Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
« 26 » марта 2019 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ»

Специальность: 11.05.01 Радиоэлектронные системы и комплексы

Специализация: Радиоэлектронная борьба

Уровень высшего образования: специалитет

Квалификация (степень) выпускника: инженер

Форма обучения: очная

Королев
2019

Автор: к.в.н., доцент Сухотерин А.И. Рабочая программа дисциплины «Методы и средства защиты информации в телекоммуникационных системах» . – Королев МО: «Технологический университет», 2019.

Рецензент: к.в.н., доцент Воронов А.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки специалистов 11.05.01 «Радиоэлектронные системы и комплексы» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 7 от 26.03.2019 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.	к.в.н., доцент Соляной В.Н.	к.в.н., доцент Соляной В.Н.	к.в.н., доцент Соляной В.Н.
Год утверждения (переутверждения)	2019	2020	2021	2022
Номер и дата протокола заседания кафедры	№8 от 18.03.19	№10 от 12.05.20	№12 от 11.06.21	№12 от 20.06.22

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)		
Год утверждения (переутверждения)	2023	
Номер и дата протокола заседания кафедры		

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Соляной В.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2019	2020	2021	2022	2023	
Номер и дата протокола заседания УМС	№6а от 26.03.19	№9 от 29.06.20	№7 от 15.06.21	№5от 21.06.22		

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, а также получение навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Профессиональные компетенции:

ПК-1. Разработка научно-технических проектов, проектирование и сопровождение РТС и РЭС изделий ракетно-космической техники

ПК-2. Эксплуатация радиоэлектронных систем

Основными **задачами** дисциплины являются:

- ознакомление обучаемых с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, разработка планов и программ проведения научных исследований и технических проектов, подготовка отдельных заданий для исполнителей и выполнение научных исследований по выбранной теме;
- формирование у обучаемых способности самостоятельно организовывать работу коллектива исполнителей, принятию управленческих решений в условиях спектра мнений, определению порядка выполнения работ;
- участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности, разработке проектов методических и нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ;
- формирование обучаемыми предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

После завершения освоения данной дисциплины студент должен:

Знать:

- ИД-1.1 $_{ПК-1}$. Руководящие. методические и нормативные технические документы по выпуску технической документации.
- ИД-1.2 $_{ПК-1}$.Порядок работы с персональной вычислительной техникой, файловой системой, форматы представления электронной графической и текстовой информации.
- ИД-1.1 $_{ПК-2}$. Виды и содержание эксплуатационных документов.
- ИД-1.2 $_{ПК-2.}$ Передовой отечественный и зарубежный опыт эксплуатации и технического обслуживания электронного оборудования.

Уметь:

- ИД-2.1.$_{ПК-1}$. Уметь разрабатывать материалы проектной конструкторской документации на РТС и РЭС.

- ИД-2.2. $_{ПК-1}$.Использовать программные приложения для поиска, обработки и анализа патентной и научно-технической информации, для работы в информационно-телекоммуникационной сети «Интернет», локальной сети.
- ИД-2.1. $_{ПК-2}$. Уметь организовывать рабочие места персонала, обслуживающего радиоэлектронные системы.
- ИД-2.2. $_{ПК-2}$. Уметь работать с эксплуатационной документацией по техническому обслуживанию радиоэлектронных систем.

Владеть:

- ИД-3.1. $_{ПК-1}$. Владеть навыками по организации совместной работы по проектированию РТС и РЭС со смежными подразделениями.
- ИД-3.2. $_{ПК-1}$. Разработка плана мероприятий или работы с организациями-исполнителями (соисполнителями) НИР.
- ИД-3.1. $_{ПК-2}$. Владеть организацией и осуществлением мероприятий по контролю соблюдения эксплуатационной документации по техническому обслуживанию радиоэлектронных систем.
- ИД-3.2. $_{ПК-2}$. Подготовка предложений по улучшению конструкции, эксплуатации, повышению надежности функционирования радиоэлектронных систем.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методы и средства защиты информации в телекоммуникационных системах» относится к части, формируемой участниками образовательных отношений, рабочего учебного плана основной образовательной программы подготовки студентов по специальности 11.05.01 Радиоэлектронные системы и комплексы (уровень специалитета).

Изучение данной дисциплины базируется на изученной ранее дисциплине: «Физика», и компетенциях: ОПК-4,6.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при выполнении выпускной квалификационной работы.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единиц, 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 10
Общая трудоемкость	**108**	**108**
Аудиторные занятия	**48**	**48**
Лекции (Л)	**16**	**16**
Практические занятия (ПЗ)	**32**	**32**
Лабораторные работы (ЛР)	**-**	**-**
Самостоятельная работа	**60**	**60**
КСР	**-**	**-**
Курсовые работы (проекты)	**-**	**-**
Расчетно-графические работы	**-**	**-**
Контрольная работа, домашнее задание	+	+
Текущий контроль знаний	**Тест**	**Тест**
Вид итогового контроля	**Зачет**	**Зачет**

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час. Очное	Код компетенций
Раздел 1. Концептуально-теоретические основы компьютерной безопасности					
Тема 1. Введение. Основные понятия теории компьютерной безопасности	**1**	**2**	**-**	**1**	**ПК-1,2**
Тема 2. Основные угрозы и уязвимости информационных	**1**	**2**	**-**	**1**	**ПК-1,2**

систем, возможные атаки на них					
Тема 3. Основные уровни защиты информации в компьютерных системах	**1**	**2**	**-**	**1**	**ПК-1,2**
Тема 4. Основные положения формальной теории защиты информации	**1**	**2**	**-**	**1**	**ПК-1,2**
Тема 5. Формальные модели безопасности	**2**	**4**	**-**	**1**	**ПК-1,2**
Тема 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	**2**	**4**	**-**	**1**	**ПК-1,2**
Тема 7. Построение систем защиты от угрозы нарушения кон-фиденциальности, целостности и доступности компьютерной информа-ции	**2**	**4**	**-**	**2**	**ПК-1,2**
Раздел 2. Прикладные основы теории компьютерной безопасности					
Тема 8. Методология обследования и проектирования защищенных информационных (автоматизированн ых) систем	**2**	**4**	**-**	**2**	**ПК-1,2**
Тема 9. Общие сведения о стандартах в области информационной безопасности	**2**	**4**	**-**	**2**	**ПК-1,2**
Тема 10. Концепция защиты СВТ и АС от НСД в	**2**	**4**	**-**	**2**	**ПК-1,2**

соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России					
Итого:	**16**	**32**	**-**	**14**	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы компьютерной безопасности

Тема 1. Введение. Основные понятия теории компьютерной безопасности

Введение. Место и роль дисциплины в процессе подготовки магистра, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература.

Актуальность проблемы обеспечения информационной безопасности (ИБ) в компьютерных системах. Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам). Основные термины и определения в области ИБ компьютерных систем и сетей.

Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Факты, свидетельствующие о способах злоупотребления информацией, циркулирующей в компьютерных системах.

Тема 2. Основные угрозы и уязвимости информационных систем, возможные атаки на них

Проблемы безопасности компьютерных систем (сетей). Основные угрозы и уязвимости информационных систем, возможные атаки на них. Виды и анализ угроз информационных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу информационных систем злоумышленников. Уязвимости ИС, возможные атаки на них. Базовые модели угроз для различных типов информационных систем. Особенности построения систем обнаружения атак (СОА) в ИС

Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.

Тема 3. Основные уровни защиты информации в компьютерных системах

Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы. Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.

Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.

Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников. Виды защищаемой компьютерной информации. Условия доступа к защищаемой информации со стороны злоумышленников.

Тема 4. Основные положения формальной теории защиты информации

Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.

Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.

Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.

Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.

Тема № 5. Формальные модели безопасности

Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое. Формальное описание системы в модели HRU. Поведение системы во времени. Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.

Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.

Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.

Тема № 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Тема № 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации. Организация защиты субъектов информационных отношений.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях. Циклический контрольный код как механизм обеспечения контроля целостности информации. Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.

Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.

Раздел 2. Прикладные основы теории компьютерной безопасности

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх». Иерархический метод построения защищённой АС («сверху вниз»). Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (TCB). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000). Цель создания АСЗИ.

Тема № 9. Общие сведения о стандартах в области информационной безопасности

Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем. Основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий (ИТ). Регламентация необходимости применения средств, механизмов, алгоритмов. Требования безопасности.

Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Набор требований к подсистемам защиты АС. Проверка соответствия требованиям по защите информации от НСД для АС. Показатели защищённости от НСД к информации в АС.

Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.

Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.

Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.

Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Категории пользователей. Среда безопасности. Задачи, решаемые при подготовке к оценке. Требования по безопасности. Каталоги требований безопасности. Общая модель безопасности. Недостатки «Общих критериев».

Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).

Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.

Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации. Определение НСД к информации. Два направления защиты от НСД. Особенности функций защиты в СВТ и АС. Основные способы НСД. Принципы защиты от НСД. Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Характеристики оценки технических средств защиты от НСД. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Защита информации в центрах обработки данных [Электронный ресурс]: учебное пособие / Ушаков И.А., Десницкий В.А., Чечулин А.А., Захарова Т.Е., Сахаров Д.В. - Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2019. - 92 с. URL: https://e.lanbook.com/book/180085.

2. Телекоммуникационные системы и сети. В 3 т. Т. 2. Радиосвязь, радиовещание, телевидение: учеб. пособие для вузов / [н/д]. - 3-е изд., стер. - М.: Горячая линия – Телеком, 2014. - 673: - ISBN 978-5-9912-0338-8. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/297882.

3. Быховский М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие спутниковых телекоммуникационных систем: учеб. пособие для вузов / Быховский М. А. - М.: Горячая линия – Телеком, 2014. - 441: - ISBN 978-5-9912-0405-7. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/297875.

4. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2015.

5. Васильков А.В., Васильков А.А., Васильков И. А. Информационные системы и их безопасность М.: ФОРУМ, 2011.

6. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.Технические средства и методы защиты информации. Учебное пособие для вузов.:-4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

7. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.

8. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7

Дополнительная литература:

1. Афанасьев А.А., Веденньев Л.Т. и др. Аутентификация.Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.
2. Малюк А.А. Теория защиты информации.-М.:Горячая линия-Телеком,2012.
3. Хорев П.Б. Программно-аппаратная защита информации. М.: ФОРУМ, 2009.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008. Москва, «ИД ФОРУМ – ИНФРА-М».
5. В.А. Тихонов В.В. Райх. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.
6. В.А. Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.
7. Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.
8. Шерстобитова В.Н. Передача данных в автоматизированных системах технологической подготовки производства: метод. указания к лаб. и самостоят. работам / Шерстобитова. - Оренбург: ГОУ ОГУ, 2004. - 21. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/213204.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://www.gov.ru** - сервер органов государственной власти Российской Федерации.
2. **http://www.minfin.ru** - официальный сайт Министерства финансов Российской Федерации.
3. http://www.biblioclub.ru
4. http://znanium.com

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды;
2. Рабочая программа и методическая обеспечение по дисциплине: «Методы и средства защиты информации в телекоммуникационных системах».

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Методы и средства защиты информации в телекоммуникационных системах».

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах академии с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ»

Специальность: 11.05.01 Радиоэлектронные системы и комплексы

Специализация: Радиоэлектронная борьба

Уровень высшего образования: специалитет

Квалификация (степень) выпускника: инженер

Форма обучения: очная

Королев
2019

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ПК-1	Разработка научно-технических проектов, проектирование и сопровождение РТС и РЭС изделий ракетно-космической техники	Темы 1-10	ИД-1.1 ПК-1. Руководящие. методические и нормативные технические документы по выпуску технической документации. ИД-1.2 ПК-1.Порядок работы с персональной вычислительной техникой, файловой системой, форматы представления электронной графической и текстовой информации.	ИД-2.1.ПК-1. Уметь разрабатывать материалы проектной конструкторской документации на РТС и РЭС. ИД-2.2. ПК-1.Использовать программные приложения для поиска, обработки и анализа патентной и научно-технической информации, для работы в информационно-телекоммуникационной сети «Интернет», локальной сети.	ИД-3.1. ПК-1. Владеть навыками по организации совместной работы по проектированию РТС и РЭС со смежными подразделениями. ИД-3.2. ПК-1. Разработка плана мероприятий или работы с организациями-исполнителями (соисполнителями) НИР.
2.	ПК-2	Эксплуатация радиоэлектронных систем	Темы 1-10	ИД-1.1 ПК-2. Виды и содержание эксплуатационных	ИД-2.1. ПК-2. Уметь организовывать рабочие места	ИД-3.1. ПК-2. Владеть организацией и осуществлением мероприятий по

				документов. ИД-1.2 ПК-2. Передовой отечественный и зарубежный опыт эксплуатации и технического обслуживания электронного оборудования.	персонала, обслуживающего радиоэлектронные системы. ИД-2.2. ПК-2. Уметь работать с эксплуатационной документацией по техническому обслуживанию радиоэлектронных систем.	контролю соблюдения эксплуатационной документации по техническому обслуживанию радиоэлектронных систем. ИД-3.2. ПК-2. Подготовка предложений по улучшению конструкции, эксплуатации, повышению надежности функционирования радиоэлектронных систем.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ПК-1,2	Тест	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: •компетенция освоена на продвинутом уровне – 4 балла; •компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не освоена) – 2 и менее баллов	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы, выносимые на тестирование

ПК-1: Разработка научно-технических проектов, проектирование и сопровождение РТС и РЭС изделий ракетно-космической техники
ПК-2: Эксплуатация радиоэлектронных систем

Вопросы закрытого типа

Пассивная атака доступа реализуется путем
(!)прослушивания информации, проходящей по сети
(?)подмены адреса передаваемого кадра
(?)перенаправления трафика к сниферу

Согласно стандарту IS0/IEC 27002, информационная безопасность — это:
Выберите все правильные ответы (один или несколько)
(!)обеспечение целостности информации
(?)внедрение и соблюдение политик безопасности
(!)сохранение конфиденциальности информации
(?)комплекс мер по предотвращению несанкционированного доступа к информации
(!)обеспечение доступности информации

Атака модификации имеет больше шансов на успех если выполняется
(?)через Интернет
(!)в локальной сети отправителя
(?)место атаки не имеет значения

Атака на отказ в обслуживании обычно выполняется с помощью:
(!)заполнения сети посторонним трафиком
(?)использования уязвимостей в аппаратной инфраструктуре сети
(?)верный ответ отсутствует
(?)посылки специальных запросов, выводящих из строя
ПО сервера

Чтобы хранить пароли сетевых элементов (маршрутизаторов и коммутаторов) в зашифрованном виде, нужно выполнить команду
(?)service encryption
(?)enable password-encryption
(!)service password-encryption
(?)enable secret

По умолчанию пароли сетевых элементов (маршрутизаторов и коммутаторов) хранятся:

(!)в открытом виде, кроме секретного пароля привилегированного режима

(?)в открытом виде

(?)в зашифрованном виде

Web-серверы, доступные из внешней сети, следует размещать:

(?)за межсетевым экраном

(!)в демилитаризованной зоне DMZ

(?)перед межсетевым экраном

Стандартные списки доступа проверяют:

(!)только IP-адрес источника

(?)IP-адрес источника и IP-адрес назначения

IP-адрес источника, IP-адрес назначения, поле протокола в заголовке пакета Сетевого уровня и номер порта в заголовке Транспортного уровня

(?)IP-адрес источника, IP-адрес назначения, тип трафика

Условие deny any неявно содержится в конце

(?)именованных и расширенных списков доступа

(?)стандартных списков доступа

(?)только расширенных списков доступа

(!)любого списка доступа

Списки доступа могут использоваться, чтобы:

(?)разрешать (permit) продвижение пакетов через маршрутизатор

(!)как разрешать, так и запрещать продвижение пакетов через маршрутизатор

(?)запрещать (deny) продвижение пакетов через маршрутизатор

Для двух интерфейсов маршрутизатора, сконфигурированных для трех протоколов, может быть создано:

(?)верный ответ отсутствует

(!)12 списков доступа

(?)3 списка доступа

(?)6 списков доступа

Списки доступа бывают:

Выберите все правильные ответы (один или несколько)

(!)расширенные (extended)

(!)именованные (named)

(?)транзитные (pass-through)

(?)динамически формируемые (dynamic)

(!)стандартные (standard)

Если список доступа должен содержать как адреса сетей, так и адреса отдельных узлов, в списке необходимо:
(!)использовать маски Wildcard 0.0.0.0 при указании адресов узлов
(?)использовать маски Wildcard 0.0.0.255 при указании адресов узлов

Последовательность команд создания списка:
RouterJ (confi g) # access-list 12 deny host 192.168.20.11
RouterJ (confi g) # access-list 12 deny host 192.168.30.24
Router_A (confi g) # access-list 12 permit any
RouterJ (confi g) # int f0/0
Router_A (confi g-if) # ip access-group 12 out
Выберите один правильный ответ
(?)запретит доступ станциям с IP 192.168.20.11 и 192.168.30.24
(?)разрешит доступ всем станциям
(!)разрешит доступ всем станциям, кроме 192.168.20.11 и 192.168.30.24

Чтобы удалить список доступа, используется команда:
(?)Router_A (confi g) # del access-list {номер}
(?)Router_A (confi g) # remove access-list {номер}
(!)Router_A (confi g) # no access-list {номер}
(?)Router_A (confi g) # discard access-list {номер}

Вопросы открытого типа

Запись_____ означает требование анализа пакетов только с данным номером порта назначения. Введите на месте пропуска текст (регистр не учитывается).
Ответ **eq.**

Именованные списки доступа — это_____:
(стандартные или расширенные списки доступа с собственным именем)

Для просмотра всех списков доступа нужно выполнить команду_____(show access-list)

Для управления коммутатором на интерфейс виртуальной локальной сети VLAN1 задаются_____:
(IP-адрес, маска, шлюз)

Если число MAC-адресов на порт ограничено до 1, безопасным адресом считается_____:
(первый адрес, динамически полученный коммутатором)

Команда switchport port-security включает_____:
(динамический режим обеспечения безопасности)

Если рабочая станция сети VLAN1 захочет переслать кадр рабочей станции сети VLAN2, адресом назначения кадра будет MAC-адрес_____:
(интерфейса маршрутизатора).

Пропускная способность транковых соединений равна_____:
(сумме пропускных способностей отдельных каналов)

Назначение виртуальных сетей на интерфейсы производится командами_____:
switchport access, switchport vlan {номер/имя} inf
{интерфейс}

В случае, когда три локальных сети управляются двумя коммутаторами, число задействованных интерфейсов маршрутизатора равно____:
(6)

При транковом соединении коммутатора и маршрутизатора вместо нескольких физических каналов используется_____:
(один логический канал).