МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации в радиоэлектронных системах передачи информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль): **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РТС, Кафедра радиотехнических систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	18	18	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 7 семестр

Томск 2017

Согласована на портале № 22791

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от «27» 11 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.05.01 Радиоэлектронные системы и комплексы, утвержденного 11 августа 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент кафедры, к.т.н., ст.н.с. каф.
РТС _____ А. М. Голиков

Заведующий обеспечивающей каф.
РТС _____ С. В. Мелихов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РТС _____ С. В. Мелихов

Эксперт:

старший преподаватель кафедры
РТС кафедра РТС _____ Д. О. Ноздреватых

Согласована на портале № 22791

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Дисциплина "Защита информации в радиоэлектронных системах передачи информации (ЗИвРЭСПИ) относится к числу дисциплин специализации рабочего учебного плана для подготовки инженеров по специальности 11.05.01-Радиоэлектронные системы и комплексы (специализация Радиоэлектронные системы передачи информации). Целью преподавания дисциплины является изучение методов защиты и основных закономерностей передачи информации в цифровых телекоммуникационных системах.

1.2. Задачи дисциплины

– Основной задачей дисциплины является формирование у студентов компетенций, позволяющих самостоятельно проводить математический анализ физических процессов в ана¬логовых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчи¬вости телекоммуникационных систем и сетей.

– В курсе ЗИвРЭСПИ принят единый методологический подход к анализу и синтезу современных телекоммуникационных систем и устройств на основе вероятностных моделей со¬общений, сигналов, помех и каналов в системах связи. Предусмотренные программой курса ЗИвРЭСПИ знания являются не только базой для последующего изучения специальных дисцип¬лин, но имеют также самостоятельное значение для формирования инженеров по специальности 11.05.01 Радиоэлектронные системы и комплексы.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в радиоэлектронных системах передачи информации» (Б1.Б.30.1) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Введение в специальность, Информационные технологии 2. Сетевые информационные технологии. Базы данных., Практика по получению профессиональных умений и опыта профессиональной деятельности, Теория радиосистем передачи информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Кодирование и шифрование информации в радиоэлектронных системах передачи информации, Моделирование в радиоэлектронных системах передачи информации, Научно-исследовательская работа, Проектирование радиотехнических систем, Радиоэлектронные системы передачи информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-2.1 способностью разрабатывать структурные и функциональные схемы мобильных, широкополосных и спутниковых систем передачи информации;

В результате изучения дисциплины студент должен:

– **знать** В результате изучения дисциплины студент должен: знать - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства; - современные подходы к построению систем защиты информации; - компьютерные системы и сети как объект информационного воздействия, критерии оценки их защищенности и методы обеспечения их информационной безопасности

– **уметь** уметь - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; - применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований.

– **владеть** владеть - анализом информационной инфраструктуры государства; - методами формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей.

Согласована на портале № 22791

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	72	72
Лекции	36	36
Практические занятия	18	18
Лабораторные работы	18	18
Самостоятельная работа (всего)	36	36
Оформление отчетов по лабораторным работам	10	10
Проработка лекционного материала	16	16
Подготовка к практическим занятиям, семинарам	10	10
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	2	0	0	2	4	ПСК-2.1
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.	4	4	0	4	12	ПСК-2.1
3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	6	4	10	8	28	ПСК-2.1
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	8	4	4	6	22	ПСК-2.1

Согласована на портале № 22791

5 Стандарты информационной безопасности, критерии и классы оценки защищенности	8	2	0	4	14	ПСК-2.1
6 Методология построения и анализа систем обеспечения информационной безопасности	4	0	0	4	8	ПСК-2.1
7 Технические каналы утечки информации в радиоэлектронных системах передачи	4	4	4	8	20	ПСК-2.1
Итого за семестр	36	18	18	36	108	
Итого	36	18	18	36	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
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.	2	ПСК-2.1
	Итого	2	
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	4	ПСК-2.1

Согласована на портале № 22791

	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.		
	Итого	4	
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. Эксплутационно-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.	6	ПСК-2.1

Согласована на портале № 22791

	Итого	6	
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.	8	ПСК-2.1
	Итого	8	
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 классов защиты.Единые критерии безопасности информационных технологий (Common Criteria). Основные положения «Единых критериев». Требования безопасности. Профили защиты.	8	ПСК-2.1
	Итого	8	
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 тре-	4	ПСК-2.1

Согласована на портале № 22791

	бованиями «Оранжевой книги». Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности. Рекомендации по самостоятельному углубленному изучению разделов курса. Обзор литературы.		
	Итого	4	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Про-стые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.	4	ПСК-2.1
	Итого	4	
Итого за семестр		36	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин						
	1	2	3	4	5	6	7
Предшествующие дисциплины							
1 Введение в специальность	+		+				+
2 Информационные технологии 2. Сетевые информационные технологии. Базы данных.			+	+		+	
3 Практика по получению профессиональных умений и опыта профессиональной деятельности			+			+	+
4 Теория радиосистем передачи информации			+				+
Последующие дисциплины							
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты			+	+		+	+
2 Кодирование и шифрование информации в радиоэлектронных системах передачи информации	+		+				+

Согласована на портале № 22791

3 Моделирование в радиоэлектронных системах передачи информации			+			+	+
4 Научно-исследовательская работа			+	+		+	+
5 Проектирование радиотехнических систем			+			+	+
6 Радиоэлектронные системы передачи информации			+			+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий				Формы контроля
	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПСК-2.1	+	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Экзамен, Конспект самоподготовки, Защита отчета, Коллоквиум, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Выступление (доклад) на занятии, Расчетная работа, Тест, Реферат, Отчет по практическому занятию, Дифференцированный зачет

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			

Согласована на портале № 22791

3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Изучение международного стандарта безопасности информационных систем ISO 17799	2	ПСК-2.1
	Исследование системы защиты информации «Страж NT»	2	
	Система защиты информации SecretNet	4	
	Система защиты информации Dallas	2	
	Итого	10	
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Система анализа рисков и проверки политики информационной безопасности предприятия	4	ПСК-2.1
	Итого	4	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Энергетическое скрытие речевой информации (с использованием звуковой карты и звукового редактора ПЭВМ).	4	ПСК-2.1
	Итого	4	
Итого за семестр		18	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.	Стандарты информационной безопасности и критерии оценки безопасности компьютерных систем и сетей	4	ПСК-2.1
	Итого	4	
3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Разработка архитектуры модели безопасности информационных систем и сетей	4	ПСК-2.1
	Итого	4	
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Разработка практических рекомендаций по обеспечению безопасности информационных систем	4	ПСК-2.1
	Итого	4	
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	Законодательство в области информационной безопасности	2	ПСК-2.1
	Итого	2	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических	4	ПСК-2.1

Согласована на портале № 22791

	каналов утечки информации. Про-стые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.		
	Итого	4	
Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	Проработка лекционного материала	2	ПСК-2.1	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Тест, Экзамен
	Итого	2		
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Выступление (доклад) на занятии, Домашнее задание, Защита отчета, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Выступление (доклад) на занятии, Дифференцированный зачет, Домашнее задание, Защита отчета, Конспект самоподготовки, Контрольная работа,
	Проработка лекционного материала	2		
	Оформление отчетов по	2		

Согласована на портале № 22791

информации	лабораторным работам			Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Собеседование, Тест, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	8		
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Домашнее задание, Защита отчета, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Реферат, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	6		
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Домашнее задание, Защита отчета, Коллоквиум, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
6 Методология построения и анализа систем обеспечения информационной безопасности	Проработка лекционного материала	4	ПСК-2.1	Домашнее задание, Защита отчета, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Реферат, Тест, Экзамен
	Итого	4		
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Домашнее задание, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Реферат, Собеседование, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	8		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен

Согласована на портале № 22791

Итого	72		

9.1. Вопросы для подготовки к практическим занятиям, семинарам

1. Радиоэлектронные системы и устройства защиты информации
2. Безопасность сетевых операционных систем
3. Политика и модели безопасности
4. Безопасность локальных и глобальных сетевых технологий

9.2. Вопросы на проработку лекционного материала

1. Комплексная защита информации в компьютерных системах и сетях
2. Криптографические методы и средства защиты информации в компьютерных системах и сетях

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Выступление (доклад) на занятии		2	4	6
Домашнее задание		2	4	6
Защита отчета		2	4	6
Коллоквиум		4		4
Конспект самоподготовки		2	2	4
Контрольная работа		2	2	4
Опрос на занятиях	2	2	2	6
Отчет по индивидуальному заданию			4	4
Отчет по лабораторной работе		4	4	8
Отчет по практическому занятию	2	2		4
Расчетная работа			4	4
Реферат			4	4
Собеседование		2	2	4
Тест	2	2	2	6
Итого максимум за период	6	26	38	70
Экзамен				30
Нарастающим итогом	6	32	70	100

Согласована на портале № 22791

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Защита информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7072, дата обращения: 29.11.2017.

12.2. Дополнительная литература

1. Защита информации в инфокоммуникационных системах и сетях: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 655 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7079, дата обращения: 29.11.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7072, дата обращения: 29.11.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

Согласована на портале № 22791

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Яндекс

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 401. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 401. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой,

Согласована на портале № 22791

аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает

Согласована на портале № 22791

предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 22791

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Защита информации в радиоэлектронных системах передачи информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль): **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РТС, Кафедра радиотехнических систем**
Курс: **4**
Семестр: **7**

Учебный план набора 2016 года

Разработчик:
- доцент кафедры, к.т.н., ст.н.с. каф. РТС А. М. Голиков

Экзамен: 7 семестр

Томск 2017

Согласована на портале № 22791

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПСК-2.1	способностью разрабатывать структурные и функциональные схемы мобильных, широкополосных и спутниковых систем передачи информации	Должен знать В результате изучения дисциплины студент должен: знать - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства; - современные подходы к построению систем защиты информации; - компьютерные системы и сети как объект информационного воздействия, критерии оценки их защищенности и методы обеспечения их информационной безопасности ; Должен уметь уметь - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; - применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований. ; Должен владеть владеть - анализом информационной инфраструктуры государства; - методами формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей. ;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучае-	Обладает диапазоном практических умений, требуемых для решения	Берет ответственность за завершение задач в исследовании, приспосаб-

Согласована на портале № 22791

	мой области	определенных проблем в области исследования	ливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПСК-2.1

ПСК-2.1: способностью разрабатывать структурные и функциональные схемы мобильных, широкополосных и спутниковых систем передачи информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Должен знать: - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства; - современные подходы к построению систем защиты информации; - компьютерные системы и сети как объект информационного воздействия, критерии оценки их защищенности и методы обеспечения их информационной безопасности	Должен уметь: - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; - применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований	Должен владеть: - анализом информационной инфраструктуры государства; - методами формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей.
Виды занятий	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Конспект самоподготовки; • Коллоквиум; • Собеседование; • Отчет по лабораторной работе;	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Конспект самоподготовки; • Коллоквиум; • Собеседование; • Отчет по лабораторной работе;	• Отчет по лабораторной работе; • Домашнее задание; • Отчет по индивидуальному заданию; • Выступление (доклад) на занятии; • Расчетная работа; • Коллоквиум; • Реферат;

Согласована на портале № 22791

	• Опрос на занятиях; • Выступление (доклад) на занятии; • Расчетная работа; • Тест; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;	• Опрос на занятиях; • Выступление (доклад) на занятии; • Расчетная работа; • Тест; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;	• Отчет по практическому занятию; • Дифференцированный зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития твор-ческих решений, абстрагирования проблем;	• Контролирует работу, проводит оценку, совершенствует действия работы;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области ;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования;	• Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, требуе-мыми для выполне-ния простых задач;	• Работает при прямом наблюдении;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Вопросы на самоподготовку

– - усвоение лекционного материала по учебным пособиям с самопроверкой по контрольным вопросам (контрольные вопросы содержатся в учебном пособии – см. - подготовка к экзамену [Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. – 2015. 284 с. https://edu.tusur.ru/training/publications/5262]

3.2 Тестовые задания

– 1. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?

– 2. Назовите два типа биометрических систем. Назовите основные категории атак.

– 3. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

– 4. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентифи-

Согласована на портале № 22791

кация сильнее, чем однофакторная? Зачем нужен аудит?

– 5. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?

– 6. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

– 7. Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?

– 8. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?

– 9. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?

– 10. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?

– 11. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

– 12. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 13. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

– 14. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 15. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

– 16. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования? Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

– 17. Может ли быть взломан правильно реализованный "одноразовый блокнот"? Какую длину имеют ключи DES?

– 18. В чем заключается основной недостаток DES? За счет чего тройной DES повышает уровень безопасности алгоритма DES?

– 19. Для чего предназначен алгоритм AES? На сложности какой задачи базируется безопасность, обеспечиваемая алгоритмом Диффи-Хеллмана?

– 20. Что такое цифровая подпись? Почему открытые ключи должны быть сертифицированными?

3.3 Темы рефератов

– 1. Исследование и разработка методики развертывания и администрирования WEB-сервера на Windows Server 2012

– 2. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom

– 3. Система защиты информации от несанкционированного доступа "Страж"

– 4. Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом

– 5. Система защиты информации "SecretNet"

– 6. Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ

– 7. Система защиты информации Dallas Lock

– 8. Защита беспроводных сетей стандартов IEEE 802.11

– 9. Исследование методов аналогового скремблирования на базе LabView

– 10. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP

– 11. Защита беспроводных сетей стандартов IEEE 802.15

Согласована на портале № 22791

– 12. Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии
– 13. Защита беспроводных сетей стандартов GSM, CDMA
– 14. Защита беспроводных сетей стандартов WiMAX
– 15. Защита беспроводных сетей стандартов LTE
– 16. Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO
– 17. Формальные политики и математические модели компьютерной безопасности
–
– 18. Организация защиты сетей CISCO
– 19. Обзор и анализ наиболее важных стандартов и спецификаций в области информационной безопасности
–
– 20. Обзор и анализ классических криптографических шифров
– 21. Обзор и анализ симметричных криптографических шифров
– 22. Обзор и анализ ассиметричных криптографических шифров
– 23. Программные комплексы для создания криптовалюты Биткойн
– 24. Алгоритм шифрования данных AES и его программная реализация
– 25. Инфраструктуры открытых ключей PKI

3.4 Темы коллоквиумов

– 1. Исследование и разработка методики развертывания и администрирования WEB-сервера на Windows Server 2012
– 2. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom
– 3. Система защиты информации от несанкционированного доступа "Страж"
– 4. Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом
– 5. Система защиты информации "SecretNet"
– 6. Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ
– 7. Система защиты информации Dallas Lock
– 8. Защита беспроводных сетей стандартов IEEE 802.11
– 9. Исследование методов аналогового скремблирования на базе LabView
– 10. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP
– 11. Защита беспроводных сетей стандартов IEEE 802.15
– 12. Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии
– 13. Защита беспроводных сетей стандартов GSM, CDMA
– 14. Защита беспроводных сетей стандартов WiMAX
– 15. Защита беспроводных сетей стандартов LTE
– 16. Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO
– 17. Формальные политики и математические модели компьютерной безопасности
–
– 18. Организация защиты сетей CISCO
– 19. Обзор и анализ наиболее важных стандартов и спецификаций в области информационной безопасности
–
– 20. Обзор и анализ классических криптографических шифров
– 21. Обзор и анализ симметричных криптографических шифров

Согласована на портале № 22791

– 22. Обзор и анализ ассиметричных криптографических шифров
– 23. Программные комплексы для создания криптовалюты Биткойн
– 24. Алгоритм шифрования данных AES и его программная реализация
– 25. Инфраструктуры открытых ключей PKI

3.5 Темы домашних заданий

– 1. Исследование и разработка методики развертывания и администрирования WEB-сервера на Windows Server 2012
– 2. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom
– 3. Система защиты информации от несанкционированного доступа "Страж"
– 4. Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом
– 5. Система защиты информации "SecretNet"
– 6. Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ
– 7. Система защиты информации Dallas Lock
– 8. Защита беспроводных сетей стандартов IEEE 802.11
– 9. Исследование методов аналогового скремблирования на базе LabView
– 10. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP
– 11. Защита беспроводных сетей стандартов IEEE 802.15
– 12. Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии
– 13. Защита беспроводных сетей стандартов GSM, CDMA
– 14. Защита беспроводных сетей стандартов WiMAX
– 15. Защита беспроводных сетей стандартов LTE
– 16. Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO
– 17. Формальные политики и математические модели компьютерной безопасности
–
– 18. Организация защиты сетей CISCO
– 19. Обзор и анализ наиболее важных стандартов и спецификаций в области информационной безопасности
–
– 20. Обзор и анализ классических криптографических шифров
– 21. Обзор и анализ симметричных криптографических шифров
– 22. Обзор и анализ ассиметричных криптографических шифров
– 23. Программные комплексы для создания криптовалюты Биткойн
– 24. Алгоритм шифрования данных AES и его программная реализация
– 25. Инфраструктуры открытых ключей PKI

3.6 Темы индивидуальных заданий

– 1. Исследование и разработка методики развертывания и администрирования WEB-сервера на Windows Server 2012
– 2. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom
– 3. Система защиты информации от несанкционированного доступа "Страж"
– 4. Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом
– 5. Система защиты информации "SecretNet"
– 6. Методы оценки качества алгоритмов поточного шифрования и программная реализа-

Согласована на портале № 22791

ция статистических тестов НИСТ

– 7. Система защиты информации Dallas Lock

– 8. Защита беспроводных сетей стандартов IEEE 802.11

– 9. Исследование методов аналогового скремблирования на базе LabView

– 10. Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP

– 11. Защита беспроводных сетей стандартов IEEE 802.15

– 12. Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии

– 13. Защита беспроводных сетей стандартов GSM, CDMA

– 14. Защита беспроводных сетей стандартов WiMAX

– 15. Защита беспроводных сетей стандартов LTE

– 16. Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO

– 17. Формальные политики и математические модели компьютерной безопасности

–

– 18. Организация защиты сетей CISCO

– 19. Обзор и анализ наиболее важных стандартов и спецификаций в области информационной безопасности

–

– 20. Обзор и анализ классических криптографических шифров

– 21. Обзор и анализ симметричных криптографических шифров

– 22. Обзор и анализ ассиметричных криптографических шифров

– 23. Программные комплексы для создания криптовалюты Биткойн

– 24. Алгоритм шифрования данных AES и его программная реализация

– 25. Инфраструктуры открытых ключей PKI

3.7 Вопросы на собеседование

– 1.Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?

– 2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

– 3.Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

– 4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?

– 5. Назовите два типа биометрических систем. Назовите основные категории атак.

– 6.Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

– 7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности инфор¬мации.

– 8. Структурированная схема потенциально возможных злоумышлен¬ных действий в автоматизированных системах обработки данных.

– 9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

– 10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификаци

Согласована на портале № 22791

– 11. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости ин¬формации. Допущения в моделях оценки уязвимости информации.

– 12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обуслов¬ленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации.

– 13. Требования к защите, определяемые структурой автоматизирован¬ной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой инфор¬мации. Требования, обусловливаемые взаимодействием пользователя с ком¬плексом средств автоматизации.

– 14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?

– 15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

– 16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?

– 17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

– 18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

– 20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 21. Анализ существующих методик определения требований к защите информации.

– 22. Стандарт США «Критерии оценки гарантировано защищенный вы¬числительных систем в интересах Министерства обороны США». Основные положения. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. 1. Классы защищенности средств вычислительной техники от несанк¬ционированного доступа.

– 23. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи защиты информации. Основные положения меха¬низмов непосредственной защиты и механизмы управления меха¬низмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.

– 24. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?

– 25. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией

– 26. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?

– 27. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?

– 28. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.

– 29. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?

– 30. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

–

– 31. Согласно ГОСТ Р ИСО/МЭК 17799:2005 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?

– 32. Какие основные информационные активы д.б. учтены и закреплены за ответственны-

Согласована на портале № 22791

ми владельцами для обеспечения информационной безопасности организации?

– 34. Ключевые моменты этапа анализа рисков: (перечислите)

– 35. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 36. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

– 37. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?

– 38. Перечислите стандарте ОК 11 классов функциональных требований.

– 39. Как производится вычисление потенциала нападения?

– 40. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 41. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность?

3.8 Темы опросов на занятиях

– Комплексная защита информации в компьютерных системах и сетях

– Криптографические методы и средства защиты информации в компьютерных системах и сетях

– Радиоэлектронные системы и устройства защиты информации

– Безопасность сетевых операционных систем

– Политика и модели безопасности

– Безопасность локальных и глобальных сетевых технологий

3.9 Темы докладов

– Исследование и разработка методики развертывания и администрирования WEB-сервера на Windows Server 2012

– Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet Custom

– Система защиты информации от несанкционированного доступа "Страж"

– Исследование защищенной системы хранения данных на базе программного обеспечения с открытым исходным кодом

– Система защиты информации "SecretNet"

– Методы оценки качества алгоритмов поточного шифрования и программная реализация статистических тестов НИСТ

– Система защиты информации Dallas Lock

– Защита беспроводных сетей стандартов IEEE 802.11

– Исследование методов аналогового скремблирования на базе LabView

– Исследование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения ViPNet CSP

– Защита беспроводных сетей стандартов IEEE 802.15

– Исследование защищенной многоточечной видеоконференц связи на базе WEB-технологии

– Защита беспроводных сетей стандартов GSM, CDMA

– Защита беспроводных сетей стандартов WiMAX

– Защита беспроводных сетей стандартов LTE

– Исследование технологии множественного доступа на базе OFDM-модуляции и технологии MIMO

– Формальные политики и математические модели компьютерной безопасности

–

– Организация защиты сетей CISCO

– Обзор и анализ наиболее важных стандартов и спецификаций в области информацион-

Согласована на портале № 22791

ной безопасности

–

– Обзор и анализ классических криптографических шифров
– Обзор и анализ симметричных криптографических шифров
– Обзор и анализ ассиметричных криптографических шифров
– Программные комплексы для создания криптовалюты Биткойн
– Алгоритм шифрования данных AES и его программная реализация
– Инфраструктуры открытых ключей PKI

3.10 Экзаменационные вопросы

– Экзаменационные вопросы

– 1.Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?

– 2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

– 3.Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

– 4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?

– 5. Назовите два типа биометрических систем. Назовите основные категории атак.

– 6.Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

– 7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности инфор¬мации.

– 8. Структурированная схема потенциально возможных злоумышлен¬ных действий в автоматизированных системах обработки данных.

– 9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

– 10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификаци

– 11. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости ин¬формации. Допущения в моделях оценки уязвимости информации.

– 12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обуслов¬ленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации.

– 13. Требования к защите, определяемые структурой автоматизирован¬ной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой инфор¬мации. Требования, обусловливаемые взаимодействием пользователя с ком¬плексом средств автоматизации.

– 14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?

– 15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

– 16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?

– 17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

– 18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользо-

Согласована на портале № 22791

вательские VPN требуют строгой аутентификации?

– 19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

– 20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 21. Анализ существующих методик определения требований к защите информации.

– 22. Стандарт США «Критерии оценки гарантировано защищенный вы¬числительных систем в интересах Министерства обороны США». Основные положения. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. 1. Классы защищенности средств вычислительной техники от несанк¬ционированного доступа.

– 23. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи защиты информации. Основные положения меха¬низмов непосредственной защиты и механизмы управления меха¬низмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.

– 24. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?

– 25. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией

– 26. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?

– 27. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?

– 28. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.

– 29. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?

– 30. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

–

– 31. Согласно ГОСТ Р ИСО/МЭК 17799:2005 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?

– 32. Какие основные информационные активы д.б. учтены и закреплены за ответственными владельцами для обеспечения информационной безопасности организации?

– 34. Ключевые моменты этапа анализа рисков: (перечислите)

– 35. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 36. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

– 37. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?

– 38. Перечислите стандарте ОК 11 классов функциональных требований.

– 39. Как производится вычисление потенциала нападения?

– 40. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 41. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность?

3.11 Темы контрольных работ

– КОНТРОЛЬНАЯ_РАБОТА_2015 Ст./гр._____

– 1. Что такое информационная безопасность? Какие компоненты входят в информацион-

Согласована на портале № 22791

ную безопасность?

– 2. Назовите два типа биометрических систем. Назовите основные категории атак.

– 3. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

– 4. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная? Зачем нужен аудит?

– 5. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?

– 6. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

– 7. Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?

– 8. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?

– 9. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?

– 10. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?

– 11. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

– 12. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 13. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

– 14. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 15. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

– 16. Почему процесс реализации VPN представляет собой гораздо большее, чем выбор алгоритма шифрования? Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

– 17. Может ли быть взломан правильно реализованный "одноразовый блокнот"? Какую длину имеют ключи DES?

– 18. В чем заключается основной недостаток DES? За счет чего тройной DES повышает уровень безопасности алгоритма DES?

– 19. Для чего предназначен алгоритм AES? На сложности какой задачи базируется безопасность, обеспечиваемая алгоритмом Диффи-Хеллмана?

– 20. Что такое цифровая подпись? Почему открытые ключи должны быть сертифицированными?

3.12 Вопросы для подготовки к практическим занятиям, семинарам

– Комплексная защита информации в компьютерных системах и сетях

– Криптографические методы и средства защиты информации в компьютерных системах и сетях

– Радиоэлектронные системы и устройства защиты информации

– Безопасность сетевых операционных систем

– Политика и модели безопасности

– Безопасность локальных и глобальных сетевых технологий

3.13 Вопросы дифференцированного зачета

– 1.Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осу-

Согласована на портале № 22791

ществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?

– 2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

– 3.Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

– 4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?

– 5. Назовите два типа биометрических систем. Назовите основные категории атак.

– 6.Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

– 7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности инфор¬мации.

– 8. Структурированная схема потенциально возможных злоумышлен¬ных действий в автоматизированных системах обработки данных.

– 9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?

– 10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификаци

– 11. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости ин¬формации. Допущения в моделях оценки уязвимости информации.

– 12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обуслов¬ленные спецификой автоматизированной обработки информации. Классификация требований к средствам защиты информации.

– 13. Требования к защите, определяемые структурой автоматизирован¬ной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой инфор¬мации. Требования, обусловливаемые взаимодействием пользователя с ком¬плексом средств автоматизации.

– 14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?

– 15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

– 16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?

– 17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

– 18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?

– 20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 21. Анализ существующих методик определения требований к защите информации.

– 22. Стандарт США «Критерии оценки гарантировано защищенный вы¬числительных систем в интересах Министерства обороны США». Основные положения. О Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. 1. Классы защищенности средств вычислительной техники от несанк¬ционированного доступа.

– 23. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи

Согласована на портале № 22791

защиты информации. Основные положения меха¬низмов непосредственной защиты и механизмы управления меха¬низмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.

– 24. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?

– 25. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией

– 26. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?

– 27. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?

– 28. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.

– 29. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?

– 30. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?

–

– 31. Согласно ГОСТ Р ИСО/МЭК 17799:2005 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?

– 32. Какие основные информационные активы д.б. учтены и закреплены за ответственными владельцами для обеспечения информационной безопасности организации?

– 34. Ключевые моменты этапа анализа рисков: (перечислите)

– 35. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?

– 36. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?

– 37. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?

– 38. Перечислите стандарте ОК 11 классов функциональных требований.

– 39. Как производится вычисление потенциала нападения?

– 40. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

– 41. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность?

3.14 Темы расчетных работ

– Криптографические методы и средства защиты информации в компьютерных системах и сетях

– Безопасность сетевых операционных систем

– Политика и модели безопасности

3.15 Темы лабораторных работ

– Изучение международного стандарта безопасности информационных систем ISO 17799

– Система анализа рисков и проверки политики информационной безопасности предприятия

– Исследование системы защиты информации «Страж NT»

– Система защиты информации SecretNet

– Система защиты информации Dallas

– Энергетическое скрытие речевой информации (с использованием звуковой карты и звукового редактора ПЭВМ).

Согласована на портале № 22791

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Защита информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7072, свободный.

4.2. Дополнительная литература

1. Защита информации в инфокоммуникационных системах и сетях: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 655 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7079, свободный.

4.3. Обязательные учебно-методические пособия

1. Защита информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7072, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. Яндекс

Согласована на портале № 22791