

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

Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника

Наименование образовательной программы: Вычислительные машины, комплексы, системы и сети

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б1.Ч.08
Трудоемкость в зачетных единицах:	7 семестр - 4;
Часов (всего) по учебному плану:	144 часа
Лекции	7 семестр - 16 часов;
Практические занятия	не предусмотрено учебным планом
Лабораторные работы	7 семестр - 32 часа;
Консультации	7 семестр - 2 часа;
Самостоятельная работа	7 семестр - 93,5 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая: Интервью Лабораторная работа Тестирование	
Промежуточная аттестация:	
Экзамен	7 семестр - 0,5 часа;

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Рытов А.А.
	Идентификатор	R37263e31-RytovAA-c7235577

(подпись)

А.А. Рытов

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Гольцов А.Г.
	Идентификатор	R64210572-GoltsovAG-cebbd3e8

(подпись)

А.Г. Гольцов

(расшифровка подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

(подпись)

С.В. Вишняков

(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Изучение математических основ криптологии, изучение основ информационной безопасности компьютерных систем, формирование у слушателей знаний и навыков, которые необходимы для эффективного применения средств защиты информации от несанкционированного доступа.

Задачи дисциплины

- изучение алгебраических и информационных основ криптологии, а также элементов теории вероятности и теории сложности;
- освоение классификации защищаемой информации, её свойств и правовых вопросов, связанных с защитой информации;
- изучение основных принципов обеспечения безопасности автоматизированных систем обработки информации;
- реализация парольных систем в целях защиты информации от несанкционированного доступа.

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-1 Способен обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	ИД-3 _{ПК-1} Производит оценку влияния применяемых технических решений на общее функционирование системы	знать: - показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста. уметь: - обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-1 _{ПК-2} Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	знать: - методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем. уметь: - использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-2ПК-2 Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	<p>знать:</p> <ul style="list-style-type: none"> - угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации. <p>уметь:</p> <ul style="list-style-type: none"> - – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-4ПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	<p>знать:</p> <ul style="list-style-type: none"> - способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты. <p>уметь:</p> <ul style="list-style-type: none"> - использовать современные инструментальные средства и технологии программирования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Вычислительные машины, комплексы, системы и сети (далее – ОПОП), направления подготовки 09.03.01 Информатика и вычислительная техника, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать Дискретную математику
- знать Информатику
- знать Схемотехнику
- знать Программирование
- уметь конвертировать данные из одной системы счисления в другую
- уметь вводить и обрабатывать информацию средствами операционной системы
- уметь разрабатывать алгоритмы обработки данных сложной структуры
- уметь работать с виртуальными средами

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 4 зачетных единицы, 144 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	Математические основы криптологии	42	7	6	12	-	-	-	-	-	-	24	-	<p><u>Подготовка к аудиторным занятиям:</u> Подготовка к защите лаб. раб. № 9,10, [8], стр. 12-20, [2] стр 181-188</p> <p><u>Подготовка к контрольной работе:</u> Подготовка к защите лаб. раб. № 6, 7, К332</p> <p><u>Подготовка к аудиторным занятиям:</u> Подготовка к защите лаб. раб. № 5 [1], стр. 63-96</p> <p><u>Подготовка к аудиторным занятиям:</u> Подготовка к защите лабораторных работ № 1,2,3 К331 [1], стр. 12-62;</p> <p><u>Изучение материалов литературных источников:</u> [2], стр. 302-315 [4], стр. 1-16 [5], стр. 301-318 [6], п. 11.1-11.3</p>		
1.1	Математические основы криптологии	42		6	12	-	-	-	-	-	-	24	-			
2	Информационная безопасность компьютерных систем	48		6	16	-	-	-	-	-	-	-	26		-	<p><u>Подготовка к аудиторным занятиям:</u> Подготовка к защите лаб. раб. № 11,12,13 [8], стр. 111-158,</p> <p><u>Изучение материалов литературных источников:</u> [1], стр. 1-32 [5], стр. 12-30 [7], стр. 1-31</p>
2.1	Информационная безопасность компьютерных систем	48		6	16	-	-	-	-	-	-	-	26		-	
3	Парольные системы	18		4	4	-	-	-	-	-	-	-	10		-	
3.1	Парольные системы	18		4	4	-	-	-	-	-	-	-	10		-	<p><u>Подготовка к аудиторным занятиям:</u> Подготовка к защите лаб. раб. № 9,10, [8], стр. 12-20, [2] стр 181-188</p>

													<i><u>Изучение материалов литературных источников:</u></i> [3], стр. 25-60
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	144.0	16	32	-	-	2	-	-	0.5	60	33.5	
	Итого за семестр	144.0	16	32	-	2	-	-	0.5	60	33.5	93.5	

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. Математические основы криптологии

1.1. Математические основы криптологии

Множества и отображения. Сюръекция, инъекция, биекция. Бинарные отношения. Бинарные операции. Алгебраические структуры. Полугруппы и моноиды. Группа, абелева группа, циклическая и конечная группа. Кольца, идеал. Поля, примеры полей, образующий элемент, простые поля. Парадокс дней рождений. Лямбда – алгоритм Полларда. Функция возведения в степень по модулю. Математические модели открытого текста. Частотные характеристики. Вероятностная модель первого приближения. Теория сложности. Большие числа. Сложность алгоритмов. Сложность проблем. Машина Тьюринга. Детерминированное полиномиальное время. Полиномиальные вычислительные задачи. Оценки сложности основных операций в модулярной арифметике. Недетерминированное полиномиальное время. Классы сложности..

2. Информационная безопасность компьютерных систем

2.1. Информационная безопасность компьютерных систем

Типы секретных систем. Обзор литературы. Определение информации. Классификация защищаемой информации и ее носителей. Правовая основа. Государственная тайна. Коммерческая тайна. Информация как продукт. Характеристики информации. Количество информации в сообщении. Энтропия и неопределенность. Избыточность информации. Энтропия языка. Стойкость криптосистем. Расстояние единственности. Основные понятия. Политика безопасности. Основные угрозы безопасности АСОИ. Компоненты АСОИ. Основные каналы несанкционированного доступа. Обеспечение безопасности АСОИ. Матрица доступа. Домен безопасности. Основы проектирования системы защиты АСОИ. Меры обеспечения безопасности компьютерных систем. Классы защищенности АСОИ. Подсистема управления доступом. Подсистема регистрации и учета. Подсистема криптографической защиты. Подсистема обеспечения целостности. Хранение секретов. Безопасность хранения информации на жестких дисках. Методы уничтожения информации на НЖМД. Алгоритм Гутманна..

3. Парольные системы

3.1. Парольные системы

Парольные системы для защиты от несанкционированного доступа к информации. Основные термины. Методы аутентификации. Биометрические методы. Требования к выбору и использованию паролей. Длина паролей и безопасное время. Хранение паролей. Хэш-функция. Аутентификация "с нулевым разглашением". Противодействие пассивному перехвату. Защита при компрометации проверяющего. Противодействие несанкционированному воспроизведению. Одноразовые пароли. Метод «запрос-ответ»..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Лабораторная работа №4 Модулярная арифметика. Определение обратного элемента в конечном поле.;
2. Лабораторная работа №5."Парадокс дней рождений";
3. Лабораторная работа №1."Элементы множеств. Простые типы данных в системе Mathematica";

4. Лабораторная работа №2. "Элементы множеств. Сложные типы данных и их функции в системе Mathematica";
5. Лабораторная работа №3. "Методы автоматизированной подготовки открытого текста (plaintext) к операциям шифрования. Работа со строками и массивами";
6. Лабораторная работа №6 Средства анализа данных.;
7. Лабораторная работа МСЗИ №12 (SNS 3-2) "Настройка механизма дискреционного управления доступом";
8. Лабораторная работа №8 Защита информации по паролю в WinWord и 7-Zip. Системы восстановления паролей AOPR и ARPR.;
9. Лабораторная работа МСЗИ №9 (SNS 2-1) "Локальная настройка Secret Net Studio в соответствии с заданными параметрами";
10. Лабораторная работа МСЗИ №10 (SNS 2-2) "Настройка механизма контроля целостности";
11. Лабораторная работа №7. Удаление и восстановление информации на магнитном носителе.;
12. Лабораторная работа МСЗИ №11 (SNS 3-1) "Настройка полномочного управления доступом".

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Математические основы криптологии"
2. Обсуждение материалов по кейсам раздела "Информационная безопасность компьютерных систем"
3. Обсуждение материалов по кейсам раздела "Парольные системы"

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:					
показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста	ИД-3ПК-1		+		Лабораторная работа/Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) Тестирование/Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%)
методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем	ИД-1ПК-2			+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%)
угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации	ИД-2ПК-2			+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное

					занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%)
способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	ИД-4ПК-2			+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). Тестирование/Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) Интервью/Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%)
Уметь:					
обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования	ИД-3ПК-1			+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) Тестирование/Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%)
использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ	ИД-1ПК-2			+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%)

				Интервью/Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%)
– устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	ИД-2ПК-2		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). Тестирование/Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) Интервью/Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%)
использовать современные инструментальные средства и технологии программирования	ИД-4ПК-2		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%)

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

4.1. Текущий контроль успеваемости

7 семестр

Форма реализации: Компьютерное задание

1. Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). (Лабораторная работа)
2. Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)
3. Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)
4. Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
5. Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)
6. Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью)
2. Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%) (Интервью)
3. Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%) (Интервью)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №7)

Итоговая оценка по курсу может быть рассчитана как среднее от текущей успеваемости и итогов промежуточной аттестации по 100 балльной шкале. Текущая успеваемость также рассчитывается как среднее по трем модулям по 100 балльной шкале. Только после этого можно переходить к 5-и балльной шкале. Промежуточное округление оценок в 5-и балльной системе и нелинейная шкала оценок в БАРС приводят к существенному завышению результирующих оценок.

В диплом выставляется оценка за 7 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Бондаренко И. С., Демчишин Ю. В.- "Методы и средства защиты информации", Издательство: "МИСИС", Москва, 2018 - (32 с.)
<https://e.lanbook.com/book/115269>;
2. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата вузов по инженерно-техническим направлениям и специальностям / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, Нац. исслед. ун-т "Высшая школа экономики" . – 2-е изд., испр . – М. : Юрайт, 2018 . – 473 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-01530-0 .;

3. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учебное пособие для вузов по направлению 230100(654600) "Информатика и вычислительная техника" / П. Б. Хорев . – 4-е изд., стер . – М. : АКАДЕМИЯ, 2008 . – 256 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-5118-5 .;
4. Рытов, А. А. Парадокс дней рождений. Лабораторная работа №4 : методическое пособие по курсу "Методы и средства защиты информации" по направлению "Информатика и вычислительная техника" / А. А. Рытов, И. А. Яшин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2014 . – 16 с.;
5. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин . – М. : Радио и связь, 1999 . – 328 с. - ISBN 5-256-01436-6 : 53.00 .;
6. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си : пер. с англ. / Б. Шнайер . – М. : Триумф, 2002 . – 816 с. - ISBN 5-89392-055-4 .;
7. Костин В. Н.- "Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей", Издательство: "МИСИС", Москва, 2018 - (31 с.)
<https://e.lanbook.com/book/116743>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. Office / Российский пакет офисных программ;
2. Windows / Операционная система семейства Linux;
3. Acrobat Reader;
4. Scilab.

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. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	3-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Учебные аудитории для проведения лабораторных занятий	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	3-506, Аналоговые и цифровые системы обработки и передачи информации	стол преподавателя, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, лабораторный стенд, сервер, компьютер персональный, инвентарь специализированный
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	3-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный

	3-506, Аналоговые и цифровые системы обработки и передачи информации	стол преподавателя, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, лабораторный стенд, сервер, компьютер персональный, инвентарь специализированный
Помещения для самостоятельной работы	Е-522/3, Компьютерный класс №1	стол преподавателя, стол компьютерный, стул, доска маркерная, компьютер персональный
	Е-522/4, Компьютерный класс №2	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	Е-522/6, Компьютерный класс №3	стол преподавателя, стол компьютерный, стул, доска маркерная, компьютер персональный
	Е-522/9, Компьютерный класс №4	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Помещения для консультирования	3-508, Кабинет сотрудников каф. "ВМСС"	
Помещения для хранения оборудования и учебного инвентаря	3-308, Помещение для инвентаря	

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Методы и средства защиты информации

(название дисциплины)

7 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%) (Интервью)
- КМ-2 Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)
- КМ-3 Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
- КМ-4 Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью)
- КМ-5 Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)
- КМ-6 Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)
- КМ-7 Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%) (Интервью)
- КМ-8 Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). (Лабораторная работа)
- КМ-9 Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) (Тестирование)

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	КМ-9
		Неделя КМ:	4	4	8	12	12	12	16	16	16
1	Математические основы криптологии										
1.1	Математические основы криптологии		+	+	+						
2	Информационная безопасность компьютерных систем										
2.1	Информационная безопасность компьютерных систем					+	+	+			
3	Парольные системы										
3.1	Парольные системы								+	+	+
Вес КМ, %:			3	8	22	3	8	22	3	8	23