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

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯПРОГРАММАДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании

Форма обучения: Очная

Разработчик: Жаркова Ю.С., канд. физ.-мат.. наук, доцент кафедры информатики и вычислительной техники

Программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной техники, протокол № 3 от 21.10.2021 года

Зав. кафедрой  Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – формирование умений проектировать индивидуальные образовательные маршруты обучающихся в области защиты информации в компьютерных системах при помощи программно-аппаратных средств.

Задачи дисциплины:

- ознакомление со стандартами, методическими и нормативными материалами, которые определяют проектирование и разработку объектов профессиональной деятельности;
- изучение моделей, методов и форм организации процесса разработки объектов профессиональной деятельности;
- изучение методов и средств анализа и моделирования объектов профессиональной деятельности и их компонентов;
- проектирование цели своего профессионального и личностного развития.

В том числе воспитательные задачи:

- формирование мировоззрения и системы базовых ценностей личности;
- формирование основ профессиональной культуры обучающегося в условиях трансформации области профессиональной деятельности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.06.23 «Программно-аппаратные средства защиты информации» относится к обязательной части учебного плана.

Дисциплина изучается на 2 курсе, в 3 и 4 семестрах.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет.

Изучению дисциплины «Программно-аппаратные средства защиты информации» предшествует освоение дисциплин (практик):

ИКТ и медиаграмотность;

Основы информационной безопасности.

Освоение дисциплины «Программно-аппаратные средства защиты информации» является необходимой основой для последующего изучения дисциплин (практик):

Безопасность образовательных Интернет-систем;

Архитектура ЭВМ, системное и прикладное обеспечение;

Безопасность информационных систем и баз данных.

Область профессиональной деятельности, на которую ориентирует дисциплина «Программно-аппаратные средства защиты информации», включает:

01 Образование и наука (в сфере дошкольного, начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования).

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 следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
ПК-7. Способен проектировать индивидуальные образовательные маршруты обучающихся по преподаваемым учебным предметам.	

педагогическая деятельность

ПК-7.1. Разрабатывает индивидуально-ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.	знать: - состав и классификацию защищаемой информации с помощью программно-аппаратных средств; уметь: - определять структуру индивидуально-ориентированных материалов в области использования аппаратного и программного обеспечения определенного класса для решений служебных задач; владеть: - навыками разработки программно-аппаратных средств защиты информации.
ПК-8. Способен проектировать траектории своего профессионального роста и личностного развития.	

педагогическая деятельность

ПК-8.1. Проектирует цели своего профессионального и личностного развития.	знать: - принципы построения программно-аппаратных средств защиты информации; уметь: - проектировать цели своего профессионального и личностного развития в области программно-аппаратных средств защиты информации; владеть: - навыками использования программно-аппаратных средств защиты информации.
ПК-8.3. Разрабатывает программы профессионального и личностного роста.	знать: - аппаратно-программные средства диагностики систем защиты информации. уметь: - разрабатывать программы профессионального и личностного роста для применения современные программно-аппаратные системы защиты информации; владеть: - навыками разработки и использования программно-аппаратных средств защиты информации.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	3 семестр	4 семестр
Контактная работа (всего)	**68**	**36**	**32**
Лекции	34	18	16
Лабораторные	34	18	16
Самостоятельная работа (всего)	**38**	**16**	**22**
Виды промежуточной аттестации			
Экзамен	38	20	18
Общая трудоемкость часы	**144**	**72**	**72**
Общая трудоемкость зачетные единицы	**4**	**2**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Современные требования к программно-аппаратным средствам обеспечения информационной безопасности (10 ч.)

История развития средств защиты информации. Программные и аппаратные механизмы защиты. Программно-аппаратные средства идентификации и аутентификации пользователей. Типовые схемы хранения ключевой информации. Стандарты и рекомендации в области информационной безопасности.

Раздел 2. Нормативно-правовой аспект создания и использования средств защиты информации (8 ч.)

Технические требования стандартов к программно- аппаратным средствам защиты информации. Политика безопасности организации. Эффективная защита информации при учете характеристик среды ее обработки и хранения. Лицензирование программно-аппаратных средств защиты информации.

Раздел 3. Комплексы программно-аппаратных средств обеспечения информационной безопасности (8 ч.)

Многоуровневые схемы управления доступом. Технические устройства идентификации и аутентификации. Идентификация и аутентификация пользователей с помощью биометрических устройств. Модульная архитектура технических средств защиты ПО от несанкционированного копирования.

Раздел 4. Принципы технологии создания безопасного программного обеспечения (8 ч.)

Защита программ с помощью электронных ключей. Механизм защиты структурного кода. Защита программного обеспечения от исследования. Защита от разрушающих программных воздействий.

5.2. Содержание дисциплины:

3 семестр. Лекции (18 ч.)

Раздел 1. Современные требования к программно-аппаратным средствам обеспечения информационной безопасности (10 ч.)

Тема 1. История развития средств защиты информации (2 ч.).

История развития средств защиты информации. Этапы становления средств защиты информации.

Тема 2. Программные и аппаратные механизмы защиты (2 ч.).

Основные принципы и механизмы защиты программного обеспечения. Обзор нескольких существующих решений для автоматизации процесса защиты.

Тема 3. Программно-аппаратные средства идентификации и аутентификации пользователей (2 ч.).

Основные понятия, концепции идентификации и аутентификации. Идентификация пользователей компьютерных сетевых технологий и подтверждение санкционированности пользователей (методы подтверждения подлинности пользователя в сетевых структурах и системах удаленного доступа к компьютерным ресурсам). Методы взаимной проверки подлинности пользователей в компьютерных технологиях. Методы идентификации пользователей в сетевых компьютерных системах с нулевой передачей знаний.

Тема 4. Типовые схемы хранения ключевой информации (2 ч.).

Типовые схемы хранения ключевой информации в открытых компьютерных системах. Угрозы базы данных аутентификации в КС.

Тема 5. Стандарты и рекомендации в области информационной безопасности (2 ч.).

Основополагающие документы в области информационной безопасности: Оранжевая книга (TCSEC), Радужная серия, Гармонизированные критерии Европейских стран (ITSEC),

Рекомендации X.800, Концепция защиты от НСД Гостехкомиссии при Президенте РФ.

Раздел 2. Нормативно-правовой аспект создания и использования средств защиты информации (8 ч.)

Тема 6. Технические требования стандартов к программно- аппаратным средствам защиты информации (2 ч.).

Международный стандарт критериев оценки безопасности информационных технологий и ГОСТ Р ИСО/МЭК 15408-2002.

Тема 7. Политика безопасности организации (2 ч.).

Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления. Классификация политик безопасности. Формальные и неформальные политики безопасности.

Тема 8. Эффективная защита информации при учете характеристик среды ее обработки и хранения (2 ч.).

Эффективная защита информации при учете характеристик среды ее обработки и хранения. Международный стандарт по критериям оценки безопасности информационных технологий.

Тема 9. Лицензирование программно-аппаратных средств защиты информации (2 ч.).

Лицензирование всех видов деятельности в области связи, использования ЭЦП и шифровальных средств. Интеллектуальная собственность под защитой закона. Законодательство Российской Федерации о коммерческой тайне.

4 семестр. Лекции (16 ч.)

Раздел 3. Комплексы программно-аппаратных средств обеспечения информационной безопасности (8 ч.)

Тема 10. Многоуровневые схемы управления доступом (2 ч.).

Аппаратное средство – электротехническое, электронное или радиоэлектронное изделие. Пластиковые карты – характерный пример аппаратных средств. Многоуровневые схемы управления доступом. Два типа аутентификации: статическая и динамическая. Идентификационные карты.

Тема 11. Технические устройства идентификации и аутентификации (2 ч.).

Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Карточки с незащищенной памятью. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах.

Тема 12. Идентификация и аутентификация пользователей с помощью биометрических устройств (2 ч.).

Обзор биометрических методов аутентификации. Архитектура биометрических устройств. Статические методы: аутентификация по отпечатку пальца, по радужной оболочке глаза, по сетчатке глаза, по геометрии руки и лица, по термограмме лица. Динамические методы: аутентификация по голосу, аутентификация по рукописному почерку. Комбинированная биометрическая система аутентификации.

Тема 13. Модульная архитектура технических средств защиты ПО от несанкционированного копирования (2 ч.).

Технические меры защиты. Защита аудио треков. Защита аудио компакт-дисков. Защита программного обеспечения. Методы обхода технических мер защиты от

копирования.

Раздел 4. Принципы технологии создания безопасного программного обеспечения (8 ч.)

Тема 14. Защита программ с помощью электронных ключей (2 ч.).

Защита ПО с помощью электронного ключа: комплект разработчика ПО, технология защиты. Защита с помощью автоматических средств. Реализация защиты с помощью функций API. Обход защиты. Эмуляция ключа. Взлом программного модуля

Тема 15. Механизм защиты структурного кода (2 ч.).

Общая характеристика механизма защиты структурного кода. Шаблоны доступа к электронному ключу.

Тема 16. Защита программного обеспечения от исследования (2 ч.).

Локальная программная защита. Сетевая программная защита. Защита при помощи компакт-дисков. Защита при помощи электронных ключей. Привязка к параметрам компьютера и активация. Защита программ от копирования путём переноса их в онлайн. Защита кода от анализа. Защита программного обеспечения на мобильных платформах.

Тема 17. Защита от разрушающих программных воздействий (2 ч.).

Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Классификация и методы внедрения программных закладок.

3 семестр. Лабораторные (18 ч.)

Раздел 1. Современные требования к программно-аппаратным средствам обеспечения информационной безопасности (10 ч.)

Тема 1. Введение в проблематику программно-аппаратных средств защиты информации (2 ч.).

Анализ требований государственных стандартов применения программно-аппаратных средств защиты информации.

Тема 2. Основные принципы и механизмы защиты программного обеспечения (2 ч.).

Изучение принципов требования к программно-аппаратным средствам обеспечения информационной безопасности.

Тема 3. Программно-аппаратные средства идентификации и аутентификации пользователей (2 ч.).

Методы подтверждения подлинности пользователя в сетевых структурах и системах удаленного доступа к компьютерным ресурсам. Методы взаимной проверки подлинности пользователей в компьютерных технологиях. Методы идентификации пользователей в сетевых компьютерных системах с нулевой передачей знаний.

Тема 4. Схемы хранения ключевой информации (2 ч.).

Типовые схемы хранения ключевой информации в открытых компьютерных системах. Угрозы базы данных аутентификации в КС.

Тема 5. Стандарты и рекомендации в области информационной безопасности (2 ч.).

Изучение основополагающих документов в области информационной безопасности: Радужная серия, Гармонизированные критерии Европейских стран (ITSEC), Рекомендации X.800.

Раздел 2. Нормативно-правовой аспект создания и использования средств защиты информации (8 ч.)

Тема 6. Технические требования стандартов к программно- аппаратным средствам защиты информации (2 ч.).

Правовая и организационная основы электронной цифровой подписи в Российской Федерации.

Тема 7. Политика безопасности организации (2 ч.).

Классификация политик безопасности. Формальные и неформальные политики безопасности.

Тема 8. Международный стандарт по критериям оценки безопасности информационных технологий (2 ч.).

Эффективная защита информации при учете характеристик среды ее обработки и хранения.

Тема 9. Лицензирование программно-аппаратных средств защиты информации (2 ч.).

Лицензирование всех видов деятельности в области связи, использования ЭЦП и шифровальных средств. Интеллектуальная собственность под защитой закона. Законодательство Российской Федерации о коммерческой тайне.

4 семестр. Лабораторные (16 ч.)

Раздел 3. Комплексы программно-аппаратных средств обеспечения информационной безопасности (8 ч.)

Тема 10. Многоуровневые схемы управления доступом (2 ч.).

Два типа аутентификации: статическая и динамическая. Идентификационные карты. Аппаратное средство – электротехническое, электронное или радиоэлектронное изделие. Пластиковые карты – характерный пример аппаратных средств. Многоуровневые схемы управления доступом.

Тема 11. Технические устройства идентификации и аутентификации (2 ч.).

Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Карточки с незащищенной памятью. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах.

Тема 12. Идентификация и аутентификация пользователей с помощью биометрических устройств (2 ч.).

Обзор биометрических методов аутентификации. Архитектура биометрических устройств. Статические методы: аутентификация по отпечатку пальца, по радужной оболочке глаза, по сетчатке глаза, по геометрии руки и лица, по термограмме лица. Динамические методы: аутентификация по голосу, аутентификация по рукописному почерку. Комбинированная биометрическая система аутентификации.

Тема 13. Модульная архитектура технических средств защиты ПО от несанкционированного копирования (2 ч.).

Технические меры защиты. Защита аудио треков. Защита аудио компакт-дисков. Защита программного обеспечения. Методы обхода технических мер защиты от копирования.

Раздел 4. Принципы технологии создания безопасного программного обеспечения (8 ч.)

Тема 14. Защита программ с помощью электронных ключей (2 ч.).

Защита ПО с помощью электронного ключа: комплект разработчика ПО, технология защиты. Защита с помощью автоматических средств. Реализация защиты с помощью функций API. Обход защиты. Эмуляция ключа. Взлом программного модуля

Тема 15. Механизм защиты структурного кода (2 ч.).

Общая характеристика механизма защиты структурного кода. Шаблоны доступа к электронному ключу.

Тема 16. Защита программного обеспечения от исследования (2 ч.).

Локальная программная защита. Сетевая программная защита. Защита при помощи компакт-дисков. Защита при помощи электронных ключей. Привязка к параметрам компьютера и активация. Защита программ от копирования путём переноса их в онлайн. Защита кода от анализа. Защита программного обеспечения на мобильных платформах.

Тема 17. Защита от разрушающих программных воздействий (2 ч.).

Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Классификация и методы внедрения программных закладок.

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

6.1 Вопросы и задания для самостоятельной работы

Третий семестр (16 ч.)

Раздел 1. Современные требования к программно-аппаратным средствам обеспечения информационной безопасности (8 ч.)

Вид СРС: индивидуальные задания

1.Составить план-конспект по истории микропроцессоров.

2.Составить классификацию требования к программно-аппаратным средствам обеспечения информационной безопасности.

Раздел 2. Нормативно-правовой аспект создания и использования средств защиты информации (8 ч.)

Вид СРС: индивидуальные задания

1.Сделать анализ нормативно-правовых аспектов создания и использования средств защиты информации.

2.Составить план-конспект по аппаратным средствам информационной безопасности.

3.Составить план-конспект по программным средствам информационной безопасности.

Четвертый семестр (22 ч.)

Раздел 3. Комплексы программно-аппаратных средств обеспечения информационной безопасности (12 ч.)

Вид СРС: индивидуальные задания

1.Составить схему использования программных средств.

2.Разработать инструкцию по использованию любого комплекса программно-аппаратных средств обеспечения информационной безопасности.

3.Составить классификацию требования к специфическим средствам защиты информации.

Раздел 4. Принципы технологии создания безопасного программного обеспечения (10 ч.)

Вид СРС: индивидуальные задания

1.Описать принципы технологии создания безопасного программного обеспечения

2.Составление плана-конспекта расчета экономических средств информационной

безопасности.

7. Тематика курсовых работ (проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства

8.1 Компетенции и этапы формирования

№ п/п	Оценочные средства	Компетенции, этапы их формирования
1.	Предметно-методический модуль	ПК-7, ПК-8

8.2 Показатели и критерии оценивания компетенций, шкалы оценивания

Шкала, критерии оценивания и уровень сформированности компетенции			
2 (не зачтено) ниже порогового	3 (зачтено) пороговый	4 (зачтено) базовый	5 (зачтено) повышенный
ПК-7. Способен проектировать индивидуальные образовательные маршруты обучающихся по преподаваемым учебным предметам.			
ПК-7.1. Разрабатывает индивидуально- ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.			
Не способен разрабатывать индивидуально-ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.	В целом успешно, нобессистемно разрабатывает индивидуально-ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.	В целом успешно, нос отдельными недочетами разрабатывает индивидуально-ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.	Способен в полном объеме разрабатывать индивидуально-ориентированные материалы к учебным предметам с учетом особенностей обучающихся, их образовательных потребностей.
ПК-8. Способен проектировать траектории своего профессионального роста и личностного развития.			
ПК-8.1. Проектирует цели своего профессионального и личностного развития.			
Не способен проектировать цели своего профессионального и личностного развития.	В целом успешно, но бессистемно проектирует цели своего профессионального и личностного развития.	В целом успешно, но с отдельными недочетами проектирует цели своего профессионального и личностного развития.	Способен в полном объеме проектировать цели своего профессионального и личностного развития.
ПК-8.3. Разрабатывает программы профессионального и личностного роста.			

Не способен разрабатывать программы профессионального и личностного роста.	В целом успешно, но бессистемно разрабатывает программы профессионального и личностного роста.	В целом успешно, но с отдельными недочетами разрабатывает программы профессионального и личностного роста.	Способен в полном объеме разрабатывать программы профессионального и личностного роста.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен	
Повышенный	5 (отлично)	90 – 100%
Базовый	4 (хорошо)	76 – 89%
Пороговый	3 (удовлетворительно)	60 – 75%
Ниже порогового	2 (неудовлетворительно)	Ниже 60%

8.3 Вопросы промежуточной аттестации

Третий семестр (Экзамен, ПК-7.1, ПК-8.1, ПК -8.3)

1. Дать определение понятия «Информационная безопасность». Основные методологические и нормативно-правовые документы по информационной безопасности.
2. Привести основные понятия по защите компьютерных данных – доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.
3. Охарактеризовать основные виды угроз безопасности компьютерных систем, угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
4. Привести структурные составляющие гипотетической модели нарушителя, преднамеренные потенциальные угрозы. Привести классификацию каналов несанкционированного доступа.
5. Описать наиболее распространенные способы несанкционированного доступа в компьютерных технологиях – перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.
6. Описать основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.
7. Описать политику безопасности, охарактеризовать вды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.
8. Описать этапы построения системы защиты автоматизированных информационных систем, привести составляющие отдельных этапов.
9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.
10. Описать способы идентификации и проверки подлинности электронных документов и пользователей компьютерных технологий.
11. Описать способы идентификации и механизмы подтверждения подлинности пользователя, взаимной проверки подлинности пользователей.
12. Охарактеризовать управление криптографическими ключами, генерацию и хранение ключей.

13. Привести иерархию ключей шифрования данных в корпоративных компьютерных системах.

14. Описать механизм запроса – ответа в сетевых технологиях, механизм отметки времени.

15. Описать схему защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.

16. Охарактеризовать программные методы защиты сетевых технологий в Internet структурах.

17. Описать способы защиты данных в электронных платежных системах.

18. Сформулировать принципы функционирования электронных платежных систем.

19. Описать персональный идентификационный номер (PIN). Сформулировать принципы обеспечения безопасности электронно-платежной системы POS (Point-of-Sale), схемы функционирования POS.

20. Охарактеризовать принципы обеспечения безопасности электронных платежей через сеть Internet.

21. Описать протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transac-tions), способы использования сертификатов.

22. Охарактеризовать отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

23. Охарактеризовать средства и системы управления контролем доступа в компьютерных технологиях.

24. Описать основные подходы к защите данных от несанкционированного доступа – шифрование, контроль доступа, разграничения доступа к файлам.

25. Описать способы защиты программного продукта от несанкционированного копирования.

26. Охарактеризовать несанкционированное копирование программ как тип НСД.

27. Привести юридические аспекты несанкционированного копирования программ, описать общее понятие защиты от копирования.

28. Описать разновидности задач защиты от копирования. Сформулировать подходы к задаче защиты от копирования.

29. Описать способ привязки ПО к аппаратному окружению и физическим носителям как средство защиты от копирования.

30. Описать способ привязки к внешним (добавляемым) элементам ЭВМ, привязки к портовым ключам.

31. Охарактеризовать методы «водяных знаков» и методы «отпечатков пальцев».

32. Охарактеризовать способы защиты программного продукта от изучения.

33. Описать понятие обратного проектирования программного обеспечения, способы изучения программного обеспечения (статическое и динамическое изучение).

34. Описать задачи защиты программного продукта от изучения и способы их решений: защита от отладки, динамическое преобразование кода,

35. Охарактеризовать вирусы как особый класс разрушающих программных воздействий, сформулировать необходимые и достаточные условия недопущения разрушающего воздействия.

Четвёртый семестр (Экзамен, ПК-7.1, ПК-8.1, ПК -8.3)

1. Охарактеризовать электронный документ (ЭД), описать понятие ЭД и типы ЭД.
2. Охарактеризовать виды информации, понятие исполняемого модуля.
3. Охарактеризовать уязвимость компьютерных систем. Описать понятия доступа, субъекта и объекта доступа.

4. Охарактеризовать понятие несанкционированного доступа (НСД), классы и виды НСД. Охарактеризовать несанкционированное копирование программ как особый вид НСД.

5. Охарактеризовать понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

6. Описать политику безопасности в компьютерных системах, оценку защищенности.

7. Охарактеризовать способы защиты конфиденциальности, целостности и доступности в КС.

8. Описать руководящие документы Гостехкомиссии по оценке защищенности от НСД.

9. Описать понятие идентификации пользователя, сформулировать задачу идентификации пользователя. Описать понятие протокола идентификации, локальной и удаленной идентификации, идентифицирующей информации (понятие, способы хранения, связь с ключевыми системами).

10. Привести основные подходы к защите данных от НСД – шифрование, контроль доступа, разграничение доступа.

11. Охарактеризовать файл как объект доступа. Привести оценку надежности систем ограничения доступа – сведение к задаче оценки стойкости.

12. Описать схему организации доступа к файлам, иерархический доступ к файлам. Охарактеризовать понятие атрибутов доступа. Сформулировать принципы организации доступа к файлам различных ОС.

13. Охарактеризовать защиту сетевого файлового ресурса на примерах организации доступа в различных ОС.

14. Описать способы фиксации факторов доступа – журналы доступа и критерии их информативности.

15. Классифицировать принципы выявления следов несанкционированного доступа к файлам, метод инициированного НСД.

16. Описать доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).

17. Описать понятие и примеры скрытого доступа, охарактеризовать надежность систем ограничения доступа.

18. Описать принципы защиты массивов информации от изменения (имитозащиты). Привести криптографическую постановку защиты от изменения данных. Описать подходы к решению задачи защиты данных от изменения.

19. Охарактеризовать схему защиты от разрушающих программных воздействий. Классифицировать вирусы как особый класс разрушающих программных воздействий. Сформулировать необходимые и достаточные условия недопущения разрушающего воздействия. Описать понятие изолированной программной среды.

20. Охарактеризовать схему построения программно-аппаратных комплексов шифрования.

21. Охарактеризовать аппаратные и программно-аппаратные средства криптозащиты данных – построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.

22. Охарактеризовать схему защиты алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

23. Сформулировать необходимые и достаточные функции аппаратного средства криптозащиты. Описать проектирование модулей криптопреобразований на основе сигнальных процессов.

24. Привести классификацию защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.

25. Описать процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей, механизмы расширения BIOS, привести преимущества и недостатки программных и аппаратных средств.

26. Охарактеризовать способы защиты информации на съемных дисках. Описать

организацию прозрачного режима шифрования.

27. Охарактеризовать надежность средств защиты компонент. Описать понятие временной и гарантированной надежности.

28. Описать несанкционированное копирование программ. Привести юридические аспекты несанкционированного копирования программ.

29. Привести схему защиты программ от несанкционированного копирования (общее понятие защиты от копирования). Описать разновидности задач защиты от копирования.

30. Охарактеризовать привязку ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

31. Охарактеризовать привязку программ к гибким машинным дискам (ГМД). Описать структуру данных на ГМД, схему управление контроллером ГМД.

32. Описать способы создания некопируемых меток, точное измерение характеристик форматирования дорожки, технологию «слабых битов».

33. Охарактеризовать способы привязки программ к жестким магнитным дискам (ЖМД), особенности привязки к ЖМД. Описать виды меток на ЖМД.

35. Привести классификацию средств хранения ключей и идентифицирующей информации.

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

Промежуточная аттестация проводится в форме экзамена.

Экзамен позволяет оценить сформированность универсальных и общепрофессиональных 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 в области медиаобразования.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Устный ответ на экзамене

При определении уровня достижений студентов на экзамене необходимо обращать особое внимание на следующее:

- дан полный, развернутый ответ на поставленный вопрос;
- показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;
- знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;
- ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;
- теоретические постулаты подтверждаются примерами из практики.

Тестирование. При определении уровня достижений студентов с помощью тестового контроля ответ считается правильным, если:

– в тестовом задании закрытой формы с выбором ответа выбран правильный ответ;

– по вопросам, предусматривающим множественный выбор правильных ответов, выбраны все правильные ответы;

– в тестовом задании открытой формы дан правильный ответ;

– в тестовом задании на установление правильной последовательности установлена правильная последовательность;

– в тестовом задании на установление соответствия сопоставление произведено верно для всех пар.

При оценивании учитывается вес вопроса (максимальное количество баллов за правильный ответ устанавливается преподавателем в зависимости от сложности вопроса). Количество баллов за тест устанавливается посредством определения процентного соотношения набранного количества баллов к максимальному количеству баллов.

Критерии оценки

До 60% правильных ответов – оценка «неудовлетворительно».

От 60 до 75% правильных ответов – оценка «удовлетворительно».

От 75 до 90% правильных ответов – оценка «хорошо».

Свыше 90% правильных ответов – оценка «отлично».

Вопросы и задания для устного опроса

При определении уровня достижений студентов при устном ответе необходимо обращать особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– теоретические постулаты подтверждаются примерами из практики.

Оценка за опрос определяется простым суммированием баллов:

Критерии оценки ответа

Правильность ответа – 1 балл.

Всесторонность и глубина (полнота) ответа – 1 балл.

Наличие выводов – 1 балл.

Соблюдение норм литературной речи – 1 балл.

Владение профессиональной лексикой – 1 балл.

Итого: 5 баллов.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428605. – Текст : электронный.

2. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А. М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=480637. – Текст : электронный.

3. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. – 2-е изд., испр. М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=429035. – Текст : электронный.

Дополнительная литература

1. Авдошин, С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности: курс / С.М. Авдошин, А.А. Савельева, В.А. Сердюк ; Национальный Открытый Университет «ИНТУИТ». – Москва : Интернет-Университет

Информационных Технологий (ИНТУИТ), 2010. – 384 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=233684. – Текст : электронный.

2. Сагдеев, К. М. Физические основы защиты информации [Электронный ресурс] : учебноепособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2015. – 394 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=458285. – Текст : электронный.

3. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428820. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://all-ib.ru – Информационная безопасность. Защита информации
2. http://www.securrity.ru – SecuRRity.Ru – «Информационная безопасность компьютерных систем и защита конфиденциальных данных»
3. http://www.securitylab.ru – Security Lab by Positive Technologies

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 теоретическому материалу, а затем подругим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

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

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

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

– 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. 1С: Университет ПРОФ
2. Microsoft Windows 7 Pro
3. Microsoft Office Professional Plus 2010

12.2 Перечень информационных справочных систем (обновление выполняется еженедельно)

1 Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)

2 Информационно-правовая система «ГАРАНТ» http://www.garant.ru)

2.1 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и наукиРФ» (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, экспортинформации на цифровые носители.

Учебная аудитория для проведения учебных занятий.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 24 шт.).

Учебно-наглядные пособия:

Презентации.