учебные аудитории для проведения лабораторных занятий	М-304а/1, Учебная лаборатория моделирования систем и анализа данных	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, доска маркерная, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-307, Учебная аудитория	стол преподавателя, стол учебный, стул, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-304а/2, Учебная лаборатория моделирования систем и анализа данных	кресло рабочее, стол преподавателя, стол учебный, стул, шкаф для документов, шкаф для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный
Помещения для хранения оборудования и учебного инвентаря	М-309, Кладовая	стол, стул, шкаф для хранения инвентаря
	М-301/1, Кладовая	стул

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Информационная безопасность в компьютерных системах

(название дисциплины)

2 семестр

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

КМ-1 Тест № 1 (Тестирование)
КМ-2 Лабораторная работа № 1 (Лабораторная работа)
КМ-3 Тест № 2 (Тестирование)
КМ-4 Лабораторная работа № 2 (Лабораторная работа)
КМ-5 Тест № 3 (Тестирование)
КМ-6 Лабораторная работа № 3 (Лабораторная работа)
КМ-7 Тест № 4 (Тестирование)
КМ-8 Лабораторная работа № 4 (Лабораторная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8
		Неделя КМ:	3	4	7	8	11	12	14	15
1	Основы информационной безопасности									
1.1	Введение в информационную безопасность (ИБ).				+	+	+			+
1.2	Правовые аспекты и преступления в сфере ИБ.				+	+	+			+
1.3	Стандарты и рекомендации в сфере ИБ.		+		+	+	+			+
1.4	Управление доступом.		+	+	+	+	+	+	+	+
2	Основы криптографии и симметричные криптосистемы									
2.1	. Введение в криптографию.		+	+	+			+	+	
2.2	Блочные шифры и сеть Фейстеля.		+	+	+			+	+	
2.3	SP-сети.		+		+			+	+	
2.4	Односторонние функции.		+		+			+	+	
3	Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей									
3.1	Свойства симметричной криптографии.		+		+			+	+	

3.2	Протокол распределения ключей Диффи-Хеллмана.	+		+		+			+
3.3	Инфраструктура открытых ключей (PKI).					+			+
4	Защита информации при сетевом взаимодействии								
4.1	Уровни защиты данных при их передаче по сети.					+	+	+	+
4.2	Протокол IPsec.	+	+			+	+	+	+
5	Средства защиты информационных и коммуникационных систем								
5.1	Объекты защиты информационных и коммуникационных систем.	+	+				+	+	
5.2	Технологии злоумышленников и уязвимости.						+	+	
6	Новые технологии информационной безопасности								
6.1	Облегченная криптография.	+		+					
	Вес КМ, %:	10	15	15	15	10	10	15	10