



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

**«СРЕДСТВА РЭБ ДЛЯ ЗАЩИТЫ НАЗЕМНЫХ КОСМИЧЕСКИХ
ОБЪЕКТОВ»**

Специальность: 11.05.01 Радиоэлектронные системы и комплексы

Специализация: Радиоэлектронная борьба

Уровень высшего образования: специалитет

Квалификация (степень) выпускника: инженер

Форма обучения: очная

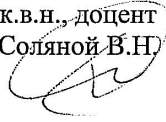
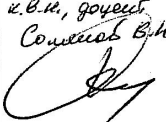
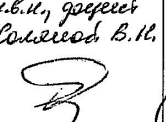
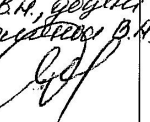
Королев
2019

Автор: к.в.н., доцент Соляной В.Н. Рабочая программа дисциплины «Средства РЭБ для защиты наземных космических объектов» . – 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.

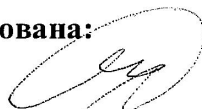
Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н. 	к.в.н., доцент Соляной В.Н. 	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	№ 64 от 26.03.19	№ 9 от 29.06.20	№ 7 от 15.06.21	№ 50 от 21.06.22		

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

Целью дисциплины является изучение базовых положений и основных принципов функционирования средств РЭБ для защиты наземных космических 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:

- сформировать у студентов знания основ построения и принципов функционирования средств РЭБ для защиты наземных космических объектов;
- освоить методологию обмена, передачи и коммутации данных в наиболее распространенных средствах РЭБ для защиты наземных космических объектов.

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 «Средства РЭБ для защиты наземных космических объектов» 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 изученных ранее дисциплинах: «Физика», «Основы теории систем и комплексов РЭБ», и компетенциях: ОПК-4,6, ПК-1,2.

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.

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
Курсовые работы (проекты)	+	+
Расчетно-графические работы	-	-
Контрольная работа, домашнее задание	-	-
Текущий контроль знаний	Тест	Тест
Вид итогового контроля	Экзамен	Экзамен

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практиче ские занятия, час. Очное	Лаборат орные работы, час. Очное	Занятия в интерактив ной форме, час. Очное	Код компетенций
Тема 1. Общие сведения о радиотехнических системах для защиты наземных космических объектов	2	4	-	2	ПК-1 ПК-2
Тема 2. Методы радионавигационных измерений наземных космических объектов	2	4	-	2	ПК-1 ПК-2
Тема 3. Радиотехнические системы передачи информации для наземных космических объектов	2	4	-	2	ПК-1 ПК-2
Тема 4. Методы и системы радиоуправления наземных космических объектов	2	4	-	2	ПК-1 ПК-2
Тема 5. Методы и средства радиоэлектронной борьбы для защиты наземных космических объектов	4	8	-	2	ПК-1 ПК-2
Тема 6. Контроль работы радиоэлектронных систем наземных космических объектов	4	8	-	4	ПК-1 ПК-2
Итого:	16	32	-	14	

4.2. Содержание тем дисциплины

Тема 1. Общие сведения о радиотехнических системах для защиты наземных космических объектов

Определения, основные задачи, решаемые радиотехническими системами. Радиосигнал, как носитель информации в РТС. Классификация РТС. Обобщённая структурная схема РТС. Эксплуатационно – тактические характеристики РТС. Технические характеристики РТС. Элементы теории оптимального обнаружения сигналов. Энергетические характеристики РТС.

Тема 2. Методы радионавигационных измерений наземных космических объектов

Методы измерения расстояний. Методы измерения угловых координат. Методы измерения скорости движения объектов. Методы измерения углов ориентации летательных аппаратов. Методы радиолокационного обзора пространства. Методы определения местоположения объектов. Методы измерения угловой скорости движения объектов. Методы построения измерителей навигационных параметров следящего типа. Комплексование измерителей навигационных параметров.

Тема 3. Радиотехнические системы передачи информации для наземных космических объектов

Общие сведения. Одноканальные РТС передачи информации. Многоканальные РТС передачи информации. Цифровые методы передачи информации. Методы защиты информации. Асинхронные адресные системы передачи информации. Ретрансляционные линии связи.

Тема 4. Методы и системы радиоуправления наземных космических объектов

Общие принципы построения систем радиоуправления. Методы наведения летательных аппаратов. Системы радиотеленаведения. Системы командного

радиотелеуправления. Системы самонаведения. Корреляционно – экстремальные системы радиоуправления.

Тема 5. Методы и средства радиоэлектронной борьбы для защиты наземных космических объектов

Общие сведения. Активные помехи РТС, работающим в режимах обзора пространства. Активные помехи РТС, работающим в режимах автоматического сопровождения целей по направлению. Активные помехи РТС, работающим в режимах автоматического сопровождения целей по дальности. Активные помехи РТС, работающим в режимах автоматического сопровождения целей по скорости. Пассивное радиоподавление с помощью дипольных отражателей. Ложные цели. Пассивные переизлучатели. Методы снижения эффективной поверхности рассеяния объектов. Изменение свойств среды распространения электромагнитных волн. Комплексирование активных и пассивных методов радиоподавления. Перспективы развития средств радиоэлектронного подавления.

Тема 6. Контроль работы радиоэлектронных систем наземных космических объектов

Общие сведения. Построение КПА внешнего контроля. Системы встроенного контроля.

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. 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>.
2. 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>.
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. Проектирование радиопередающих устройств для систем подвижной радиосвязи / Зырянов Ю.Т., Федюнин П.А., Белоусов О.А., Рябов А.В.; Головченко Е.В., Курносое Р.Ю. - 1-е изд. - : Лань, 2017. - 116 с. - ISBN 978-5-8114-2514-3. - Электронная программа (визуальная). Электронные данные: электронные. URL: <https://e.lanbook.com/book/93691>.
5. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации : учебное пособие. - М. : Форум, 2011 г;
6. Малюк А.А. Теория защиты информации. Научное издание.- М.: Горячая линия-телеком, 2013 г.;
7. Зайцев, А.П. и др. Технические средства и методы защиты информации: учебное пособие для вуза / под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2012 г.;
8. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов. - 4-е изд., стереотип. - М. : Горячая линия - Телеком, 2011 г.

Дополнительная литература:

1. Купряшкин И. Ф., Космическая радиолокационная съемка земной поверхности в условиях помех : монография / И.Ф. Купряшкин, В.П. Лихачев. - Воронеж : Научная книга, 2014. - 458 с.
2. Радиолокационные системы авиационно-космического мониторинга земной поверхности и воздушного пространства : монография / [В. С.

Верба, Б.Г. татарский, А.Р. Ильчук и др.]; под ред. д.т.н., проф. В. С. Вербы, д.т.н., проф. Б. Г. Татарского Федер. науч.-произв. центр ОАО "Концерн "Вега"]. - Москва : Радиотехника, 2014. - 570 с;

3. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М. : ИД "ФОРУМ" : ИНФРА-М, 2013 г.;
4. Мельников, Д.А. Информационная безопасность открытых систем: учебник. - М.: ФЛИНТА, 2013 г.;
5. Грибунин, В.Г. Комплексная система защиты информации на предприятии : учеб. пособие. - М.: Академия ИЦ, 2009 г.;
6. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. - М.: Горячая линия-Телеком, 2013 г.;
7. Чипига, А.Ф. Информационная безопасность автоматизированных систем : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности - М. : Гелиос АРВ, 2010 г.;
8. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность: учебное пособие. - М.: ФОРУМ, 2013 г.

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

Интернет-ресурсы:

1. <http://eup.ru> – научно - образовательный портал.
2. <http://znanium.com> – образовательный портал
3. <http://www.academy.it> – академия АЙТИ

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: «Средства РЭБ для защиты наземных космических объектов».

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Средства РЭБ для защиты наземных космических объектов».

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

Лекционные занятия:

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

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекции в форме слайд-презентации, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows 7, офисные программы MSOffice;
- рабочее место преподавателя, оснащенное компьютером с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

*ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ ФАКУЛЬТЕТ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«СРЕДСТВА РЭБ ДЛЯ ЗАЩИТЫ
НАЗЕМНЫХ КОСМИЧЕСКИХ ОБЪЕКТОВ»**

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

1	ПК-1	Разработка научно-технических проектов, проектирование и сопровождение РТС и РЭС изделий ракетно-космической техники	Тема 1-6	<p>ИД-1.1 ПК-1. Руководящие, методические и нормативные технические документы по выпуску технической документации.</p> <p>ИД-1.2 ПК-1. Порядок работы с персональной вычислительной техникой, файловой системой, форматы представления электронной графической и текстовой информации.</p>	<p>ИД-2.1. ПК-1. Уметь разрабатывать материалы проектной конструктивной документации на РТС и РЭС.</p> <p>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.</p>	<p>ИД-3.1. ПК-1. Владеть навыками по организации совместной работы по проектированию РТС и РЭС со смежными подразделениями.</p> <p>ИД-3.2. ПК-1. Разработка плана мероприятий или работы с организационными исполнителями (соисполнителями) НИР.</p>
2	ПК-2	Эксплуатация радиоэлектронных систем	Тема 1-6	<p>ИД-1.1 ПК-2. Виды и содержание эксплуатационных документов.</p> <p>ИД-1.2 ПК-2. Передовой отечественной и</p>	<p>ИД-2.1. ПК-2. Уметь организовывать рабочие места персонала, обслуживающего радиоэлект</p>	<p>ИД-3.1. ПК-2. Владеть организацией и осуществлением мероприятий по контролю соблюдения</p>

				зарубежный опыт эксплуатации и технического обслуживания электронного оборудования .	ронные системы. ИД-2.2. ПК-2. Уметь работать с эксплуатационной документацией по техническому обслуживанию радиоэлектронных систем.	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	Тесты	<p>А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов</p> <p>Б) частично сформирована: •компетенция освоена на продвинутом уровне – 4 балла; •компетенция освоена на базовом уровне – 3 балла;</p> <p>В) не сформирована (компетенция не освоена) – 2 и менее баллов</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> 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 тематике (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.</p>

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

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

ПК-2: Эксплуатация радиоэлектронных систем

**Вопросы, выносимые на тестирование
Вопросы закрытого типа**

С уменьшением расстояния между подавляемой РТС и помехоносителем соотношение сигнал /помеха на входе РТС:

(!)А - Увеличивается.

(?)Б - Уменьшается

(?)В - Остается постоянным

Наибольшая уязвимость радиоэлектронных средств управления оружием заключается:

(?)А - в малой чувствительности приемных каналов

(?)Б - в ограниченной дальности действия

(!)В - в наличии радиоизлучения

В какой последовательности при выполнении боевой операции осуществляют подавление различных РТС?

(?)А - РТС наведения оружия, РТС обзора и целеуказания, РТС подрыва боевой части наводимого оружия

(?)Б - РТС подрыва боевой части наводимого оружия, РТС наведения оружия, РТС обзора и целеуказания.

(!)В - РТС обзора и целеуказания, РТС наведения оружия, РТС подрыва боевой части наводимого оружия

Для какого вида помех не требуется создавать большое превышение помехи над сигналом на входе подавляемой РТС?

(?)А - Для маскирующих помех

(!)Б - Для имитирующих помех

(?)В - Для подавляющих помех

На каком расстоянии от подавляемой РТС целесообразно включать средства радиопротиводействия?

(?)А - На расстоянии 0,7 от максимальной дальности действия РТС.

(?)Б - На расстоянии 1,0 от максимальной дальности действия РТС.

(!)В - На расстоянии 1,3 от максимальной дальности действия РТС.

Какой вид помехового воздействия можно осуществить полуактивной РТС самонаведения, работающей в режиме непрерывного излучения?

- (?)А - Уводящую помеху по дальности.
- (?)Б - Хаотическую помеху типа «ХИП»
- (!)В - Уводящую помеху по скорости.**

Что дает уменьшение эффективной поверхности рассеяния (ЭПР) защищаемых объектов?

- (!)А - Уменьшает дальность обнаружения объектов**
- (?)Б - Увеличивает скорость движения объектов
- (?)В - Уменьшает массогабаритные характеристики объектов.

Какие формы отражающих поверхностей имеют наименьшую эффективную поверхность рассеяния (ЭПР)?

- (?)А - Сферическая форма.
- (!)Б - Конусообразная форма**
- (?)В - Плоская поверхность.

Какие помеховые сигналы называют «помехи, не оставляющие следа»?

- (!)А - Помехи, имитирующие неисправность подавляемой аппаратуры**
- (?)Б — Помехи, полностью подавляющие полезные сигналы РТС.
- (?)В - Помехи, исчезающие при их обнаружении

Скорость снижения дипольных отражателей на больших высотах:

- (?)А - Уменьшается
- (!)Б - Увеличивается**
- (?)В - Остается постоянной на всех высотах

Современные дипольные отражатели изготавливают:

- (!)А - Из металлизированного стекловолокна**
- (?)Б - Из стальной проволоки
- (?)В - Из древесной стружки

«Черные диполи» это:

- (?)А - Диполи, окрашенные в чёрный цвет.
- (!)Б - Диполи, поглощающие электромагнитную энергию**
- (?)В - Диполи, наиболее эффективно отражающие электромагнитную энергию

Эффектом воздействия многократных импульсных помех на РТС, работающих в режимах обзора пространства, является:

- (!)А - Увеличение времени анализа принимаемых РТС сигналов.**
- (?)Б - Уменьшение мощности сигналов на входе подавляемой РТС
- (?)В - Изменение параметров модуляции принимаемых РТС сигналов

Пассивная атака доступа реализуется путем

Выберите один правильный ответ

(!) прослушивания информации, проходящей по сети

(?) подмены адреса передаваемого кадра

(?) перенаправления трафика к сниферу

Согласно стандарту ISO/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

Вопросы открытого типа

Атака модификации имеет больше шансов на успех если выполняется (в локальной сети отправителя)

Атака на отказ в обслуживании обычно выполняется с помощью: (заполнения сети посторонним трафиком)

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

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

(в открытом виде, кроме секретного пароля привилегированного режима)

Web-серверы, доступные из внешней сети, следует размещать: (в демилитаризованной зоне DMZ)

Стандартные списки доступа проверяют:

(только IP-адрес источника)

Условие deny any неявно содержится в конце (любого списка доступа)

Списки доступа могут использоваться, чтобы:

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

Для двух интерфейсов маршрутизатора, сконфигурированных для трех протоколов, может быть создано:
(12 списков доступа)

Списки доступа бывают:
(расширенные (extended), именованные (named), 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)

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

(разрешит доступ всем станциям, кроме 192.168.20.11 и 192.168.30.24)

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

Запись _____ означает требование анализа пакетов только с данным номером порта назначения.
(!)eq

1. Именованные списки доступа — это:
(стандартные или расширенные списки доступа с собственным именем)

2. Для просмотра всех списков доступа нужно выполнить команду _____
(show access-list)

Коммутаторы можно конфигурировать через:
(веб-интерфейс, интерфейс командной строки, браузер)

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

Таблица коммутации содержит:
(имя VLAN, интерфейс, тип записи, MAC-адрес)

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)

Виртуальные сети:

(создаются для сегментации сети на коммутаторах, являются логическим объединением групп станций сети)

Для нормального функционирования виртуальных сетей необходимо:

(приписать порты коммутатора к соответствующей сети VLAN, сконфигурировать все виртуальные локальные сети на коммутаторе)

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}`)

Создание виртуальных сетей может производиться:

(по команде `vlan database` из привилегированного режима конфигурирования, в режиме глобального конфигурирования, динамически через ПО управления сети)

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)