МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА 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) / специализация: **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 2018

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Согласована на портале № 24570

Рассмотрена и одобрена на заседании кафедры
протокол № 9 от «26» 4 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.05.01 Радиоэлектронные системы и комплексы, утвержденного 11.08.2016 года, рассмотрена и одобрена на заседании кафедры РТС «___» _____ 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 дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РТС _____ С. В. Мелихов

Эксперты:

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

Доцент кафедры радиотехнических систем (РТС) _____ В. А. Громов

Согласована на портале № 24570

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.31.1) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Введение в специальность, Информационные технологии 2. Сетевые информационные технологии. Базы данных., Научно-исследовательская работа, 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, Практика по получению профессиональных умений и опыта профессиональной деятельности, 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 обучающийся 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 № 24570

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	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	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
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	8	2	0	4	14	ПСК-2.1
6 Методология построения и анализа	4	0	0	4	8	ПСК-2.1

Согласована на портале № 24570

систем обеспечения информационной безопасности						
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 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,	4	ПСК-2.1

Согласована на портале № 24570

	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
	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	8	ПСК-2.1

Согласована на портале № 24570

	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.		
	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 требованиями «Оранжевой книги». Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности. Рекомендации по самостоятельному углубленному изучению разделов курса. Обзор литературы.	4	ПСК-2.1
	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 оп-	4	ПСК-2.1

Согласована на портале № 24570

	тических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.		
	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 Научно-исследовательская работа			+	+		+	+
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	+		+				+
3 Моделирование в радиоэлектронных системах передачи информации			+			+	+
4 Практика по получению профессиональных умений и опыта профессиональной деятельности			+			+	+
5 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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	

Согласована на портале № 24570

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			
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

Согласована на портале № 24570

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 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		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	Проработка лекционного материала	2	ПСК-2.1	Выступление (доклад) на занятии, Домашнее задание, Защита от-
	Итого	2		

Согласована на портале № 24570

национальной безопасности Российской Федерации				чета, Конспект самоподготовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Расчетная работа, Реферат, Тест, Экзамен
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 информации	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Выступление (доклад) на занятии, Дифференцированный зачет, 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, Собеседование, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	8		
4 Основы комплексного обеспечения	Подготовка к практическим занятиям, семинарам	2	ПСК-2.1	Домашнее задание, Защита отчета, Конспект самопод-

Согласована на портале № 24570

информационной безопасности в радиоэлектронных системах передачи	Проработка лекционного материала	2		готовки, Контрольная работа, Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Отчет по практическому занятию, Реферат, Тест, Экзамен
	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 эк-	36		Экзамен

Согласована на портале № 24570

	замена			
Итого		72		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

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			4	4
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	2	6
Расчетная работа			4	4
Реферат			4	4
Собеседование		2	2	4
Тест	2	2	2	6
Итого максимум за период	6	24	40	70
Экзамен				30
Нарастающим итогом	6	30	70	100

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

Согласована на портале № 24570

< 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 [Электронный ресурс]: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. — Режим доступа: https://edu.tusur.ru/publications/7072 (дата обращения: 05.06.2018).

12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / Голиков А. М. - 2015. 256 с. — Режим доступа: https://edu.tusur.ru/publications/5263 (дата обращения: 05.06.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации в радиоэлектронных системах передачи информации [Электронный ресурс]: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. — Режим доступа: https://edu.tusur.ru/publications/7072 (дата обращения: 05.06.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются 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.

Согласована на портале № 24570

12.4. Профессиональные базы данных и информационные справочные системы

1. Яндекс

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное 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 демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Free Pascal
- Free Pascal Lazarus (версия 1.6)
- GIMP
- Google Chrome
- Microsoft Windows Server 2008
- Microsoft Windows XP
- Mozilla Firefox
- OpenOffice
- Opera
- Opera Developer
- PTC Mathcad13, 14
- Scilab

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);

Согласована на портале № 24570

- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Microsoft Windows XP
– PTC Mathcad 13, 14

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:
- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **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 комфортного просмотра.

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

Согласована на портале № 24570

14.1.1. Тестовые задания

1. Какие три основные составляющие информационной безопасности вам известны?

- зашифрованность, целостность, доступность
- конфиденциальность, закрытость, доступность
- конфиденциальность, целостность, защищенность
• конфиденциальность, целостность, доступность

2. Чем характеризуются, согласно «Оранжевой книге», уровни безопасности С, В, А?

• произвольным управлением доступом, принудительным управлением доступом, верифицируемой безопасностью
- принудительным управлением доступом, произвольным управлением доступом, верифицируемой безопасностью
- верифицируемой безопасностью, произвольным управлением доступом, ролевым управлением доступом
- ролевым управлением доступом, принудительным управлением доступом, верифицируемой безопасностью

3. Какие классы АС наиболее защищены, согласно руководящим документам Гостехкомиссии РФ:

- 3Б и 3А
- 2Б и 2А
- 1Д, 1Г, 1В
• 1Б, 1А

4. Какая модель является моделью произвольного (дискреционного) управлению доступом?

- Модель Белла - ЛаПадула
- Модель Биба
• Хиррисона–Руззо-Ульмана
- Модель Кларка - Вилсона

5. Какая модель является моделью мандатного управлению доступом?

• Модель Белла - ЛаПадула
- Модель Биба
- Хиррисона–Руззо-Ульмана
- Модель Кларка - Вилсона

6. Перечислите три основных вида угроз информационной безопасности

- угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения защищенности
• угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения доступности
- угроза нарушения конфиденциальности, угроза нарушения закрытости, угроза нарушения доступности
- угроза нарушения зашифрованности, угроза нарушения целостности, угроза нарушения доступности

7. Что такое политика безопасности?

- основные положения информационной безопасности
- цели и задачи обеспечения информационной безопасности
• систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.
- распределение ролей и ответственности

8. На каком уровне рассматривается управление рисками (или их анализ) при формирования политики предприятия?

- на процедурном уровне
• на административном уровне
- на уровне управления персоналом
- на уровне физической защиты

9. Назовите физические метода биометрической аутентификации

• распознавание черт лица

Согласована на портале № 24570

- анализ подписи
- анализ тембра голоса
- анализ почерка

10.Какая аутентификация наиболее сильная?

• цифровая подпись
- пароль
- биометрическая
- уникальный предмет

11. Какие два основных вида требований безопасности содержат «Общие критерии»

- требованиях безопасности, проектирование и разработка
- использование ресурсов, криптографическая поддержка
- оценка уязвимостей, оценка задания по безопасности
• функциональные, требования доверия

12. Какие межсетевые экраны используют на границе локальной сети и сети Интернет?

- коммутаторы, функционирующие на канальном уровне
- сетевые или пакетные фильтры
• шлюзы сеансового уровня (circuit-level proxy);
- пакетные фильтры

13. Какой вариант VPN позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь)

• Вариант "Remote Access VPN",
- Вариант «Intranet VPN»,
- Вариант «Client/Server VPN»,
- вариант «Extranet VPN»

14. Укажите какой шифр является поточным?

• RC6
- DES
- AES
- RSA

15. Сколько ключей используют блочные, поточные, ассиметричные алгоритмы шифрования?

• 1, 1, 2
- 2, 1, 3
- 3, 2 1
- 2, 2, 1

16. Какие методы защиты информации используются в стандарте IEEE802.11 (WiFi)?

- PAW, EWR
- WER, WAP
- PEW, APW
• WEP, WPA

17. Какие шифры используются в стандарте GSM?

- не используются
• поточные
- блочные
- с открытым ключем

18. Что является источником побочные электромагнитные излучения и наводки (ПЭМИН), используемых радиотехнической разведкой

- автомобильный транспорт
- электрический транспорт
• радиоэлектронная аппаратура
- линии электропередач

19. Какие виды скремблеров являются наиболее защищенными

Согласована на портале № 24570

- временные
- частотные
- комбинированные
• поточные

20. Какой диапазон частот используется в стеганографии (создании стега) акустического канала

• 50 - 300 Гц
- 300 - 3400 Гц
- 50 - 1800 Гц
- 0 - 20000 Гц

14.1.2. 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 пользова-

Согласована на портале № 24570

тельские 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?

14.1.3. Темы опросов на занятиях

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,

Согласована на портале № 24570

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.

Основные понятия теории компьютерной безопасности. Понятие информации, информационной безопасности АС. Субъектно-объектная модель информационной системы. Основные определения. Язык. Объекты. Субъекты. Доступ. Информационный поток. Монитор безопасности. Ядро безопасности. Иерархические модели вычислительных систем и модель взаимодействия открытых систем (OSI/ISO). Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

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

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

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.

14.1.4. 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

Согласована на портале № 24570

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

14.1.5. 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

14.1.6. 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"

Согласована на портале № 24570

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

14.1.7. 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

11. Методологические подходы к оценке уязвимости информации. Модель защиты системы с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости ин¬форма-

Согласована на портале № 24570

ции. 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 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?

Согласована на портале № 24570

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?

14.1.8. 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
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

14.1.9. 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

Согласована на портале № 24570

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 информационной 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

14.1.10. 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]

14.1.11. Темы контрольных работ

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 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?

Согласована на портале № 24570

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?

14.1.12. Вопросы для подготовки к практическим занятиям, семинарам

Стандарты информационной безопасности и критерии оценки безопасности компьютерных систем и сетей

Разработка архитектуры модели безопасности информационных систем и сетей

Разработка практических рекомендаций по обеспечению безопасности информационных систем

Законодательство в области информационной безопасности

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.

14.1.13. Вопросы дифференцированного зачета

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

Согласована на портале № 24570

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 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 учи-

Согласована на портале № 24570

тывать 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?

14.1.14. Темы расчетных работ

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.

14.1.15. 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).

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Согласована на портале № 24570

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	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 материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов 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.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся 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 лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает 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 лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 24570