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: Информационные технологии

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ЗАЩИТА ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.26**
Трудоемкость в зачетных единицах:	**8 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**8 семестр - 24 часа;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**8 семестр - 24 часа;**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 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	**8 семестр - 0,5 часа;**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Рытов А.А. Идентификатор: R37263e31-RytovAA-c7235577	А.А. Рытов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Целью освоения дисциплины является изучение методов защиты информации и формирование практических навыков по обеспечению информационной безопасности процессов хранения, преобразования и передачи компьютерной информации.

Задачи дисциплины

- ознакомление с основными методами защиты информации;
- освоение современных стандартов шифрования;
- освоение принципов управления ключевой информацией;
- ознакомление с основными принципами финансовой криптографии;
- формирование навыков работы с современными криптосистемами.

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-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-2$_{ОПК-3}$ Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	знать: - угрозы безопасности при работе в сети Интернет. уметь: - устанавливать и применять средства защиты информации при её хранении и передаче по сети.
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: - принципы построения современных криптографических систем; - этапы проведения эксперимента по проверке корректности принимаемого проектного решения; - способы и технологии применения криптографии в решении задач идентификации и аутентификации; - основные алгоритмы и стандарты криптографической защиты информации. уметь: - использовать современные инструментальные средства и технологии программирования; - осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности; - инсталлировать, тестировать,

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты; - использовать современные информационные технологии при решении задач защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Информационные технологии (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
- знать Методы и средства защиты информации
- уметь Определять вычет в конечном поле
- уметь Производить перевод данных из двоичной системы в шестнадцатеричную
- уметь Представлять двоичные данные в полиномиальной форме
- уметь Проектировать регистры сдвига с последовательно-параллельным вводом данных
- уметь Разрабатывать сложные программные модули на современных языках программирования
- уметь Определять энтропию криптосистемы
- уметь Оценивать ожидаемое время раскрытия ключа криптосистемы

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	Традиционные симметричные криптосистемы	24	8	4	6	-	-	-	-	-	-	14	-	***Подготовка к аудиторным занятиям:*** Повторение материала по разделу "Традиционные симметричные криптосистемы" и подготовка защите лабораторных работ №1,2,3 [1] стр. 7-39; [7] стр. 1-32; [8] стр. 1-36;
1.1	Традиционные симметричные криптосистемы	24		4	6	-	-	-	-	-	-	14	-	
2	Проектирование и анализ потоковых шифров	22		4	6	-	-	-	-	-	-	12	-	***Подготовка к аудиторным занятиям:*** Повторение материала по разделу "Проектирование и анализ потоковых шифров", выполнение и подготовка к защите лабораторных работ №4,6,7 [2], стр. 150-169, 192-200,200-207. [3], стр. 156-168, [9] стр. 1-16
2.1	Проектирование и анализ потоковых шифров	22		4	6	-	-	-	-	-	-	12	-	
3	Современные симметричные криптосистемы	24		6	6	-	-	-	-	-	-	12	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Современные симметричные криптосистемы и подготовка к контрольной работе, защита лабораторной работы №8 [1], стр. 73-148
3.1	Современные симметричные криптосистемы	24		6	6	-	-	-	-	-	-	12	-	
4	Асимметричные криптосистемы	18		4	4	-	-	-	-	-	-	10	-	***Подготовка к аудиторным занятиям:*** Повторение материала по разделу "Асимметричные криптосистемы" и подготовка к защите лабораторных работ №11,12 [1], стр. 182-251.
4.1	Асимметричные криптосистемы	18		4	4	-	-	-	-	-	-	10	-	
5	Управление криптографическими ключами	12		4	2	-	-	-	-	-	-	6	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Управление криптографическими ключами и подготовка к контрольной работе: [2], стр. 375-400.
5.1	Управление	12		4	2	-	-	-	-	-	-	6	-	

	криптографическими ключами													
6	Алгоритмы шифрования на основе SP-сети	8		2	-	-	-	-	-	-	-	6	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Алгоритмы шифрования на основе SP-сети": [1] стр.124-136. [2], стр. 228-239.
6.1	Алгоритмы шифрования на основе SP-сети	8		2	-	-	-	-	-	-	-	6	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**24**	**24**	**-**	**-**	**2**	**-**	**-**	**0.5**	**60**	**33.5**	
	Итого за семестр	**144.0**		**24**	**24**	**-**	**2**		**-**		**0.5**	**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. Традиционные симметричные криптосистемы

1.1. Традиционные симметричные криптосистемы

Принципы криптографической защиты информации. Обобщенная схема симметричной криптосистемы. Обобщенная схема асимметричной криптосистемы. Варианты реализации криптосистем. Криптоаналитическая атака, фундаментальное правило криптоанализа. Традиционные симметричные криптосистемы. Шифр, ключ, криптостойкость. Требования, предъявляемые к шифрам. Алфавиты и n-граммы. Шифры перестановки. Шифр перестановки "скитала". Шифрующие таблицы. Одиночная и двойная перестановка по ключу. Применение магических квадратов. Шифры простой замены. Полибианский квадрат. Система шифрования Цезаря. Математический анализ шифра простой замены (подстановки). Афинная система подстановок Цезаря. Система Цезаря с ключевым словом. Шифры простой замены. Шифрующие таблицы Трисемуса . Биграммный шифр Плейфейра . Криптосистема Хилла . Система омофонов . Шифры сложной замены. Шифр Гронсфельда . Система шифрования Вижинера. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом Вернама..

2. Проектирование и анализ потоковых шифров

2.1. Проектирование и анализ потоковых шифров

Шифрование методом гаммирования. Линейные конгруэнтные генераторы. Генератор Макларена-Марсальи . Генератор Фибоначчи с запаздываниями. Регистры сдвига с линейной обратной связью. РСЛОС конфигурации Фибоначчи и Галуа. Проектирование и анализ потоковых шифров. Линейная сложность. Потоковые шифры на основе РСЛОС. Генератор Геффе . Чередующийся генератор «старт-стоп». Каскад Голлманна. Шифр A5 . Регистры сдвига с обратной связью по переносу. Регистры сдвига с нелинейной обратной связью. Генератор Блюма-Микали. Генератор RSA. Генератор BBS. Алгоритм RC4..

3. Современные симметричные криптосистемы

3.1. Современные симметричные криптосистемы

Современные симметричные криптосистемы. Американский стандарт шифрования данных DES. Сети Файстеля. 0сновные режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Стандарт шифрования данных ГОСТ 28147-89. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Алгоритм Blowfish. Структура алгоритма. Процедура расширения ключа. Достоинства и недостатки алгоритма Blowfish. Алгоритм шифрования RC2 . Структура алгоритма. Алгоритм RC5. Алгоритм RC6 ..

4. Асимметричные криптосистемы

4.1. Асимметричные криптосистемы

Асимметричные криптосистемы системы. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA . Процедуры шифрования и расшифрования в криптосистеме RSA. Пример-Шифрование сообщения CAB. Взлом RSA на основе подобранного шифртекста. Атаки при использовании общего модуля. Схема Полига-Хеллмана. Схема шифрования Эль Гамаля. Комбинированный метод шифрования. Электронная цифровая подпись. Однонаправленные хэш-функции. Adler-32. Алгоритм CRC. Алгоритм безопасного хэширования SHA. Функция хэширования ГОСТ Р 34.11-2012..

5. Управление криптографическими ключами

5.1. Управление криптографическими ключами

Управление криптографическими ключами. Ключевая информация. Генерация ключей. Стандарт ANSI X9.17. Модификация ключа. Хранение ключей. Носители ключевой информации. Концепция иерархии ключей. Схема аутентификации мастер -ключа хост-компьютера. Распределение ключей. Механизм запроса-ответа и механизм отметки времени. Распределение ключей с участием центра распределения для симметричных криптосистем. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей. Прямой обмен ключами между пользователями. Алгоритм открытого распределения ключей Диффи–Хеллмана. Алгоритм Диффи–Хеллмана с тремя и более участниками. Специальные алгоритмы для протоколов. Трехпроходный протокол Шамира. Скрытый канал на основе схемы Эль - Гамаля . Криптография с несколькими открытыми ключами. Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа. Криптография с временным раскрытием. Метод построения «шарад», основанный на последовательном применении операции возведения в квадрат. Квадратичные вычеты. Символ Лежандра. Символ Якоби. Протоколы с нулевым разглашением. Протокол Фиата—Шамира. Протокол идентификации Шнорра. Неотслеживаемость. Электронные деньги. Монетная система Чаума (David Chaum)..

6. Алгоритмы шифрования на основе SP-сети

6.1. Алгоритмы шифрования на основе SP-сети

Поля. Основные понятия. Порядок поля. Характеристика поля. Кольцо многочленов. Арифметика по модулю неприводимых многочленов. Поля GF(2n). Определение элементов ai поля. Алгебраические операции в поле Галуа GF(2n). Стандарт шифрования данных AES. Базовая единица обработки. Массив State. Математические предпосылки. Умножение в конечном поле GF (28). Умножение на x – операция xtime ( ). Полиномы с коэффициентами – элементами поля GF(28) . Описание алгоритма AES, основные параметры. Преобразование SubBytes ( ). Преобразование ShiftRows ( ). Преобразование MixColumns ( ). Преобразование AddRoundKey (). Процедура Key Expansion. Алгоритм «Кузнечик» ГОСТ Р 34.12-2015 . Основные параметры. XSL-конструкция. Преобразование X, преобразование S, преобразование L, раундовое преобразование R. Полнораундовый алгоритм зашифрования ГОСТ Р 34.12-2015. Алгоритм развертки ключа.

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Lab 2 Криптосистема Хилла;
2. Lab 3 Шифры перестановки;
3. Lab 1 Шифры простой замены;
4. Lab 6 РСЛОС;
5. Lab 11 Схемы разделения секрета;
6. Lab 8 Основы работы с системой «Криптон»;
7. Lab 7 Потоковый шифр;
8. Lab 9 Криптосистема RSA;
9. Lab 5 Система шифрования Вернама;
10. Lab 4 Система шифрования Вижинера;
11. Lab 10 ЭЦП RSA.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Традиционные симметричные криптосистемы"
2. Обсуждение материалов по кейсам раздела "Проектирование и анализ потоковых шифров"
3. Обсуждение материалов по кейсам раздела "Современные симметричные криптосистемы"
4. Обсуждение материалов по кейсам раздела "Асимметричные криптосистемы"
5. Обсуждение материалов по кейсам раздела "Управление криптографическими ключами"
6. Обсуждение материалов по кейсам раздела "Алгоритмы шифрования на основе SP-сети"

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:								
угрозы безопасности при работе в сети Интернет	ИД-2$_{ОПК-3}$				+			Лабораторная работа/Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) Тестирование/Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) Интервью/Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%)
основные алгоритмы и стандарты криптографической защиты информации	ИД-3$_{ПК-1}$					+		Лабораторная работа/Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) Тестирование/Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) Интервью/Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%)
способы и технологии применения криптографии в решении задач идентификации и аутентификации	ИД-3$_{ПК-1}$					+	+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) Интервью/Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%)
этапы проведения эксперимента по проверке корректности принимаемого проектного решения	ИД-3$_{ПК-1}$		+	+				Лабораторная работа/Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) Тестирование/Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%)

								Интервью/Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%)
принципы построения современных криптографических систем	ИД-3$_{ПК-1}$	+						Лабораторная работа/Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) Тестирование/Контрольно-зачетное занятие (КЗ31) по курсу ЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%)
Уметь:								
устанавливать и применять средства защиты информации при её хранении и передаче по сети	ИД-2$_{ОПК-3}$				+			Тестирование/Контрольно-зачетное занятие (КЗ33) по курсу ЗИ Модуль 3 (65%) Интервью/Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%)
использовать современные информационные технологии при решении задач защиты информации	ИД-3$_{ПК-1}$	+						Лабораторная работа/Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) Тестирование/Контрольно-зачетное занятие (КЗ31) по курсу ЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%)
инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	ИД-3$_{ПК-1}$					+		Тестирование/Контрольно-зачетное занятие (КЗ33) по курсу ЗИ Модуль 3 (65%)
осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	ИД-3$_{ПК-1}$		+					Лабораторная работа/Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) Тестирование/Контрольно-зачетное занятие (КЗ32) по курсу ЗИ Модуль 2 (65%)

								Интервью/Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%)
использовать современные инструментальные средства и технологии программирования	ИД-З$_{ПК-1}$					+	+	Тестирование/Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%)

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

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Компьютерное задание

1. Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) (Лабораторная работа)
2. Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа)
3. Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)
4. Контрольно-зачетное занятие (КЗЗ1) по курсу ЗИ Модуль 1 (65%) (Тестирование)
5. Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%) (Тестирование)
6. Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью)
2. Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%) (Интервью)
3. Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

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 бальной 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 8 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата вузов по инженерно-техническим направлениям / И. Н. Васильева, С.-Петерб. гос. экономич. ун-т . – М. : Юрайт, 2017 . – 349 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-02883-6 .;
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. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа : учебное пособие для вузов по специальностям 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации" / Л. К. Бабенко, Е. А. Ищукова . – М. : Гелиос АРВ, 2006 . – 376 с. - ISBN 5-85438-149-4 .;
4. 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 .;
5. 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 .;
6. Рытов, А. А. Шифры перестановки. Лабораторная работа №2 : практикум по курсу "Защита информации" по направлению "Информатика и вычислительная техника" / А. А. Рытов, И. А. Яшин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2016 . – 32 с. http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=8153;
7. Рытов, А. А. Шифры простой замены : практикум по курсу "Защита информации" по направлению 09.03.01 "Информатика и вычислительная техника" / А. А. Рытов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ") . – М. : Изд-во МЭИ, 2019 . – 36 с. - ISBN 978-5-7046-2167-6 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=10929;
8. Рытов, А. А. Исследование принципов формирования псевдослучайных последовательностей на основе регистров сдвига с линейными обратными связями. Лабораторная работа № 6 : методическое пособие по курсу "Защита 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. - книга только в электронном виде, перейти по ссылке в Электронную библиотеку МЭИ . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=7027;
9. Г. В. Басалова- "Основы криптографии: курс лекций", Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)", Москва, 2011 - (253 с.) https://biblioclub.ru/index.php?page=book&id=233689.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. Office / Российский пакет офисных программ;
2. Windows / Операционная система семейства Linux;
3. Acrobat Reader;
4. Python.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
2. **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
	Г-306, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории	Ж-120, Машинный	сервер, кондиционер

для проведения лабораторных занятий	зал ИВЦ	
	З-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
	З-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
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	З-508, Кабинет сотрудников каф. "ВМСС"	
Помещения для хранения оборудования и учебного инвентаря	З-308, Помещение для инвентаря	

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита информации

(название дисциплины)

8 семестр

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

КМ-1 Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%) (Интервью)
КМ-2 Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) (Лабораторная работа)
КМ-3 Контрольно-зачетное занятие (КЗЗ1) по курсу ЗИ Модуль 1 (65%) (Тестирование)
КМ-4 Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью)
КМ-5 Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа)
КМ-6 Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%) (Тестирование)
КМ-7 Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью)
КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)
КМ-9 Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ 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:	5	5	5	9	9	9	12	12	12
1	Традиционные симметричные криптосистемы										
1.1	Традиционные симметричные криптосистемы		+	+	+						
2	Проектирование и анализ потоковых шифров										
2.1	Проектирование и анализ потоковых шифров					+	+	+			
3	Современные симметричные криптосистемы										
3.1	Современные симметричные криптосистемы					+	+	+			
4	Асимметричные криптосистемы										
4.1	Асимметричные криптосистемы								+	+	+

5	Управление криптографическими ключами									
5.1	Управление криптографическими ключами							+	+	+
6	Алгоритмы шифрования на основе SP-сети									
6.1	Алгоритмы шифрования на основе SP-сети							+	+	+
	Вес КМ, %:	5	7	21	5	7	21	5	7	22