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

Направление подготовки/специальность: 02.03.02 Фундаментальная информатика и информационные технологии

Наименование образовательной программы: Информационные технологии и системы искусственного интеллекта

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ЗАЩИТА ДАННЫХ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.24**
Трудоемкость в зачетных единицах:	**7 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**7 семестр - 32 часа;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**7 семестр - 32 часа;**
Консультации	**7 семестр - 18 часов;**
Самостоятельная работа	**7 семестр - 93,2 часа;**
в том числе на КП/КР	**7 семестр - 15,7 часов;**
Иная контактная работа	**7 семестр - 4 часа;**
включая: **Лабораторная работа**	
Промежуточная аттестация:	
Экзамен **Защита курсовой работы**	**7 семестр - 0,5 часа;** **7 семестр - 0,3 часа;** **всего - 0,8 часа**

Москва 2025

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Хорев П.Б. Идентификатор: Rdf0a0f96-KhorevPB-ab4b01e2	П.Б. Хорев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Чернецов А.М. Идентификатор: Re594826f-ChernetsovAM-0080e09	А.М. Чернецов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Варшавский П.Р. Идентификатор: R9a563c96-VarshavskyPR-efb4bbd	П.Р. Варшавский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Приобретение необходимых теоретических знаний и практических навыков по защите данных и обеспечению информационной безопасности компьютерных систем и сетей.

Задачи дисциплины

- Ознакомление с общей постановкой задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацией методов ее решения;
- Представление способов идентификации и аутентификации субъектов компьютерных систем и сетей;
- Обучение выбору (разработке) и использованию конкретных программно-аппаратных средств защиты данных и безопасных информационных технологий;
- Представление методов разграничения доступа к объектам компьютерных систем, построения и использования симметричных и асимметричных криптографических 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**
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	ИД-2$_{ОПК-5}$ Устанавливает и инсталлирует программные комплексы, применяет основы сетевых технологий	знать: - Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей; - Модели и способы построения симметричных и асимметричных криптографических систем; - Достоинства и недостатки методов и программно-аппаратных средств защиты данных в компьютерных системах и сетях; - Достоинства и недостатки симметричных и асимметричных криптографических систем; - Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей. уметь: - Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации; - Разрабатывать новые программные средства защиты данных и безопасных информационных технологий; - Использовать результаты анализа защищенности для устранения уязвимостей в подсистемах безопасности компьютерных систем и

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		сетей.
ОПК-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1$_{ОПК-6}$ Выбирает современные информационно-коммуникационные технологии для решения прикладных задач	знать: - Тенденции развития средств защиты информации в операционных системах; - Стандарты оценки и методы анализа защищенности компьютерных систем и информационных технологий; - Тенденции развития методов защиты данных в компьютерных системах и сетях; - Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения. уметь: - Использовать средства анализа защищенности компьютерных систем и сетей; - Использовать методы и средства криптографической защиты информации; - Применять методы и программные средства защиты данных в компьютерных системах и сетях; - Определять цели и задачи разработки новых методов и программных средств защиты информации в компьютерных системах и сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Информационные технологии и системы искусственного интеллекта (далее – ОПОП), направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:
- знать Основные понятия общей алгебры и математической логики
- знать Архитектуру вычислительных систем
- знать Принципы построения и состав операционных систем
- уметь Программировать на языках высокого уровня и языке ассемблера с использованием инструментальных средств разработки
- уметь Использовать средства операционных систем при решении различных прикладных задач

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	Комплексный подход к обеспечению информационной безопасности	14	7	4	4	-	-	-	-	-	-	6	-	***Подготовка курсовой работы:*** Выбор темы курсовой работы. ***Подготовка к текущему контролю:*** 1. Повторение материала лекций 1-2. 2. Изучение литературы. ***Изучение материалов литературных источников:*** [1], Стр. 102-105, 151-154 [2], §§ 4.2, 5.3 [3], Глова 1 [4], Глава 1 [5], Глава 1
1.1	Комплексный подход к обеспечению информационной безопасности	14		4	4	-	-	-	-	-	-	6	-	
2	Защита от несанкционированного доступа к информации в компьютерных системах	42		14	14	-	-	-	-	-	-	14	-	***Подготовка курсовой работы:*** 1. Проектирование интерфейса программы для курсовой работы. 2. Разработка (поиск) алгоритма решения задачи курсовой работы. 3. Выбор языка и системы программирования для разрабатываемой программы. ***Подготовка к текущему контролю:*** 1. Повторение материала лекций 3-9. 2. Изучение литературы. 3. Подготовка ответов на контрольные вопросы к защите лабораторной работы 2. ***Подготовка к лабораторной работе:*** 1. Изучение заданий на лабораторные работы 1-2. 2. Проектирование программы для лабораторной работы 1.
2.1	Защита от несанкционированного доступа к информации в компьютерных системах	42		14	14	-	-	-	-	-	-	14	-	

														Изучение материалов литературных источников: [1], Стр. 17-52, 71-80 [2], §§ 4.3, 4.5, 5.2, 5.4 [3], Главы 2, 3 [4], Главы 3, 4 [5], Глава 7 [6], Стр. 4-10 [8], Лекции 1-4
3	Криптографические методы и средства защиты информации	36		10	10	-	-	-	-	-	-	16	-	***Подготовка курсовой работы:*** Разработка, тестирование и отладка программы для курсовой работы.
3.1	Криптографические методы и средства защиты информации	36		10	10	-	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** 1. Повторение материала лекций 10-14. 2. Изучение литературы. 3. Подготовка ответов на контрольные вопросы к защите лабораторной работы 5. ***Подготовка к лабораторной работе:*** 1. Изучение заданий на лабораторные работы 3-5. 2. Проектирование дополнительных функций программ для лабораторных работ 3-4. ***Изучение материалов литературных источников:*** [1], Стр. 52-56 [3], Главы 4, 5 [4], Глава 5 [5], Главы 5, 6 [6], Стр. 11-17 [7], Глава 1
4	Защита от вредоносных программ и несанкционированного копирования информационных ресурсов	16		4	4	-	-	-	-	-	-	8	-	***Подготовка курсовой работы:*** 1. Подготовка отчета о выполнении курсовой работы. 2. Подготовка к защите курсовой работы. ***Подготовка к текущему контролю:*** 1. Повторение материала лекций 15-16. 2. Изучение литературы. 3. Подготовка к защите лабораторной работы 6. ***Подготовка к лабораторной работе:*** 1.
4.1	Защита от вредоносных	16		4	4	-	-	-	-	-	-	8	-	

	программ и несанкционированного копирования информационных ресурсов													Изучение задания на лабораторную работу 6. 2. Проектирование (реализация дополнительных функций) программ для лабораторной работы 6. ***<u>Изучение материалов литературных источников:</u>*** [1], §§ 4.1-4.6 [3], Главы 6, 7 [4], Глава 7 [5], Глава 15
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	36.0		-	-	-	16	-	4	-	0.3	15.7	-	
	Всего за семестр	**180.0**		**32**	**32**	**-**	**16**	**2**	**4**	**-**	**0.8**	**59.7**	**33.5**	
	Итого за семестр	**180.0**		**32**	**32**	**-**	**18**		**4**		**0.8**	**93.2**		

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. Комплексный подход к обеспечению информационной безопасности

1.1. Комплексный подход к обеспечению информационной безопасности

Проблема защиты информации и подходы к ее решению. Основные понятия защиты информации. Угрозы информационной безопасности и каналы утечки информации. Комплексный подход к защите информации. Классификация методов и средств защиты информации. Специфика программных средств. Правовое обеспечение защиты информации..

2. Защита от несанкционированного доступа к информации в компьютерных системах

2.1. Защита от несанкционированного доступа к информации в компьютерных системах

Способы несанкционированного доступа и аутентификации пользователей. Аутентификация на основе паролей. Организация базы учетных записей и хранения паролей (на примере операционных систем Unix и Windows). Программно-аппаратная защита от локального несанкционированного доступа. Аутентификация пользователей на основе их биометрических характеристик. Аутентификация пользователей при удаленном доступе. Протоколы S/Key, CHAP, RADIUS и Kerberos. Использование технологии VPN для защиты от удаленного несанкционированного доступа. Дискреционное, мандатное и ролевое управление доступом к объектам компьютерных систем. Архитектура подсистемы безопасности, аутентификация пользователей и проверка прав доступа к объектам в операционных системах Windows и Unix. Аудит событий безопасности. Защита информации в глобальных компьютерных сетях (межсетевые экраны, сканеры уязвимостей автоматизированных систем, системы обнаружения атак и контроля содержания). Стандарты оценки безопасности компьютерных систем и информационных технологий..

3. Криптографические методы и средства защиты информации

3.1. Криптографические методы и средства защиты информации

Элементы теории чисел. Способы создания симметрических криптосистем. Абсолютно стойкий шифр. Криптографические системы DES и ГОСТ Р 34.12-2015. Применение и обзор современных симметричных криптосистем. Принципы построения асимметричных криптосистем. Криптографические системы RSA, Диффи-Хеллмана, Эль-Гамаля и на основе эллиптических кривых. Электронная подпись и ее применение. Функции хеширования. Использование асимметричных криптосистем. Протокол SSL. Криптографический интерфейс приложений операционной системы Windows (CryptoAPI). Использование функций CryptoAPI и криптографических классов Microsoft .Net. Файловая система с шифрованием в операционных системах Windows. Компьютерная стеганография и ее применение..

4. Защита от вредоносных программ и несанкционированного копирования информационных ресурсов

4.1. Защита от вредоносных программ и несанкционированного копирования информационных ресурсов

Вредоносные программы, их признаки и классификация. Загрузочные и файловые вирусы. Программные закладки и защита от них. Методы обнаружения и удаления вредоносных программ. Принципы построения систем защиты программного обеспечения от несанкционированного копирования. Защита от копирования инсталляционных дисков. Настройка устанавливаемого программного обеспечения на характеристики компьютера и пользователя. Защита программ от изучения..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Разработка программы разграничения полномочий пользователей на основе паролей;
2. Изучение и освоение программных средств защиты от несанкционированного доступа и разграничения прав пользователей;
3. Разработка и программная реализация алгоритмов симметричной криптографии и криптографического хеширования;
4. Использование криптографических средств операционных систем в прикладных программах;
5. Изучение и освоение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ;
6. Разработка средств защиты программного обеспечения от несанкционированного использования и копирования.

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации по порядку выполнения и защиты курсовой работы
2. Консультации по проектированию интерфейса разрабатываемой программы и подготовке отчетных материалов
3. Консультации по требованиям к разработке, тестированию и отладке программы для курсовой работы и представлению отчетных материалов
4. Консультации по содержанию и оформлению отчета о выполнении курсовой работы

Групповые консультации по разделам дисциплины (ГК)

1. 1. Консультации по проведению занятий, содержанию контрольных мероприятий и получению допуска к экзамену. 2. Консультации по разделу "Комплексный подход к обеспечению информационной безопасности".
2. Консультации по разделу "Защита от несанкционированного доступа к информации в компьютерных системах"
3. Консультации по разделу "Криптографические методы и средства защиты информации"
4. Консультации по разделу "Защита от вредоносных программ и несанкционированного копирования информационных ресурсов"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации по содержанию выбираемых тем курсовой работы
2. Консультации разработке (поиску) алгоритма решения задачи курсовой работы
3. Предварительная проверка результатов разработки программы для курсовой работы
4. Предварительная проверка и рецензирование отчетов о выполнении курсовой работы

3.6 Тематика курсовых проектов/курсовых работ

7 Семестр

Курсовая работа (КР)

Темы:

- Разработка программы обнаружения аутентификации пользователя
- Разработка программы протокола удаленного подключения
- Программная реализация алгоритма симметричного шифрования
- Программная реализация вычисления и проверки электронной подписи

- Разработка программы стеганографического скрытия и извлечения информации
- Программная реализация алгоритма асимметричного шифрования
- Разработка программы получения списка информационных ресурсов (файлов, папок, разделов реестра) к которым имеет доступ на чтение (запись) задаваемый пользователь (группа)
- Программная реализация для проведения стеганографического анализа контейнера формата JPEG
- Разработка программы получения списка пользователей, имеющих право доступа к выбираемому объекту
- Разработка программы аутентификации пользователей на основе их реакции на события
- Разработка программы выявления легко подбираемых паролей пользователей (совпадающих с паролями из специального словаря и (или) не удовлетворяющих задаваемым требованиям сложности и минимальной длины).
- Программная реализация для обнаружения скрытых объектов и потоков в файловой системе NTFS

График выполнения курсового проекта

Неделя	1 - 8	9 - 14	15 - 16	Зачетная
Раздел курсового проекта	1	2	3	Защита курсового проекта
Объем раздела, %	20	50	30	-
Выполненный объем нарастающим итогом, %	20	70	100	-

Номер раздела	Раздел курсового проекта
1	Проектирование интерфейса программной реализации
2	Выполнение программной реализации
3	Подготовка отчета о выполнении курсовой работы

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	
Знать:						
Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей	ИД-2$_{ОПК-5}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Достоинства и недостатки симметричных и асимметричных криптографических систем	ИД-2$_{ОПК-5}$			+		Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Достоинства и недостатки методов и программно-аппаратных средств защиты данных в компьютерных системах и сетях	ИД-2$_{ОПК-5}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Модели и способы построения симметричных и асимметричных криптографических систем	ИД-2$_{ОПК-5}$			+		Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3 Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей	ИД-2$_{ОПК-5}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения	ИД-1$_{ОПК-6}$	+				Лабораторная работа/Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2
Тенденции развития методов защиты данных в компьютерных системах и сетях	ИД-1$_{ОПК-6}$	+				Лабораторная работа/Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2
Стандарты оценки и методы анализа защищенности	ИД-1$_{ОПК-6}$				+	Лабораторная работа/Защита лабораторной

компьютерных систем и информационных технологий						работы 5; защита лабораторной работы 6
Тенденции развития средств защиты информации в операционных системах	ИД-1$_{ОПК-6}$			+		Лабораторная работа/Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Уметь:						
Использовать результаты анализа защищенности для устранения уязвимостей в подсистемах безопасности компьютерных систем и сетей	ИД-2$_{ОПК-5}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Разрабатывать новые программные средства защиты данных и безопасных информационных технологий	ИД-2$_{ОПК-5}$			+		Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации	ИД-2$_{ОПК-5}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Определять цели и задачи разработки новых методов и программных средств защиты информации в компьютерных системах и сетях	ИД-1$_{ОПК-6}$			+		Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Применять методы и программные средства защиты данных в компьютерных системах и сетях	ИД-1$_{ОПК-6}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №3
Использовать методы и средства криптографической защиты информации	ИД-1$_{ОПК-6}$			+		Лабораторная работа/Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5
Использовать средства анализа защищенности компьютерных систем и сетей	ИД-1$_{ОПК-6}$		+			Лабораторная работа/Защита лабораторной работы №2; защита лабораторной работы №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

7 семестр

Форма реализации: Компьютерное задание

1. Защита лабораторной работы 5; защита лабораторной работы 6 (Лабораторная работа)
2. Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 (Лабораторная работа)
3. Защита лабораторной работы №2; защита лабораторной работы №3 (Лабораторная работа)
4. Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5 (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №7)

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

Курсовая работа (КР) (Семестр №7)

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

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. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев. – М. : Форум, 2013. – 352 с. – (Высшее образование). – ISBN 978-5-91134-353-8.;
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : Учебное пособие по специальностям, не входящим в группу специальностей в области информационной безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – М. : Горячая Линия-Телеком, 2001. – 148 с. – ISBN 5-935170-62-0.;
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. Хорев, П. Б. Защита информационных систем : учебное пособие по курсам "Защита информации", "Методы и средства защиты компьютерной информации" по направлениям "Прикладная математика и информатика", "Информационные системы и технологии" и

"Прикладная информатика" / П. Б. Хорев, Моск. энерг. ин-т (МЭИ ТУ). – М. : Издательский дом МЭИ, 2010. – 88 с. – ISBN 978-5-383-00546-0.
http://elib.mpei.ru/elib/view.php?id=1956;
5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для среднего профессионального образования по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. – М. : Форум : ИНФРА-М, 2012. – 416 с. – (Профессиональное образование). – ISBN 978-5-8199-0331-5.;
6. Хорев, П. Б. Лабораторный практикум по методам и средствам защиты информации : учебное пособие по курсу "Информационная безопасность" по направлениям "Прикладная информатика", "Бизнес-информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ". – М. : Изд-во МЭИ, 2016. – 44 с. – ISBN 978-5-7046-1686-3.
http://elib.mpei.ru/elib/view.php?id=8167;
7. Хорев, П. Б. Использование средств шифрования данных в приложениях для Microsoft.Net : учебное пособие по курсу "Защита данных" по направлению "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ". – М. : Изд-во МЭИ, 2015. – 92 с. – ISBN 978-5-7046-1665-8.
http://elib.mpei.ru/elib/view.php?id=8104;
8. В. А. Галатенко- "Стандарты информационной безопасности", (2-е изд.), Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)", Москва, 2006 - (264 с.) https://biblioclub.ru/index.php?page=book&id=233065.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др);
5. Visual Studio.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **База данных Web of Science** - http://webofscience.com/
3. **База данных Scopus** - http://www.scopus.com
4. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
5. **Портал открытых данных Российской Федерации** - https://data.gov.ru
6. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
7. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
8. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-805, Учебная аудитория каф. "ПМИИ"	парта со скамьей, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный
Учебные аудитории для	М-914, Учебная	парта, стол преподавателя, стул, доска

проведения практических занятий, КР и КП	аудитория	меловая, компьютерная сеть с выходом в Интернет
Учебные аудитории для проведения лабораторных занятий	М-706, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-708, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-704, Преподавательская кафедры ПМИИ	стол, стул, шкаф, тумба, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, холодильник, кондиционер
Помещения для хранения оборудования и учебного инвентаря	М-703а/1, Кладовая каф. "ПМИИ"	стеллаж для хранения книг, тумба, экран, ноутбук, книги, учебники, пособия

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита данных

(название дисциплины)

7 семестр

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

КМ-1 Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 (Лабораторная работа)

КМ-2 Защита лабораторной работы №2; защита лабораторной работы №3 (Лабораторная работа)

КМ-3 Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5 (Лабораторная работа)

КМ-4 Защита лабораторной работы 5; защита лабораторной работы 6 (Лабораторная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Комплексный подход к обеспечению информационной безопасности					
1.1	Комплексный подход к обеспечению информационной безопасности		+			
2	Защита от несанкционированного доступа к информации в компьютерных системах					
2.1	Защита от несанкционированного доступа к информации в компьютерных системах			+		
3	Криптографические методы и средства защиты информации					
3.1	Криптографические методы и средства защиты информации		+	+	+	
4	Защита от вредоносных программ и несанкционированного копирования информационных ресурсов					
4.1	Защита от вредоносных программ и несанкционированного копирования информационных ресурсов					+
		Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Защита данных

(название дисциплины)

7 семестр

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

КМ-1 Выполнение части 1 «Проектирование интерфейса программной реализации»
КМ-2 Выполнение части 2 «Выполнение программной реализации»
КМ-3 Выполнение части 3. «Подготовка отчета о выполнении курсового проекта»

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	8	14	16
1	Проектирование интерфейса программной реализации		+		
2	Выполнение программной реализации			+	
3	Подготовка отчета о выполнении курсовой работы				+
		Вес КМ, %:	20	50	30