

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

Направление подготовки/специальность: 02.04.02 Фундаментальная информатика и информационные технологии

Наименование образовательной программы: Информационные технологии и системы искусственного интеллекта

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

| | |
|-----------------------------------------------|---------------------------------|
| Блок: | Блок 1 «Дисциплины (модули)» |
| Часть образовательной программы: | Обязательная |
| № дисциплины по учебному плану: | Б1.О.08 |
| Трудоемкость в зачетных единицах: | 3 семестр - 8; |
| Часов (всего) по учебному плану: | 288 часа |
| Лекции | 3 семестр - 16 часов; |
| Практические занятия | не предусмотрено учебным планом |
| Лабораторные работы | 3 семестр - 16 часов; |
| Консультации | 3 семестр - 18 часов; |
| Самостоятельная работа | 3 семестр - 233,2 часа; |
| в том числе на КП/КР | 3 семестр - 40 часов; |
| Иная контактная работа | 3 семестр - 4 часа; |
| включая: Лабораторная работа | |
| Промежуточная аттестация: | |
| Экзамен | 3 семестр - 0,5 часа; |
| Защита курсовой работы | 3 семестр - 0,3 часа; |
| | всего - 0,8 часа |

Москва 2026

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

| | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------|
|  | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» | |
| | Сведения о владельце ЦЭП МЭИ | |
| | Владелец | Сергеев А.В. |
| | Идентификатор | R45d170df-SergeevAVad-0ce1748 |

А.В. Сергеев

СОГЛАСОВАНО:

Руководитель
образовательной
программы

| | | |
|-----------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------|
|  | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» | |
| | Сведения о владельце ЦЭП МЭИ | |
| | Владелец | Варшавский П.Р. |
| | Идентификатор | R9a563c96-VarshavskyPR-efb4bbd |

П.Р.
Варшавский

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: изучение современных методов и средств защиты информации, включая криптографию, стеганографию, управление доступом, а также формирование навыков реагирования на инциденты информационной безопасности..

Задачи дисциплины

- Освоение методологии разработки модели угроз и модели нарушителя информационной безопасности;
- Получение навыков оценки защищенности продуктов информационных технологий и проектных решений по обеспечению информационной безопасности;
- Развитие компетенций в сфере использования передовых инструментов и техник защиты информации, включая обнаружение и предотвращение 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 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-1 Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий | ИД-2 _{ОПК-1} Осуществляет первичный сбор и анализ материала, интерпретирует различные математические объекты | знать: - Методы обнаружения угроз информационной системы; - Базовые структуры данных и механизмы поиска информации. уметь: - Проводить исследования компьютерных систем; - Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем. |
| ОПК-4 Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности | ИД-3 _{ОПК-4} Демонстрирует практический опыт анализа и интерпретации информационных систем с учетом требований информационной безопасности | знать: - Методы и средства защиты информационных процессов в компьютерных системах; - Методы и средства стеганографии. уметь: - Применять средства защиты информации; - Комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. |

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 02.04.02 Фундаментальная информатика и информационные технологии, уровень образования: высшее образование - магистратура.

Требования к входным знаниям и умениям:

- знать Основные понятия и положения теории информации и теории кодирования для анализа методов и способов кодирования и декодирования
- знать Принципы построения и состав операционных систем
- знать Структура и типы файловых систем
- знать Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей
- уметь Использовать средства операционных систем при решении различных прикладных задач
- уметь Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации
- уметь Использовать методы и средства криптографической защиты информации
- уметь Использовать средства анализа защищенности компьютерных систем и сетей

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 8 зачетных единиц, 288 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 | Основные методы реализации защиты информации в компьютерных системах. | 48 | 3 | 4 | 4 | - | - | - | - | - | - | 40 | - | <p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Основные методы реализации защиты информации в компьютерных системах." Подготовка отчета о выполнении лабораторной работы №1</p> <p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Основные методы реализации защиты информации в компьютерных системах." <u>Изучение материалов литературных источников:</u> [7], 22-29 [8], 4-6 [10], 32-54 [11], 38-56 [13], 12-27</p> | |
| 1.1 | Основные методы реализации защиты информации в компьютерных системах. | 48 | | 4 | 4 | - | - | - | - | - | - | - | 40 | | - |
| 2 | Криптографические методы защиты информации. | 48 | | 4 | 4 | - | - | - | - | - | - | - | 40 | | - |
| 2.1 | Криптографические методы защиты информации. | 48 | | 4 | 4 | - | - | - | - | - | - | - | 40 | | - |

| | | | | | | | | | | | | | |
|-----|--------------------------------------------------------------|------|---|---|---|---|---|---|---|---|------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | | | | | | | | | | | выполнения заданий по лабораторной работе необходимо предварительно изучить темы лекций и набор инструментов для анализа поставленной задачи по лабораторной работы №2, а так же изучить методы и подходы к решению задач в научной литературе <u>Изучение материалов литературных источников:</u> [1], 20-26 [9], 43-62 [10], 63-78 |
| 3 | Методы скрытия информации в цифровых носителях и их анализ. | 48 | 4 | 4 | - | - | - | - | - | - | 40 | - | <u>Подготовка курсовой работы:</u> Поиск и изучение материала по теме курсой работы <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Методы скрытия информации в цифровых носителях и их анализ." Подготовка ответов на контрольные вопросы к защите лабораторной работы №3. |
| 3.1 | Методы скрытия информации в цифровых носителях и их анализ. | 48 | 4 | 4 | - | - | - | - | - | - | 40 | - | <u>Подготовка к лабораторной работе:</u> Для выполнения заданий по лабораторной работе необходимо предварительно изучить задачи и вопросы по лабораторной работы №3 и подготовить необходимый набор программных средств <u>Изучение материалов литературных источников:</u> [2], 56-67 [3], 20-39 [5], 10-22 [8], 188-204 [10], 152-160 |
| 4 | Методы расследования инцидентов информационной безопасности. | 47.7 | 4 | 4 | - | - | - | - | - | - | 39.7 | - | <u>Подготовка к текущему контролю:</u> Подготовка отчета о выполнении лабораторной работы №4. <u>Подготовка к лабораторной работе:</u> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и |
| 4.1 | Методы | 47.7 | 4 | 4 | - | - | - | - | - | - | 39.7 | - | |

| | | | | | | | | | | | | | |
|-------------------------------------------------------|--------------|-----------|-----------|----------|-----------|----------|------------|--------------|------------|--------------|-------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| расследования инцидентов информационной безопасности. | | | | | | | | | | | | | задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Методы расследования инцидентов информационной безопасности." материалу. <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Методы расследования инцидентов информационной безопасности.", а также материала исследований и работ в соответствии с поставленными задачами Лабораторной работы №4. <u>Изучение материалов литературных источников:</u> [4], 8-16 [6], 80-93 [7], 230-241 [12], 42-61 |
| Экзамен | 36.0 | - | - | - | - | 2 | - | - | 0.5 | - | 33.5 | | |
| Курсовая работа (КР) | 60.3 | - | - | - | 16 | - | 4 | - | 0.3 | 40 | - | | |
| Всего за семестр | 288.0 | 16 | 16 | - | 16 | 2 | 4 | - | 0.8 | 199.7 | 33.5 | | |
| Итого за семестр | 288.0 | 16 | 16 | - | 18 | 4 | 0.8 | 233.2 | | | | | |

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КНР – 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. Основные методы реализации защиты информации в компьютерных системах.

1.1. Основные методы реализации защиты информации в компьютерных системах.

Основные термины и определения. Задачи информационной безопасности. Угрозы информационной безопасности, каналы утечки информации и факторы, воздействующие на информацию. Классификация методов и средств защиты информации.. Организационные меры защиты информации. Менеджмент событий и инцидентов информационной безопасности. Специфика программных средств. Журналы событий как источник информации.. Групповая политика безопасности. Методы анализа данных безопасности. Выявление угроз и уязвимостей..

2. Криптографические методы защиты информации.

2.1. Криптографические методы защиты информации.

Криптографические методы защиты информации. Применение и обзор современных симметричных криптосистем. Генераторы псевдослучайных чисел их применение в криптографии. Обзор и возможности средств криптографической защиты информации.. Основы структуры данных различных файловых форматов и их безопасность..

3. Методы скрытия информации в цифровых носителях и их анализ.

3.1. Методы скрытия информации в цифровых носителях и их анализ.

Основы стеганографии и скрытых каналов. Основные методы скрытия информации. Обзор стеганографических методов и алгоритмов. Применение стеганографии в реальном мире. Файловые системы, классификация. Виды и особенности файловых систем..

4. Методы расследования инцидентов информационной безопасности.

4.1. Методы расследования инцидентов информационной безопасности.

Концепция и базовые подходы в расследование инцидентов информационной безопасности. Методология расследования инцидентов. Инструменты и технологии расследования. Основные подходы к анализу метаданных и структуры файлов..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Компьютерная криминалистика;
2. Стеганография. Программные средства и методы;
3. Криптографические средства защиты информации и анализ защиты данных;
4. Оценка безопасности информационной системы.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основные методы реализации защиты информации в компьютерных системах."
2. Обсуждение материалов по кейсам раздела "Криптографические методы защиты информации."

- Обсуждение материалов по кейсам раздела "Методы скрытия информации в цифровых носителях и их анализ."

Текущий контроль (ТК)

- Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные методы реализации защиты информации в компьютерных системах."
- Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Криптографические методы защиты информации."
- Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы скрытия информации в цифровых носителях и их анализ."
- Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы расследования инцидентов информационной безопасности."

3.6 Тематика курсовых проектов/курсовых работ

3 Семестр

Курсовая работа (КР)

Темы:

- Разработка программы аутентификации пользователей на основе модели «рукопожатия»
- Разработка программы аутентификации пользователей по их клавиатурному почерку
- Программная реализация алгоритма симметричного шифрования
- Программная реализация функции хеширования
- Программная реализация для проведения стеганографического анализа контейнера формата docx
- Разработка программы стеганографического скрытия и извлечения информации
- Программная реализация для проведения стеганографического анализа контейнера формата PDF
- Программная реализация для проведения стеганографического анализа контейнера формата JPEG
- Разработка программы получения списка пользователей, имеющих право доступа к выбираемому объекту

График выполнения курсового проекта

| Неделя | 1 - 8 | 9 - 14 | 15 - 16 | Зачетная |
|-----------------------------------------|-------|--------|---------|--------------------------|
| Раздел курсового проекта | 1 | 2 | 3 | Защита курсового проекта |
| Объем раздела, % | 10 | 60 | 30 | - |
| Выполненный объем нарастающим итогом, % | 10 | 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: | | | | | | |
| Базовые структуры данных и механизмы поиска информации | ИД-2ОПК-1 | | + | | | Лабораторная работа/Криптографические средства защиты информации и анализ защиты данных |
| Методы обнаружения угроз информационной системы | ИД-2ОПК-1 | + | | | | Лабораторная работа/Оценка безопасности информационной системы |
| Методы и средства стеганографии | ИД-3ОПК-4 | | | + | | Лабораторная работа/Стеганография. Программные средства и методы |
| Методы и средства защиты информационных процессов в компьютерных системах | ИД-3ОПК-4 | | + | | | Лабораторная работа/Криптографические средства защиты информации и анализ защиты данных |
| Уметь: | | | | | | |
| Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем | ИД-2ОПК-1 | | | | + | Лабораторная работа/Компьютерная криминалистика |
| Проводить исследования компьютерных систем | ИД-2ОПК-1 | + | | | | Лабораторная работа/Оценка безопасности информационной системы |
| Комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности | ИД-3ОПК-4 | | | | + | Лабораторная работа/Компьютерная криминалистика |
| Применять средства защиты информации | ИД-3ОПК-4 | | | + | | Лабораторная работа/Стеганография. Программные средства и методы |

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Компьютерное задание

1. Компьютерная криминалистика (Лабораторная работа)
2. Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа)
3. Оценка безопасности информационной системы (Лабораторная работа)
4. Стеганография. Программные средства и методы (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 №3)

Определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

Курсовая работа (КР) (Семестр №3)

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

В диплом выставляется оценка за 3 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Бабаш, А. В. Информационная безопасность : история специальных методов криптографической деятельности : учебное пособие / А. В. Бабаши, Е. К. Баранова, Д. А. Ларин. – Москва : РИОР : ИНФРА-М, 2020. – 236 с. – (Высшее образование). – ISBN 978-5-369-01788-3.;
2. В. Г. Грибунин, И. Н. Оков, И. В. Туринцев- "Цифровая стеганография", Издательство: "СОЛОН-ПРЕСС", Москва, 2009 - (264 с.)
<https://biblioclub.ru/index.php?page=book&id=117549>;
3. Сергеев, А. В. Криптографические и стеганографические средства защиты данных : учебное пособие по курсу "Защита данных" по направлению 01.03.02 "Прикладная математика и информатика" / А. В. Сергеев, П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"). – Москва : Изд-во МЭИ, 2023. – 72 с. – ISBN 978-5-7046-2819-4.
<http://elib.mpei.ru/elib/view.php?id=12475>;
4. Хорев, П. Б. Криптографические протоколы : учебное пособие по курсу "Криптографические методы защиты информации" по направлению 01.03.02 "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"). – М. : Изд-во МЭИ, 2019. – 88 с. – ISBN 978-5-7046-2162-1.
<http://elib.mpei.ru/elib/view.php?id=10969>;

5. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, [и др.]. – М. : Вузовская книга, 2009. – 220 с. – ISBN 978-5-9502-0401-2.;
6. Мельников, Д. А. Информационные процессы в компьютерных сетях : Протоколы, стандарты, интерфейсы, модели... / Д. А. Мельников. – М. : Кудиц-Образ, 1999. – 256 с. – (Б-ка профессионала). – ISBN 5-933780-02-2 : 68.90.;
7. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с. – (Аспекты защиты). – ISBN 5-9800301-1-5.;
8. Хорев, П. Б. Объектно-ориентированное программирование с примерами на С# : учебное пособие для вузов по направлениям 01.03.02 "Прикладная математика и информатика" и 09.00.00 "Информатика и вычислительная техника" / П. Б. Хорев. – М. : Форум, 2018. – 200 с. – (Высшее образование. Бакалавриат). – ISBN 978-5-00091-144-0.;
9. Шнайер, Б. Прикладная криптография : протоколы, алгоритмы и исходные коды на языке С : пер. с англ. / Б. Шнайер. – 2-е изд. – Москва; Санкт-Петербург : Диалектика, 2022. – 1040 с. – Юбилейный выпуск к 20-летию книги. – Параллельн. тит. л. англ. – ISBN 978-5-9908462-4-1.;
10. Рябко Б. Я., Фионов А. Н.- "Основы современной криптографии и стеганографии", (2-е изд.), Издательство: "Горячая линия-Телеком", Москва, 2016 - (232 с.)
<https://e.lanbook.com/book/111098>;
11. Бахаров Л. Е.- "Информационная безопасность и защита информации (разделы криптография и стеганография)", Издательство: "МИСИС", Москва, 2019 - (59 с.)
<https://e.lanbook.com/book/116907>;
12. "Компьютерная криминалистика", Издательство: "СКФУ", Ставрополь, 2017 - (84 с.)
<https://e.lanbook.com/book/155227>;
13. "Стеганографические и криптографические методы защиты информации", Издательство: "БГПУ имени М. Акмуллы", Уфа, 2016 - (112 с.)
<https://e.lanbook.com/book/90963>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Видеоконференции (Майнд, Сберджаз, ВК и др);
3. Acrobat Reader;
4. Kali Linux;
5. Libre Office;
6. FAR Manager;
7. 7-zip.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - http://biblioclub.ru/index.php?page=main_ub_red
3. Научная электронная библиотека - <https://elibrary.ru/>
4. Электронные ресурсы издательства Springer - <https://link.springer.com/>
5. База данных Web of Science - <http://webofscience.com/>
6. База данных Scopus - <http://www.scopus.com>
7. 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>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, | Оснащение |
|---------------|------------------|-----------|
|---------------|------------------|-----------|

| | наименование | |
|-------------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | М-802, Учебная аудитория | парта, стул, доска интерактивная, компьютерная сеть с выходом в Интернет, доска маркерная |
| Учебные аудитории для проведения практических занятий, КР и КП | М-708, Дисплейный класс каф. "ПМИИ" | стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер |
| | 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 лабораторных занятий | М-708, 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 |

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Информационная безопасность компьютерных систем

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Оценка безопасности информационной системы (Лабораторная работа)
- КМ-2 Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа)
- КМ-3 Стеганография. Программные средства и методы (Лабораторная работа)
- КМ-4 Компьютерная криминалистика (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 | Основные методы реализации защиты информации в компьютерных системах. | | | | | |
| 1.1 | Основные методы реализации защиты информации в компьютерных системах. | | + | | | |
| 2 | Криптографические методы защиты информации. | | | | | |
| 2.1 | Криптографические методы защиты информации. | | | + | | |
| 3 | Методы скрытия информации в цифровых носителях и их анализ. | | | | | |
| 3.1 | Методы скрытия информации в цифровых носителях и их анализ. | | | | + | |
| 4 | Методы расследования инцидентов информационной безопасности. | | | | | |
| 4.1 | Методы расследования инцидентов информационной безопасности. | | | | | + |
| Вес КМ, %: | | | 30 | 20 | 20 | 30 |

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Информационная безопасность компьютерных систем

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Выполнение части 1 «Проектирование интерфейса программной реализации»

КМ-2 Выполнение части 2 «Выполнение программной реализации»

КМ-3 Подготовка и защита 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, %: | | | 10 | 60 | 30 |