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 КОМПЬЮТЕРНЫХ СЕТЯХ»

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 компьютерных сетях» . – 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	N 8 от 18.03.19	N 10 от 12.05.20	N 12 от 11.06.21	N 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	N6а от 26.03.19	N9 от 29.06.20	N 7 от 15.06.21	N 5 от 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 компьютерных сетях» 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 единицы, 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

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час. Очное	Код компетенций
Раздел 1. Общие положения, организационно-правовые и криптографические основы ЗИ					
Тема 1. Основные понятия и положения защиты информации в ин формационно-вычислительных системах и организационно-правовые меры ЗИ	**2**	**4**	**-**	**1**	**ПК-1,2**
Тема 2. Стандарты и спецификации в области информационной безопасности	**2**	**4**	**-**	**1**	**ПК-1,2**
Тема 3. Административный уровень информационной безопасности в инфор-мационно-вычислительной системе	**2**	**4**	**-**	**2**	**ПК-1,2**
Тема 4. Криптографическая защита информации	**2**	**4**	**-**	**2**	**ПК-1,2**
Раздел 2. Безопасность ОС, программного обеспечения, корпоративных ВС и антивирусная защита					
Тема 5. Модели безопасности основных операционных систем	**2**	**4**	**-**	**2**	**ПК-1,2**
Тема 6. Системы защиты программного обеспечения	**2**	**4**	**-**	**2**	**ПК-1,2**
Тема 7. Защита информации в корпоративных сетях	**2**	**4**	**-**	**2**	**ПК-1,2**

Тема 8. Защита от информационных инфекций. Вирусология	**2**	**4**	**-**	**2**	**ПК-1,2**
Итого:	**16**	**32**	**-**	**14**	

4.2. Содержание тем дисциплины

Тема 1. Основные понятия и положения защиты информации в ин формационно-вычислительных системах и организационно-правовые меры ЗИ. Предмет защиты информации. Объект защиты информации. Понятие угрозы безопасности. Классификация угроз информационной безопасности. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Правовые и организационные методы защиты информации в информационно-вычислительных системах**.** Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты.

Тема 2. Стандарты и спецификации в области информационной безопасности. Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость. Концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем («оранжевая книга» министерства обороны США). Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800

Тема 3. Административный уровень информационной безопасности в информационно-вычислительной системе. Понятие политики безопасности. Анализ риска. Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харри- Сон-Руззо-Ульмана. Модель распространения прав доступа Take-grant. Модель системы безопасности Белла-Лападула. Модель LOW-WATER-MARK. Модели ролевого разграничения доступа.

Тема 4. Криптографическая защита информации. Основные определения криптологии. Классификация методов криптографического закрытия информации. Основы теории к. Шеннона. Основные криптографические модели и алгоритмы шифрования. Симметричные методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования.

Тема 5. Модели безопасности основных операционных систем. Механизмы защиты операционных систем. Система безопасности ос WINDOWS NT. Защита в операционной системе UNIX. Защита в операционной системе NOVELL NETWARE.

Тема 6. Системы защиты программного обеспечения. Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.

Тема 7. Защита информации в корпоративных сетях. Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов.

Тема 8. Защита от информационных инфекций. Вирусология. Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов.

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, для проведения промежуточной аттестации обучающихся по дисциплине «Теоретические основы компьютерной безопасности» приведена в Приложении 1.

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

Основная литература:

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учеб. пособие / Шелухин О.И. - М. : Горячая линия – Телеком, 2013. - 221: есть. - ISBN 978-5-9912-0323-4. - Электронная программа (визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/214235.
2. Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK: учеб. пособие / [н/д]. - М.: Горячая линия – Телеком, 2013. - 217: есть. - ISBN 978-5-9912-0287-9. - Электронная программа

(визуальная). Электронные данные: электронные. URL: https://lib.rucont.ru/efd/214212.
3. Торстейнсон, П. Криптография и безопасность в технологии .NET [Электронный ресурс] / Торстейнсон П., Ганеш Г.А. - 2-е изд. (эл.). - Москва: Лаборатория знаний, 2013. - 480 с. - ISBN 978-5-9963-1345-7. URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=8767.
4. Фокин, Г. А. Сети радиодоступа [Электронный ресурс] : учебное пособие / Фокин Г. А. - Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. - 314 с. URL: https://e.lanbook.com/book/180148.
5. В.Ф. Шаньгин Комплексная защита информации в корпоративных системах. М.: ИД «Форум»: ИНФРА-М., 2015.
6. Васильков А.В., Васильков А.А., Васильков И. А. Информационные системы и их безопасность М.: ФОРУМ, 2011.
7. 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.
8. А.Ф. Чепига Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.
9. 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. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

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 (модуля) 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 МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Методы и средства защиты информации в компьютерных сетях»

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 КОМПЬЮТЕРНЫХ СЕТЯХ»

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 1-8	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 1-8	ИД-1.1 ПК-2. Виды и содержание эксплуатаци	ИД-2.1. ПК-2. Уметь организовывать рабочие	ИД-3.1. ПК-2. Владеть организацией и осуществлением

				онных документов. ИД-1.2 ПК-2. Передовой отечественный и зарубежный опыт эксплуатации и технического обслуживания электронного оборудования.	места персонала, обслуживающего радиоэлектронные системы. ИД-2.2. ПК-2. Уметь работать с эксплуатационной документацией по техническому обслуживанию радиоэлектронных систем.	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

Пассивная атака доступа реализуется путем
Выберите один правильный ответ
(!)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
Выберите один правильный ответ
(?)через Интернет
(!)в локальной сети отправителя
(?)место атаки не имеет значения

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

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

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

Web-серверы, доступные из внешней сети, следует размещать:
Выберите один правильный ответ
(?)за межсетевым экраном
(!)в демилитаризованной зоне DMZ
(?)перед межсетевым экраном

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

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

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

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

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:
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

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:
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

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).

"Троянский конь" является разновидностью модели воздействия программных закладок
• искажение

"Уполномоченные серверы" были созданы для решения проблемы
• имитации IP-адресов

"Уполномоченные серверы" фильтруют пакеты на уровне
• приложений

ACL-список ассоциируется с каждым
• объектом

Абстрактное описание системы, без связи с ее реализацией, дает модель

политики безопасности
• Белла-ЛаПадула

Административные действия в СУБД позволяют выполнять привилегии
• безопасности

Администратор сервера баз данных имеет имя
• ingres

Администратором базы данных является:
• любой пользователь, создавший БД

Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем.
• физическом

Брандмауэры второго поколения представляли собой ...
• "уполномоченные серверы"

Брандмауэры первого поколения представляли собой ...
• маршрутизаторы с фильтрацией пакетов

Брандмауэры третьего поколения используют для фильтрации
• специальные многоуровневые методы анализа состояния пакетов

В "Европейских критериях" количество классов безопасности равно:
• 10

В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен:
• доминировать

В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:
• быть равен

В многоуровневой модели, если субъект доступа формирует запрос на чтение, то уровень безопасности субъекта относительно уровня безопасности объекта должен:
• доминировать

В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то ...

• никакие запросы на выполняются

В модели политики безопасности Лендвера многоуровневая информационная структура называется:
• контейнером

В модели политики безопасности Лендвера одноуровневый блок информации называется:
• объектом

В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется ...
• прямой

В модели политики безопасности Лендвера ссылка на сущность, если это последовательность имен сущностей, называется ...
• косвенной

В СУБД Oracle под ролью понимается:
• набор привилегий

Взаимодействие с глобальными ресурсами других организаций определяет уровень ОС
• внешний

Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
• доступность

Восстановление данных является дополнительной функцией услуги защиты
• целостность

Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это:
• принцип минимазации привилегий

Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:
• целостность

Главным параметром криптосистемы является показатель
• криптостойкости

Готовность устройства к использованию всякий раз, когда в этом возникает

необходимость, характеризует свойство
• доступность

Два ключа используются в криптосистемах
• с открытым ключом

Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели
• искажение

Дескриптор защиты в Windows 2000 содержит список
• пользователей и групп, имеющих доступ к объекту

Длина исходного ключа в ГОСТ 28147-89 (бит):
• 256

Длина исходного ключа у алгоритма шифрования DES (бит):
• 56

Для реализации технологии RAID создается:
• псевдодрайвер

Для решения проблемы правильности выбора и надежности функционирования средств защиты в "Европейских критериях" вводится понятие:
• адекватности средств защиты

Для создания базы данных пользователь должен получить привилегию от:
• администратора сервера баз данных

Домены безопасности согласно "Оранжевой книге" используются в системах класса
• B3

Достоинствами аппаратной реализации криптографического закрытия данных являются:
• высокая производительность и простота

Достоинствами программной реализации криптографического закрытия данных являются:
• практичность и гибкость

Достоинством дискретных моделей политики безопасности является:
• простой механизм реализации

Достоинством матричных моделей безопасности является:
• легкость представления широкого спектра правил обеспечения безопасности

Достоинством модели конечных состояний политики безопасности является:
• высокая степень надежности

Достоинством модели политики безопасности на основе анализа угроз системе является:
• числовая вероятностная оценка надежности

Единственный ключ используется в криптосистемах
• симметричных

Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:
• высокой

Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается:
• средней

Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:
• базовой

Задачей анализа модели политики безопасности на основе анализа угроз системе является:
• минимизация вероятности преодоления системы защиты

Запись определенных событий в журнал безопасности сервера называется:
• аудитом

Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты
• встроенных в ОС

Защита исполняемых файлов обеспечивается:
• обязательным контролем попытки запуска

Защита от программных закладок обеспечивается:
• аппаратным модулем, устанавливаемым на системную шину ПК

Защита от форматирования жесткого диска со стороны пользователей обеспечивается:
• аппаратным модулем, устанавливаемым на системную шину ПК

Защита с применением меток безопасности согласно "Оранжевой книге" используется в системах класса
• B1

Идентификаторы безопасности в Windows 2000 представляют собой ...
• двоичное число, состоящее из заголовка и длинного случайного компонента