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

«РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И КОМПЛЕКСЫ КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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 Соляной В.Н. Рабочая программа дисциплины «Радиоэлектронные системы и комплексы как объекты информационной безопасности» . – Королев МО: «Технологический университет», 2019.

Рецензент: к.в.н., доцент Сухотерин А.И.

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.		
Год утверждения (переутверждения)	2019	2020		
Номер и дата протокола заседания кафедры	№8 от 18.03.19	№10 от 12.05.20		

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

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2019	2020				
Номер и дата протокола заседания УМС	№6а от 26.03.19	№9 от 29.06.20				

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

Целью дисциплины является изучение радиоэлектронных систем и комплексов как объектов информационной безопасности.

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;
- 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 «Радиоэлектронные системы и комплексы как объекты информационной безопасности» относится к факультативной части основной профессиональной образовательной программы подготовки студентов по специальности 11.05.01 Радиоэлектронные системы и комплексы (уровень специалитета).

Изучение данной дисциплины базируется на знаниях школьной программы.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики и выполнения выпускной квалификационной работы специалиста.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 2 зачетных единицы, 72 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 3
Общая трудоемкость	**72**	**72**
Аудиторные занятия	**32**	**32**
Лекции (Л)	**16**	**16**
Практические занятия (ПЗ)	**16**	**16**
Лабораторные работы (ЛР)	**-**	**-**
Самостоятельная работа	**40**	**40**
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
Тема 1. Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	**2**	**4**	**-**	**-**	ПК-1, ПК-2
Тема 2. Основные понятия теории	**2**	**4**	**-**	**-**	ПК-1, ПК-2

информационной безопасности. Анализ угроз информационной безопасности.					
Тема 3. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	**2**	**4**	**-**	**-**	ПК-1, ПК-2
Тема 4. Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	**2**	**4**	**-**	**-**	ПК-1, ПК-2
Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности	**2**	**4**	**-**	**-**	ПК-1, ПК-2
Тема 6. Методология построения и анализа систем обеспечения информационной безопасности	**2**	**4**	**-**	**-**	ПК-1, ПК-2
Тема 7. Технические каналы утечки информации в радиоэлектронных системах передачи	**4**	**8**	**-**	**-**	ПК-1, ПК-2
Итого:	**16**	**32**	**-**	**-**	

4.2. Содержание тем дисциплины

Тема 1. Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации

Цели и задачи курса. Предмет, структура и краткое содержание курса. История возникновения и развития систем защиты информации. Понятие национальной безопасности. Виды безопасности личности, общества и государства: экономическая, внутриполитическая, социальная, международная,

информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях. Основные правовые и нормативные акты в области информационной безопасности. Методические указания по изучению курса. Рекомендуемая основная и дополнительная литература.

Тема 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.

Основные понятия теории компьютерной безопасности. Понятие информации, информационной безопасности АС. Субъектно-объектная модель информационной системы. Основные определения. Язык. Объекты. Субъекты. Доступ. Информационный поток. Монитор безопасности.

Ядро безопасности. Иерархические модели вычислительных систем и модель взаимодействия открытых систем(OSI/ISO).

Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.

Тема 3. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации

Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно-режимные меры. Защита от несанкционированного доступа (НСД). Построение парольных систем.-

Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации. Построение системы защиты от угрозы доступности информации. Эксплуатационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.

Тема 4. Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи

Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Решетка мандатных моделей. Ролевая политика безопасности.

Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности

Основные критерии защищенности информационных автоматизированных систем (АС). Классы защищенности АС. Критерии и классы защищенности средств вычислительной техники (СВТ) и АС.

Стандарты по оценки защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ- по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классовзащиты. Единые критерии безопасности информационных технологий (Common Criteria).Основные положения «Единых критериев». Требования безопасности. Профили защиты.

Тема 6. Методология построения и анализа систем обеспечения информационной безопасности

Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).Информационные АС и программные средства, сертифицированные в соответствии с требованиями «Оранжевой книги». Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности. Рекомендации по самостоятельному углубленному изучению разделов курса. Обзор литературы.

Тема 7. Технические каналы утечки информации в радиоэлектронных системах передачи

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

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. Стасенко И.В. Радиоэлектронные системы и устройства / Стасенко И.В. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. - 44: - ISBN 978-5-7038-3685-9. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/287592.

2. Юрков Н.К. Технология производства электронных средств [Электронный ресурс] / Юрков Н. К. - 2-е изд., испр., доп. - Санкт-Петербург: Лань, 2021. - 480 с. - Рекомендовано УМО вузов РФ по образованию в области радиотехники, электроники, биомедицинской техники и автоматизации в качестве учебника для студентов вузов, обучающихся по направлению 211000 — «Конструирование и технология электронных средств». - ISBN 978-5-8114-1552-6. URL: https://e.lanbook.com/book/168617.

3. Семенихина Д.В. Теоретические основы радиоэлектронной борьбы. Радиоэлектронная разведка и радиоэлектронное противодействие / Д.В. Семенихина; Ю.В. Юханов; Т.Ю. Привалова. - Ростов-на-Дону: Издательство Южного федерального университета, 2015. - 252 с. - ISBN 978-5-9275-1815-9. - Электронная программа (визуальная). Электронные данные : электронные. URL: http://biblioclub.ru/index.php?page=book&id=445197.

4. Ламанов А.И. Основы конструирования и технологии производства радиоэлектронных систем. Ч. 2. Взаимозаменяемость. Допуски и посадки : учеб. пособие по курсу «Основы конструирования и технология производства радиоэлектронных систем» / Ламанов А.И. - М. : Изд-во МГТУ им. Н.Э. Баумана, 2008. - 52: - ISBN 978-5-7038-3150-2. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/287546.

5. Семенихина Д.В. Теоретические основы радиоэлектронной борьбы. Радиоэлектронная разведка и радиоэлектронное противодействие / Д.В. Семенихина; Ю.В. Юханов; Т.Ю. Привалова. - Ростов-на-Дону: Издательство Южного федерального университета, 2015. - 252 с. - ISBN 978-5-9275-1815-9. - Электронная программа (визуальная). Электронные данные: электронные. URL: http://biblioclub.ru/index.php?page=book&id=445197.

6. Проскурин В.И. Радиолокационное наблюдение. Методы, модели, алгоритмы: монография. - Москва: Радиотехника, 2017. - 368 с.: ил. - (Научная серия " Конфликтно-устойчивые радиоэлектронные системы"). - ISBN 978-5-93108-137-3.

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

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

9. 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.

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

11. 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. Введение в специальность «Радиоэлектронные системы»: учеб. пособие / И.В. Вознесенский, А.В. Галев, Д.Д. Дмитриев, В.А. Петров; ред. В.Н. Митрохин.— Москва : Изд-во МГТУ им. Н.Э. Баумана, 2009.— 64 с. — ISBN 978-5-7038-3318-6 .— URL: https://lib.rucont.ru/efd/287506.

2. 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.

3. Малюк А.А. Теория защиты информации.-М.:Горячая линия-Телеком,2012.

4. Хорев П.Б. Программно-аппаратная защита информации. М.: ФОРУМ, 2009.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008. Москва, «ИД ФОРУМ – ИНФРА-М».

6. В.А. Тихонов, В.В. Райх. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.

7. В.А. Северин. Комплексная защита информации на предприятии. М.: Издательский дом «Городец»,2008.- 368с.

Мельников В.П. идр Информационная безопасность.М.: Издателский центр «Академия» , 2008.-336с.

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: «Радиоэлектронные системы и комплексы как объекты информационной безопасности».

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Радиоэлектронные системы и комплексы как объекты информационной безопасности».

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

«РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И КОМПЛЕКСЫ КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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	Тема 1-7	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	Тема 1-7	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.	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.	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.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.

3. 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
Правильные ответы отмечены знаком (!)

1. **Пассивная атака доступа реализуется путем**

Выберите один правильный ответ
(!)прослушивания информации, проходящей по сети
(?)подмены адреса передаваемого кадра
(?)перенаправления трафика к сниферу

2. **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

3. **Атака модификации имеет больше шансов на успех если выполняется**

Выберите один правильный ответ
(?)через Интернет
(!)в локальной сети отправителя
(?)место атаки не имеет значения

4. **Атака на отказ в обслуживании обычно выполняется с помощью:**

Выберите один правильный ответ
(!)заполнения сети посторонним трафиком
(?)использования уязвимостей в аппаратной инфраструктуре сети
(?)верный ответ отсутствует
(?)посылки специальных запросов, выводящих из строя ПО сервера

5. Чтобы хранить пароли сетевых элементов (маршрутизаторов и коммутаторов) в зашифрованном виде, нужно выполнить команду

Выберите один правильный ответ

(?)service encryption
(?)enable password-encryption
(!)service password-encryption
(?)enable secret

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

Выберите один правильный ответ

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

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

Выберите один правильный ответ

(?)за межсетевым экраном
(!)в демилитаризованной зоне DMZ
(?)перед межсетевым экраном

8. Стандартные списки доступа проверяют:

Выберите один правильный ответ

(!)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

9. Условие deny any неявно содержится в конце

Выберите один правильный ответ

(?)именованных и расширенных списков доступа
(?)стандартных списков доступа
(?)только расширенных списков доступа
(!)любого списка доступа

10. Списки доступа могут использоваться, чтобы:

Выберите один правильный ответ

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

11. Для двух интерфейсов маршрутизатора, сконфигурированных для трех протоколов, может быть создано:
Выберите один правильный ответ
(?)верный ответ отсутствует
(!)12 списков доступа
(?)3 списка доступа
(?)6 списков доступа

12. Списки доступа бывают:
Выберите все правильные ответы (один или несколько)
(!)расширенные (extended)
(!)именованные (named)
(?)транзитные (pass-through)
(?)динамически формируемые (dynamic)
(!)стандартные (standard)

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

14. 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

15. Чтобы удалить список доступа, используется команда:
Выберите один правильный ответ
(?)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

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

Ответ **eq.**

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

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

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

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

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

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

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

9. **Назначение виртуальных сетей на интерфейсы производится командами_____:**
(switchport access, switchport vlan {номер/имя} inf {интерфейс})

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

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