федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет
Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Решение задач по криптографии
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Профиль подготовки: Математика. Информатика
Форма обучения: Очная

Разработчик:
Лапин К. С., канд. физ.-мат. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 13 от 17.05.2018 года

Зав. кафедрой _____Вознесенская Н. В.

Программа рассмотрена и утверждена на заседании кафедры, протокол № 12 от 18.06.2020 года

Зав. кафедрой _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

Зав. кафедрой _____Зубрилин А.А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - подготовка специалиста, владеющего методами криптографической защиты информации на компьютере

Задачи дисциплины:

- формирование знаний о криптографии, как науке о шифрование данных;
- выработка представлений о методах криптографической защиты информации;
- формирование умений защищать информацию на компьютере с использованием программых средств, использующих криптографию.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.03.04 «Решение задач по криптографии» относится к вариативной части учебного плана.

Дисциплина изучается на 3 курсе, в 5,6 семестре.

Для изучения дисциплины требуется: знание основ информационной безопасности

Изучению дисциплины «Криптографические основы безопасности» предшествует освоение дисциплин (практик):

Компьютерное моделирование;

Практикум по информационным технологиям.

Освоение дисциплины «Криптографические основы безопасности» является необходимой основой для последующего изучения дисциплин (практик):

Интернет-технологии.

Область профессиональной деятельности, на которую ориентирует дисциплина «Криптографические основы безопасности», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие;
- просвещение;
- образовательные системы.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-1. готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

педагогическая деятельность

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	знать: - методы криптографической защиты информации; уметь: - использовать программные средства для организации криптографической защиты информации на компьютере; владеть: - программными средствами для организации

	криптографической защиты информации на компьютере.
ПК-3. способностью решать задачи воспитания и духовно-нравственного развития, обучающихся в учебной и внеучебной деятельности	

педагогическая деятельность

ПК-3 способностью решать задачи воспитания и духовно-нравственного развития, обучающихся в учебной и внеучебной деятельности	знать: - программные продукты и сервисы сети Интернет для реализации криптографической защиты информации на компьютере; уметь: - использовать сервисы сети Интернет для шифрования информации; владеть: - методами шифрования информации.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Пятый семестр	Шестой семестр
Контактная работа (всего)	**36**	**18**	**18**
Практические	36	18	18
Самостоятельная работа (всего)	**72**	**36**	**36**
Виды промежуточной аттестации			
Зачет			+
Общая трудоемкость часы	**108**	**54**	**54**
Общая трудоемкость зачетные единицы	**3**	**1**	**2**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Введение в криптографию:

Предмет криптографии. Подходы к криптографической защите информации. Подходы к криптографической защите информации. Модели шифров. Решение задач на виды шифров.

Модуль 2. Системы шифрования с открытым ключом:

Алгоритмы симметричного шифрования. Алгоритмы шифрования. Криптосистемы. Хэш-функции. Решение задач по алгоритмам и хэш-функциям.

Модуль 3. Принципы построения криптографических алгоритмов:

Методы построения алгоритмов. Симметричные криптосистемы. Алгоритм Des. Решени задач по шифрованию с использованием алгоритмов.

Модуль 4. Криптографические стандарты и протоколы:

Криптографические протоколы. Электронная ЦП. Стандарты ЭЦП. Формирование ЭЦП. Повторение пройденного материала.

5.2. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Теоретические основы криптографической защиты информации (8 ч.)

Тема 1. Предмет криптографии. Основные понятия и алгоритмы криптографии (2 ч.)

Предмет криптографии. История развития криптографии. Цели и задачи изучения криптографии.

Подходы к криптографической защите информации. Криптография, криптология, стеганография.

Тема 2. Шифр и требования к нему. Оценка качества криптографических преобразований (2 ч.)

Модели шифров. Основной объект криптографии. Простейшие шифры. Надежность, имитостойкость и криптостойкостьшифров.

Решение задач с использованием основных видов шифров.

Тема 3. Системы открытого распределения ключей и открытого шифрования. Алгоритмы симметричного шифрования (2 ч.)

Алгоритмы симметричного шифрования. Анализ алгоритмов и решение типовых задач.

Алгоритм создания открытого и секретного ключей. Алгоритм шифрования RSA. Анализ алгоритмов и решение задач.

Тема 4. Криптосистемы (2 ч.)

Криптосистемы RSA и Эль-Гамаля. Преимущества асимметричных систем шифрования.

Криптографические хэш-функции. Характеристики и алгоритмы выработки хэш-функций.

Модуль 2. Практические вопросы криптографической защиты информации (10 ч.)

Тема 5. Криптографические интерфейсы. Способы и особенности реализации криптографических подсистем (2 ч.)

Решение криптографических задач на хэш-функции и алгоритмы шифрования. Анализ методических аспектов решения задач.

Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Применение алгоритмов к решению практических задач.

Тема 6. Прикладная криптография. Особенности сертификации и стандартизации. криптографических средств (2 ч.)

Основные классы симметричных криптосистем. Блочное и поточное шифрование. Программная реализация шифров. Исследование блочного алгоритма шифрования DES в MS Excel.

Закрепление теоретических знаний блочного шифрования на конкретных примерах.

Тема 7. Основные режимы шифрования. Простая замена. Гаммирование. Гаммирование с обратной связью (2 ч.)

Алгоритм DES шифрование 8-байтовых блоков открытого текста. Закрепление теоретических знаний блочного шифрования на конкретных примерах.

Основные примеры. классификация криптографических протоколов.

Тема 8. Электронная цифровая подпись (2 ч.)

Понятие электронной цифровой подписи. Стандарты ЭЦП.

Взаимосвязь между протоколами аутентификации и цифровой подписи. Технология формирования ЭЦП. Удостоверяющие

центры. Стандарт криптографического преобразования данных ГОСТ 28147-89.

Тема 9. Повторение изученного материала (2 ч.)

Повторение изученного материала. Решение задач по криптографии.

Модуль 3. Принципы построения криптографических алгоритмов (8 ч.)

Тема 10. Методы построения алгоритмов (2 ч.)

Принципы построения криптографических алгоритмов с симметричными

Тема 11. Симметричные криптосистемы (2 ч.)

Основные классы симметричных криптосистем. Блочное и поточное шифрование. программная реализация шифров. Исследование блочного алгоритма шифрования DES в MS Excel.

Тема 12. Блочное и поточное шифрование. (2 ч.)

Закрепление теоретических знаний блочного шифрования на конкретных примерах.

Тема 13. Алгоритм Des (2 ч.)

С помощью алгоритма DES шифрование 8-байтовых блоков открытого текста. акрепление теоретических знаний блочного шифрования на конкретных примерах.

Модуль 4. Криптографические стандарты и протоколы (10 ч.)

Тема 14. Криптографические протоколы. (2 ч.)

Основные примеры. классификация криптографических протоколов.

Тема 15. Электронная ЦП (2 ч.)

Понятие электронной цифровой подписи.

тандарты ЭЦП. Тема 16. Стандарты ЭЦП (2 ч.)

Взаимосвязь между протоколами аутентификации и цифровой подписи. Технология ормирования ЭЦП. Удостоверяющие центры. Стандарт криптографического реобразования данных ГОСТ 28147-89.

Тема 17. Формирование ЭЦП (2 ч.)

Процессы формирования и проверки электронной цифровой подписи ГОСТ Р 34.10-001. ГОСТ_Р_34.11-94 Информационная технология. Криптографическая защита нформации. Функция хеширования.

Тема 18. Повторение пройденного материала (2 ч.) Повторение пройденного атериала.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1 Вопросы и задания для самостоятельной работы

Пятый семестр (36 ч.)

Модуль 1. Теоретические основы криптографической защиты информации (18 ч.)

Вид СРС: *Выполнение компетентностно-ориентированных заданий

Изучите основные виды шифров, а также шифры, которые использовались в Древнем мире (не менее 10). Привести по 4 примера шифрования на каждый из изученных видов шифров.

Вид СРС: *Подготовка письменных работ (эссе, рефератов, докладов)

Подготовьте реферат на одну из следующих тем:

Научные подходы к криптографической защите информации.

Исторический обзор развития криптографии.

Криптология: принципы и методы.

Простейшие шифры замены и перестановки.

Шифры гаммирования и колонной замены.

Криптоаналитический частотный анализ одноалфавитных шифров.

Простейшие системы шифрования с открытым ключом.Способ нарушения конфиденциальности в системах с двухключевой схемой шифрования.

Криптографическая стойкость шифров.

Модуль 2. Практические вопросы криптографической защиты информации (18 ч.)

Вид СРС: *Выполнение компетентностно-ориентированных заданий

Приведите примеры на каждый изученный вид шифрования и объясните принципы указанных видов шифрования.

Вид СРС: *Подготовка письменных работ (эссе, рефератов, докладов)

Подготовьте реферат на одну из следующих тем:

Обзор криптографических алгоритмов и различных способов их применений.

ХЭШ – функция.

Достоинства и недостатки поточного шифрования.

Достоинства и недостатки блочного шифрования.

Алгоритмы сжатия данных. Сжатие с потерями.

Шифр Эль-Гамаля.

Криптосистема RSA.

Управление криптографическими ключами

Распределение ключей в асимметричных криптосистемах с использованием PKI.

Основные компоненты PKI.

Протокол согласования ключей Диффи-Хеллмана.

Шестой семестр (24 ч.)

Модуль 3. Принципы построения криптографических алгоритмов (18 ч.)

Вид СРС: *Подготовка к практическим / лабораторным занятиям

Привести по 3 примера на каждый изученный вид шифрования и объяснить ринципы указанных видов шифрования.

.Привести примеры решения задач.

Вид СРС: *Подготовка письменных работ (эссе, рефератов, докладов) Изучение ройденного теоретического материала.

Написание, оформление и защита реферата

Темы для реферата:

Обзор криптографических алгоритмов и различных способов их применений.

ХЭШ– функция.

Достоинства и недостатки поточного шифрования.

Достоинства и недостатки блочного шифрования.

Алгоритмы сжатия данных.

Сжатие с потерями.

Шифр Эль-Гамаля.

Криптосистема RSA.

Модуль 4. Криптографические стандарты и протоколы (18 ч.)

Вид СРС: *Подготовка к практическим / лабораторным занятиям

Привести по 3 примера на каждый изученный вид шифрования и объяснить принципы казанных видов шифрования.

Привести примеры решения задач

Вид СРС: *Подготовка письменных работ (эссе, рефератов, докладов)

Изучение пройденного теоретического материала.

Написание, оформление и защита реферата

Темы для реферата

Управление криптографическими ключами Распределение ключей в асимметричных риптосистемах с использованием PKI.

Основные компоненты PKI.

Протокол согласования ключей Диффи-Хеллмана.

Изучение стандартов криптографической защиты информации ГОСТ 28147—89,

ГОСТ Р 34.10-2001.

ГОСТ Р 34.11-94

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ПК-1	3 курс, Пятый		Модуль 1: Теоретические основы криптографической защиты информации.

	семестр		
ПК-3	3 курс, Пятый семестр		Модуль 2: Практические вопросы криптографической защиты информации.
ПК-1	3 курс, Шестой семестр	Зачет	Модуль 3: Принципы построения криптографических алгоритмов.
ПК-3	3 курс, Шестой семестр	Зачет	Модуль 4: Криптографические стандарты и протоколы.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:

Компетенция ПК-1 формируется в процессе изучения дисциплин:

3D моделирование, Алгебра, Алгоритмический подход в обучении математике, Аналитические вычисления в системах компьютерной математики, Аналитические методы исследования геометрических объектов, Вводный курс математики, Векторно-координатный метод решения геометрических задач, Визуализация и анимация в 3D редакторах, Внеурочная деятельность учащихся по информатике, Воспитательная работа в обучении математике, Вычислительный эксперимент в свободных средах программирования, Геометрические и физические приложения определенного интеграла, Геометрия, Задачи с параметрами и методы их решения, Защита информации в компьютерных сетях, Имитационное моделирование, Интеграция алгебраического и геометрического методов в обучении математике, Интерактивные технологии обучения математике, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Исследовательская и проектная деятельность в обучении математике, Исследовательская и проектная деятельность учащихся по информатике, Исторический подход в обучении математике, Комбинаторные конструкции и производящие функции, Компетентностный подход в обучении математике, Компьютерная алгебра, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Криптографические основы безопасности, Математические методы обработки экспериментальных данных, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения учащихся нестандартным методам решения математических задач, Методика подготовки к государственной итоговой аттестации по математике, Методология методики обучения математике, Методы аксиоматического построения алгебраических систем, Методы решения задач государственной итоговой аттестации по математике, Методы решения задач по информатике, Методы решения трансцендентных уравнений, неравенств и их систем, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Общая теория линейных операторов и ее приложение к решению геометрических задач, Оптимизация и продвижение сайтов, Особенности подготовки к единому государственному экзамену по математике на базовом уровне, Практикум по информационным технологиям, , Применение систем динамической математики в образовании, Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка интерактивного учебного контента, Разработка приложений в MicrosoftVisualStudio, Разработка электронных образовательных ресурсов и методика их оценки, Реализация

прикладной направленности в обучении математике, Решение геометрических задач средствами компьютерного моделирования, Решение задач основного государственного экзамена по математике, Решение задач по криптографии, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение задач повышенного уровня сложности по теории вероятностей, Решениеолимпиадных задач по информатике, Решение прикладных задач информатики, Свободное программное обеспечение в образовании, Свободные инструментальные системы, Системы компьютерной математики, Современные технологии в обучении математике, Современный урок информатики, Современный урок математики, Теоретические основы информатики, Технологии дополненной и виртуальной реальности, Технологии разработки мобильных приложений, Технологический подход в обучении математике, Технология обучения математическим доказательствам в школе, Технология обучения учащихся решению математических задач, Технология работы с теоремой в обучении математике, Технология разработки и методика проведения элективных курсов по математике, Технология укрупнения дидактических единиц в обучении математике, Формы и методы работы с одаренными детьми, Численные методы, Экстремальные задачи в школьном курсе математики, Элементарная математика, Элементы конструктивной геометрии в школьном курсе математики, Элементы математического анализа в комплексной области, Элементы функционального анализа.

Компетенция ПК-3 формируется в процессе изучения дисциплин:

Защита информации в компьютерных сетях, Информационная безопасность в образовании, История математики, Криптографические основы безопасности, Основы вожатской деятельности, Педагогическая практика, Практика по получению профессиональных умений и опыта профессиональной деятельности, Преддипломная практика, Профессиональная компетентность классного руководителя, Решение задач по криптографии

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания; умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Уровень	Шкала оценивания для промежуточной	Шкала оценивания

сформированности компетенции	аттестации	по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	Не зачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Студент знает историю криптографии, владеет навыками решения задач по криптографиии, а также навыками криптографической защиты информации на компьютере.
Незачтено	Студент не знает основного материала дисциплины “Решение задач по криптографии".

8.3. Вопросы, задания текущего контроля

Модуль 1: Теоретические основы криптографической защиты информации

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Можно ли включить углубленное изучение криптографии в программу факультативных занятий средней общеобразовательной школы?

2. Изучите вопрос изучения криптографии в образовании.

3. Изучите способы кодирования информации, используемые в криптографии.

Модуль 2: Практические вопросы криптографической защиты информации

ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

1. Как можно модернизировать содержание криптографии в школьном курсе информатики?

2. Изучите программные средства для организации криптографической защиты.

3. Изучите онлайн-сервисы, которые можно использовать шифрования данных.

Модуль 3:Принципы построения криптографических алгоритмов.

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Расскажите об аппаратной реализации криптографических алгоритмов.

2. Расскажите о различии между программными и аппаратными реализациями криптографических алгоритмов.

3. Расскажите о криптографических параметрах узлов и блоков шифраторов.

4. Расскажите о синтезе шифров.

5. Расскажите об особенностях использования вычислительной техники в криптографии.

Модуль 4. Криптографические стандарты и протоколы.

ПК-3 способностью решать задачи воспитания и духовно-нравственного развития, обучающихся в учебной и внеучебной деятельности

1. Расскажите об управлении криптографическими ключами в асимметрической криптосистеме.

2. Расскажите об управлении криптографическими ключами: генерация, хранение и распределение ключей

3. Алгоритм открытого распределения ключей Диффи-Хеллмана. Особенности шифрования.

4. Расскажите об алгоритме построения цифрового дайджеста MD5.

8.4. Вопросы промежуточной аттестации

Шестой семестр (Зачет, ПК-1, ПК-3)

1. Расскажите об истории развития криптографии. Объясните подходы к защите информации. Расскажите о зарождении криптографии.

2. Расскажите о криптографии в Новое время. Расскажите об истории тайнописи в России. Расскажите о криптография в XX веке. Расскажите о развитии математики и криптографии.

3. Расскажите о криптографии, её целях и задачах. Расскажите о стенографии.

4. Расскажите о процессе шифрования данных и дешифрования. Укажите основные проблемы шифрования. Расскажите о современных шифрах.

5. Расскажите об алгебраические и вероятностные модели шифров. Модели шифров замены с ограничениями и неограниченным ключом.

6. Расскажите о теоретико-автоматной модели шифратора.

7. Расскажите о классификации угроз и атак. Расскажите о теоретико-информационном подходе к оценке криптостойкости шифров.

8. Расскажите о математических проблемах, лежащие в основе систем с открытым ключом.

9. Расскажите о шифре Цезаря.

10. Расскажите о шифре Вижинера.

11. Расскажите о шифре подстановки.

12. Расскажите о блочных системах шифрования. Расскажите о сети Фейстеля.

13. Расскажите о стандарте шифрования DES.

14. Расскажите об алгоритме шифрования RSA.

15. Расскажите о российском стандарте шифрования ГОСТ 28147-89. Стандарт AES.

16. Расскажите о поточных системах шифрования.Поясните, что такое гаммирование. Расскажите о синхронных и поточных шифрах.

17. Расскажите о композициях шифров и использовании данного элемента в шифровании. Приведите примеры.

18. Расскажите о системах шифрования с открытым ключом.

19. Расскажите о системах шифрования с закрытым ключом.

20. Расскажите о симметричные системы шифрования.

21. Расскажите об ассиметричных системах шифрования.

22. Расскажите о криптографической стойкости шифров.

23. Расскажите о принципах построения криптографических алгоритмов.

24. Расскажите о программной реализации криптографических алгоритмов.

25. Расскажите об аппаратной реализации криптографических алгоритмов.

26. Расскажите о различии между программными и аппаратными реализациями криптографических алгоритмов.

27. Расскажите о криптографических параметрах узлов и блоков шифраторов.

28. Расскажите о синтезе шифров.

29. Расскажите об особенностях использования вычислительной техники в криптографии.

30. Расскажите о криптографических хэш-функциях.

31. Расскажите об электронной цифровой подписи.

32. Расскажите об основных методах построения схем ЭЦП.

33. Расскажите об алгоритме Эль-Гамаля

34. Расскажите об аутентификации пользователей в корпоративных сетях.

35. Расскажите об управлении криптографическими ключами в асимметрической криптосистеме.

36. Расскажите об управлении криптографическими ключами: генерация, хранение и распределение ключей

37. Алгоритм открытого распределения ключей Диффи-Хеллмана. Особенности шифрования.

38. Расскажите об алгоритме построения цифрового дайджеста MD5.

8.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме зачета.

Зачетпозволяет оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

Устный ответ на зачете:

Для оценки сформированности компетенции посредством устного ответа студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по изучаемой проблеме;

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Басалова, Г. В. Основы криптографии [Электронный ресурс] : курс лекций / Г.В. Басалова ; Национальный Открытый Университет «ИНТУИТ». – Москва : Интернет-Университет Информационных Технологий, 2011. – 253 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=233689.

2. Котова, Л. В. Сборник задач по дисциплине «Методы и средства защиты информации» [Электронный ресурс] : учебное пособие / Л. В. Котова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский педагогический государственный университет». – Москва : МПГУ, 2015. – 44 с. – Режим доступа :http://biblioclub.ru/index.php?page=book&id=469877

3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040

Дополнительная литература

1. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование : [16+] / А.В. Аграновский, Р.А. Хади. – Москва : СОЛОН-ПРЕСС, 2009. – 256 с. – (Аспекты защиты). – URL: http://biblioclub.ru/index.php?page=book&id=117663. – ISBN 5-98003-002-6. – Текст : электронный.

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях :

учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – URL: http://biblioclub.ru/index.php?page=book&id=480637. – Библиогр. в кн. – Текст : электронный.

3. Майстренко, Н.В. Основы теории информации и криптографии: учебное электронное издание / Н.В. Майстренко, А.В. Майстренко ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – URL: http://biblioclub.ru/index.php?page=book&id=570354. – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.securitylab.ru - Security Lab by Positive Technologies [Электронныйресурс] . – URL: http://www.securitylab.ru

2. http://www.intuit.ru - Интернет-Университет Информационных Технологий [Электронный ресурс] / Бесплатные учебные курсы по информационным технологиям. – М. : НОУ «ИНТУИТ». - URL: http://www.intuit.ru

3. http://all-ib.ru - Информационная безопасность. Защита информации

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;

– конкретизировать для себя план изучения материала;

– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:

– проработайте каждую тему по предлагаемому ниже алгоритму действий;

– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к сдаче зачета.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– выпишите в тетрадь основные категории и персоналии по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к зачету;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на лабораторном занятии;

–выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам на карточках, что поможет при подготовке рефератов, текстов речей, при подготовке к зачету;

– выберите те источники, которые наиболее подходят для изучения конкретной темы.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для

использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. MicrosoftWindows 7 Pro
2. MicrosoftOfficeProfessionalPlus 2010
3. 1С: Университет ПРОФ

12.2 Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Информационно-правовая система «ГАРАНТ» (http://www.garant.ru)
2. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata/)
2. Электронная библиотечная система Znanium.com(http://znanium.com/)
3. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Оснащение аудиторий

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ).

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь), интерактивный дисплей.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 13 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы(№225, главный учебный корпус).

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы

Читальный зал электронных ресурсов № 101б.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета: автоматизированные рабочие места (компьютер – 12 шт.).

Мультимедийный проектор, многофункциональное устройство, принтер.

Учебно-наглядные пособия:

Презентации, электронные диски с учебными и учебно-методическими пособиями.