МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИСТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ
Заведующий кафедрой РТС
_____Г.С. Шарыгин

_____

ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН

Методическое пособие для специальности 090106 «Информационная безопасность телекоммуникационных систем»

Разработчик
Доцент каф. РТС
_____ А.М. Голиков

_____

Томск - 2012

Рекомендовано к изданию кафедрой радиотехнических систем Томского государственного университета систем управления и радиоэлектроники

Голиков А.М. Государственный экзамен. Методическое пособие для специальности 090106 «Информационная безопасность телекоммуникационных систем». – Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2012.- 34 с.

Приводятся указания по подготовке и проведению «Государственного экзамена» для студентов специальности 09106 Информационная безопасность телекоммуникационных систем.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Государственным образовательным стандартом по специальности 075600 (090106) «Информационная безопасность телекоммуникационных систем», утвержденной приказом Министерства образования Российской Федерации № 686 от 2 марта 2000 года, предусмотрена государственная аттестация выпускников в виде:

- защиты выпускной квалификационной работы;
- государственного экзамена.

Государственный экзамен по специальности проводится в соответствии с ГОС и «Положением об итоговой государственной аттестации выпускников высших учебных заведений в Российской Федерации", утвержденном Минобразованием РФ (приказ №1155 от 25.03.2003). Порядок проведения и программа государственного экзамена определяются вузом на основании ГОС, действующего учебного плана и рекомендаций, разработанных УМО.

2. ОПРЕДЕЛЕНИЕ СОДЕРЖАНИЯ ГОСУДАРСТВЕННЫХ ИСПЫТАНИЙ

2.1. Виды деятельности выпускников и соответствующие им задачи профессиональной деятельности

Виды деятельности выпускников и соответствующие им задачи профессиональной деятельности определены ГОСом.

Объектами профессиональной деятельности специалиста по защите информации по специальности 090106 «Информационная безопасность телекоммуникационных систем» являются методы, средства и системы обеспечения информационной безопасности телекоммуникационных систем.

Специалист по защите информации в соответствии с фундаментальной и специальной подготовкой может выполнять следующие виды профессиональной деятельности:

- экспериментально-исследовательская;
- проектная;
- организационно-управленческая;
- эксплуатационная.

2.2. Соответствие профессиональных функций и требований к подготовке выпускника

В таблице 1 определено соответствие требований ГОС к профессиональной подготовленности различным видам профессиональной деятельности выпускников.

Таблица 1

Требования ГОС к профессиональной подготовленности выпускника	**Виды профессиональной деятельности**			
	Эксплуатационная.	**Проектная**	Экспериментально-**исследовательская**	**Организационно – управленческая**
Специалист по защите информации подготовлен к решению следующих типов задач:				
- сопровождение разработки и исследование специальных технических и программно-аппаратных средств защиты и обработки информации в телекоммуникационных системах; разработка модели информационной безопасности телекоммуникационных систем;			+	
- подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам обеспечения информационной безопасности телекоммуникационных систем; построение и анализ защищенных систем и сетей передачи информации;			+	

- составление информационных обзоров по вопросам комплексного обеспечения информационной безопасности телекоммуникационных систем;			+	
- алгоритмизация и программирование типовых криптосхем; проведение сравнительного анализа систем и сетей передачи информации общего и специального назначения по показателям информационной безопасности;		+		
- сопровождение разработки технического обеспечения системы информационной безопасности; участие в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации;		+		
- рациональный выбор соответствующих электронных и полупроводниковых приборов при разработке радиоэлектронной аппаратуры и составление заявок на необходимые материалы, оборудование, приборы		+		
- осуществление организационно-правового и инженерно-технического обеспечения защиты информации; проведение проверок учреждений, организаций и предприятий по выполнению требований правовых норм и стандартов, касающихся лицензирования и сертификации в области информационной безопасности, нормативно-технической документации по защите информации, участие в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию;				+

- подготовка предложений по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации; проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;				+
- разработка предложений по совершенствованию и повышению эффективности принимаемых технических мер и организационных мероприятий; изучение и обобщение опыта работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации в телекоммуникационных системах с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны;				+
- эксплуатация специальных технических и программно-аппаратных средств защищенных телекоммуникационных систем;	+			
- составление методик расчетов и программ экспериментальных исследований по технической защите информации, выполнение расчетов в соответствии с разработанными методиками и программами;	+			
- сопоставительный анализ данных исследований и испытаний, изучение возможных источников и каналов утечки информации;	+			
- оценка технических возможностей сетей передачи информации общего и специального назначения;	+			

- выполнение оперативных заданий, связанных с обеспечением контроля технических средств и механизмов системы защиты информации;	+			
- проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.	+			

2.3. Требования к профессиональной подготовленности выпускника, необходимые для выполнения им профессиональных функций, и соответствующие виды государственных аттестационных испытаний

В таблице 2 определены возможности использования различных видов итоговой аттестации для определения соответствия требованиям ГОС.

Таблица 2

Требования ГОС к профессиональной подготовленности выпускника	**Вид аттестационного испытания**		**Примечание**
	Госуд. экзамен	**Защита ВКР**	
Специалист по защите информации должен уметь:			
- решать типовые задачи линейной алгебры, дифференциального и интегрального исчисления, а также теории функций комплексного переменного; исследовать простейшие геометрические объекты по их уравнениям в различных системах координат;		+	Текущ. аттест.

- применять стандартные методы и модели к решению типовых теорико-вероятностных задач и стандартных задач математической статистики; определять погрешности вычислений и применять численные методы для решения практических задач с использованием стандартных пакетов;	+	+	Текущ. аттест.
- применять на практике знание основных законов общей физики и оценивать численные порядки величин, характерных для различных разделов естествознания;	+	+	Текущ. аттест.
- работать на современных ПЭВМ на уровне пользователя и использовать современные средства разработки программного обеспечения;		+	Текущ. аттест.
- анализировать и оценивать степень экологической опасности антропогенного воздействия на окружающую природную среду;		+	Текущ. аттест.
- использовать методы дискретной математики при решении практических задач;		+	Текущ. аттест.
- оценивать скорость передачи информации и пропускную способность каналов передачи информации при отсутствии и наличии помех, а также применять знания о кодах, корректирующие ошибки;	+	+	Текущ. аттест.
- применять системный подход к обеспечению информационной безопасности телекоммуникационных систем; разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные криптографические алгоритмы и протоколы;	+	+	Текущ. аттест.
- использовать типовые методы криптографического анализа; практически решать задачи защиты программ и данных;	+	+	Текущ. аттест.
- определять параметры сигналов утечки информации по техническим каналам, организовывать и проводить мero-		+	Текущ. аттест.

приятия технического контроля; использовать правовые акты в области информационной безопасности;			
- использовать знания о структуре и особенностях построения современных ЭВМ, микропроцессоров и операционных систем при разработке прикладных программ; реализовывать основные структуры данных и основные алгоритмы сортировки и поиска на языках программирования высокого уровня; анализировать основные механизмы, реализованные в современных операционных системах;		+	Текущ. аттест.
- использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем; использовать методы теории массового обслуживания для анализа эффективности телекоммуникационных систем;		+	Текущ. аттест.
- использовать методы планирования и оптимизации экспериментов с моделями с помощью ПЭВМ; рассчитывать и экспериментально анализировать параметры основных видов электрических цепей;		+	Текущ. аттест.
- решать волновые уравнения и простейшие краевые задачи; рассчитывать параметры электродинамических направляющих систем, решать дисперсионные уравнения;		+	Текущ. аттест.
- проводить анализ помехоустойчивости, эффективности и оптимальности построения защищенных телекоммуникационных систем;	+	+	Текущ. аттест.
- осуществлять рациональный выбор соответствующих электронных и полупроводниковых приборов при разработке радиоэлектронной аппаратуры и оконечных устройств телекоммуникационных систем; работать с чертежами и схемами в соответствии с требованиями государ-		+	Текущ. аттест.

ственных стандартов; проводить измерения параметров элементов радиотехнических цепей и сигналов, оценивать погрешности измерений;			
- применять методики управления деятельностью коллектива при решении практических задач; создавать оптимальное (нормативное) состояние среды обитания в зонах трудовой деятельности и отдыха человека;		+	Текущ. аттест.
- оценивать технические возможности и вырабатывать рекомендации по построению систем и сетей передачи информации общего и специального назначения; рассчитывать характеристики и выбирать элементы типовых оконечных устройств, устройств синхронизации и преобразования сигналов телекоммуникационных систем.	+	+	Текущ. аттест.

2.4. Основные дисциплины, позволяющие определить соответствие требованиям ГОС в процессе государственного экзамена

В таблице 3 определены основные дисциплины образовательной профессиональной программы по циклам общепрофессиональных и специальных дисциплин, контроль усвоения которых позволяет определить соответствие требованиям ГОС в процессе итоговой аттестации.

Таблица 3

Требования ГОС к профессиональной подготовленности выпускника	**Дисциплины образовательной программы (разделы)**									**Примечание**
	Теория электрической связи	**Безопасность жизнедеятельности**	**Основы управленческой деятельности**	**Электродинамика и распространение радиоволн**	**Технические средства и методы защиты информации**	**Передача дискретных сообщений**	**Основы информационной безопасности**	**Программно-аппаратные средства обеспечения информационной безопасности**	**Метрология и электрорадиоизмерения в телекоммуникационных**	
Специалист по защите информации должен уметь:										
- решать типовые задачи линейной алгебры, дифференциального и интегрального исчисления, а также теории функций комплексного переменного; исследовать простейшие геометрические объекты по их уравнениям в различных системах координат;	+			+		+				

- применять стандартные методы и модели к решению типовых теорико-вероятностных задач и стандартных задач математической статистики; определять погрешности вычислений и применять численные методы для решения практических задач с использованием стандартных пакетов;	+		+			+			+	
- применять на практике знание основных законов общей физики и оценивать численные порядки величин, характерных для различных разделов естествознания;	+	+		+	+	+			+	
- работать на современных ПЭВМ на уровне пользователя и использовать современные средства разработки программного обеспечения;	+			+	+	+	+	+	+	
- анализировать и оценивать степень экологической опасности антропогенного воздействия на окружающую природную среду;		+								

- использовать методы дискретной математики при решении практических задач;							+	+		
- оценивать скорость передачи информации и пропускную способность каналов передачи информации при отсутствии и наличии помех, а также применять знания о кодах, корректирующие ошибки;	+					+				
- применять системный подход к обеспечению информационной безопасности телекоммуникационных систем; разрабатывать модели информационной безопасности телекоммуникационных систем, использовать стандартные криптографические алгоритмы и протоколы;					+	+	+	+		
- использовать типовые методы криптографического анализа; практически решать задачи защиты программ и данных;							+	+		

- определять параметры сигналов утечки информации по техническим каналам, организовывать и проводить мероприятия технического контроля; использовать правовые акты в области информационной безопасности;					+		+			
- использовать знания о структуре и особенностях построения современных ЭВМ, микропроцессоров и операционных систем при разработке прикладных программ; реализовывать основные структуры данных и основные алгоритмы сортировки и поиска на языках программирования высокого уровня; анализировать основные механизмы, реализованные в современных операционных системах;					+		+			

- использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем; использовать методы теории массового обслуживания для анализа эффективности телекоммуникационных систем;	+			+		+		+		
- использовать методы планирования и оптимизации экспериментов с моделями с помощью ПЭВМ; рассчитывать и экспериментально анализировать параметры основных видов электрических цепей;	+		+						+	
- решать волновые уравнения и простейшие краевые задачи; рассчитывать параметры электродинамических направляющих систем, решать дисперсионные уравнения;			+			+				
- проводить анализ помехоустойчивости, эффективности и оптимальности построения защищенных телекоммуникационных систем;	+					+				

- осуществлять рациональный выбор соответствующих электронных и полупроводниковых приборов при разработке радиоэлектронной аппаратуры и оконечных устройств телекоммуникационных систем; работать с чертежами и схемами в соответствии с требованиями государственных стандартов; проводить измерения параметров элементов радиотехнических цепей и сигналов, оценивать погрешности измерений;	+					+			+	
- применять методики управления деятельностью коллектива при решении практических задач; создавать оптимальное (нормативное) состояние среды обитания в зонах трудовой деятельности и отдыха человека;		+	+	+	+					

- оценивать технические возможности и вырабатывать рекомендации по построению систем и сетей передачи информации общего и специального назначения; рассчитывать характеристики и выбирать элементы типовых оконечных устройств, устройств синхронизации и преобразования сигналов телекоммуникационных систем	+			+	+	+		+	+	

3. ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН ПО СПЕЦИАЛЬНОСТИ. ОБЩИЕ ПОЛОЖЕНИЯ

Государственный экзамен по специальности проводится в соответствии с ГОС и «Положением об итоговой государственной аттестации выпускников высших учебных заведений в Российской Федерации", утвержденном Минобразованием РФ (приказ №1155 от 25.03.2003). Порядок проведения и программа государственного экзамена определяются вузом на основании соответствующего ГОС, действующего учебного плана и рекомендаций, разработанных УМО.

Всю организационную работу по подготовке и проведению экзамена проводит деканат совместно с кафедрами, привлекаемыми к его проведению.

УМО формулирует следующие общие рекомендации по организации и проведению государственного экзамена по специальности:

- - экзамен носит междисциплинарный характер и проводится с привлечением не менее трех дисциплин из специального и, при необходимости, общепрофессионального циклов дисциплин, устанавливаемых советом факультета, обеспечивающего подготовку по данной специальности;

- - программа экзамена и варианты заданий утверждаются деканом факультета, а состав экзаменационной комиссии и ее председатель - ректором вуза;
- - студенты допускаются к междисциплинарному экзамену только после успешной сдачи экзаменационной сессии;
- - до проведения экзамена в соответствии с расписанием, утвержденным ректором, и учебной нагрузкой соответствующих кафедр проводится специальная подготовка, включающая чтение установочных лекций, проведение практических занятий и консультаций;
- - экзамен проводится в письменном виде, причем каждый студент выполняет индивидуальное задание;
- - задание включает одну (комплексного характера) или несколько задач, требующих конкретных решений и представляющих собой небольшие инженерные задачи, решение которых позволяет оценить соответствие подготовки выпускников требованиям ГОС в области их умений и навыков, причем объем заданий должен быть рассчитан на время проведения экзамена в течение не более 4-х академических часов;
- - содержание заданий должно быть по возможности приближено к задачам, решаемым студентами в процессе выполнения курсовых проектов и работ, на практических занятиях и в рамках индивидуальной работы в процессе реализации соответствующего ГОС;
- - на экзамене студентам, наряду с конспектами лекций, разрешается пользоваться учебно-методической, научно-технической и справочной литературой, рекомендованной соответствующими кафедрами, и техническими средствами расчета и оформления выполнения задания;
- - результаты экзамена (с выставлением оценок “отлично”, “хорошо”, “удовлетворительно” и “ неудовлетворительно”) проставляются в экзаменационную ведомость и в зачетную книжку за подписью председателя комиссии и ее членов. При принятии решения по экзаменационной оценке учитывается не только правильность полученных результатов, но и оформление работы (наличие кратких пояснений к расчетным формулам и принимаемым решениям, грамотное использование размерностей величин и степени округления результатов расчетов, анализ полученных результатов и т.п.),

причем для получения положительной оценки должны быть правильно решены не менее 50% задач;

- - студенты имеют право на апелляцию, причем заявления на проведение апелляции на имя председателя комиссии подаются в день объявления результатов;
- - кафедрам, участвующим в проведении экзамена, целесообразно осуществить подготовку и издание соответствующих внутривузовских учебно-методических
- пособий и (или) указаний.
- - образцы решения экзаменационных заданий (5-10 экз.) должны храниться в деканате не менее одного года для предоставления (в случае необходимости) органам, контролирующим или аттестующим данную специальность.

3. ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОСТИ 090106 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Проведение государственного экзамена по специальности 090106 – Информационная безопасность телекоммуникационных систем ориентированно на следующие дисциплины:

из общепрофессионального блока дисциплин:

- ОПД.Ф.02 Основы информационной безопасности;
- ОПД.Ф.04 Программно-аппаратные средства обеспечения информационной безопасности;
- ОПД.Ф.14 Теория электрической связи;

из блока специальных дисциплин:

- ДС.02 Передача дискретных сообщений.

3.1. Перечень вопросов по дисциплине «Основы информационной безопасности»

Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности. Основные понятия теории компьютерной безопасности**.** Понятие информации, информационной безопасности АС. Субъектно-объектная модель информационной

системы. Основные определения. Язык. Объекты. Субъекты. Доступ. Информационный поток. Монитор безопасности. Ядро безопасности. Иерархические модели вычислительных систем и модель взаимодействия открытых систем (*OSI/ISO*). Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.

Методы и средства обеспечения информационной безопасности. 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.

Основы комплексного обеспечения информационной безопасности. Модели, стратегии (политики) и системы обеспечения информационной безопасности. 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. 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.

Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей. 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.

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 (*TCB*).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

Рекомендуемая литература.

1. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000. – 192 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.

3.2. Перечень вопросов по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

Подсистемы защиты в современных ОС. Подсистема защиты информации в ОС UNIX. Основные компоненты подсистемы защиты UNIX. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах. Подсистема защиты информации в ОС Windows NT. Основные компоненты подсистемы защиты Windows NT и Windows 2000. Политики. Понятие домена. Особенности установления доверительных отношений. Создание и удаление бюджетов пользователей. Защита информации при интеграции UNIX и Windows NT. Основы взаимодействия элементов гетерогенных сетей. Шлюзы NFS. SMB в UNIX. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows NT. Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Защита программ. Защита программ от изучения. Защита от разрушающих программных воздействий. Защита от изменения и контроль целостности.

Защита информации в вычислительных системах и сетях. Атаки на сетевые службы. Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры. Особенности сетевого сканера Nessus. Адаптивная безопасность в ВС. Понятие адаптивной безопасности и системы обнаружения атак. Классификация по используемым механизмам обнаружения атак, и по принципам их практической реализации. Особенности применения различных типов систем обнаружения атак. Особенности существующих свободно-распространяемых систем обнаружения атак. Межсетевые экраны. Понятие межсетевых экранов. Их классификация. Основные примеры конфигурации защищенных сетей с использованием МЭ. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов. Удалённый доступ к сети. Проблемы обеспечения безопасности при удалённом доступе. Протоколы аутентификации PAP и CHAP. Протоколы аутентификации удалённого доступа в программных средствах Microsoft. Система аутентификации и авторизации TACACS и Kerberos. Виртуальные частные сети. Понятие виртуальной частной сети, её предназначение. Стандартные возможности каналообразующего обору-

дования различных производителей. Основные принципы функционирования и использования протокола PPTP. Реализация в программных средствах Microsoft. Политика безопасности Понятие политики информационной безопасности для организации. Основные требования к политике безопасности. Этапы её разработки.

Рекомендуемая литература.

1. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности: Защита в операционных системах. — М.: Радио и связь, 2000.
2. Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие // Томск, ТМЦДО, 2004. - 118 с.

3.3. Перечень вопросов по дисциплине «Теория электрической связи»

Информация и сигнал как ее материальный носитель. Случайный характер сообщений и сигналов. Системы передачи, хранения и распределения информации. Структурная схема системы передачи информации (СПИ). Линия связи с помехами, функции передатчика и приемника. Статистический анализ и синтез СПИ. Системы распределения информации. Многоканальная связь и многостанционный доступ, сети электросвязи как системы массового обслуживания.

Математические модели сигналов и помех. Вероятностное описание последовательности символов. Примеры цифровых сигналов. Дискретные сигналы. Последовательность гауссовских случайных величин. Непрерывные сигналы. Стационарный гауссовский случайный процесс, числовые характеристики. Белый шум. Случайное поле. Примеры непрерывных сигналов. Аддитивные и мультипликативные помехи. Канал многолучевого распространения волн как фильтр со случайно изменяющимися параметрами.

Преобразование сигналов в каналах связи. Основные задачи кодирования: сокращение избыточности, повышение помехоустойчивости, скрытности, криптоустойчивости. Квантование во времени непрерывных сигналов, ошибки квантования. АЦП и ЦАП. Компрессия сигнала. Модуляция несущей аналоговым сигналом: АМ, АМ с подавленной несущей, однополосная АМ, ЧМ. Спектры модулированных сигналов и полоса частот, требуемая для передачи. Модуляция импульсной несущей дискретным сигналом: АИМ, ШИМ, ВИМ. Способы

модуляции в цифровых СПИ: АМ, ЧМ, ФМ, ОФМ. Многопозиционные методы модуляции. Спектры модулированных сигналов, межсимвольная интерференция. Геометрическое представление сигналов и помех.

Помехоустойчивое и криптоустойчивое кодирование в цифровых системах передачи информации. Принципы помехоустойчивого кодирования. Блочные корректирующие коды. Обнаружение и исправление ошибок. Кодовое расстояние. Блочные линейные коды. Коды Хемминга, Рида-Малера. Циклические коды. Способы кодирования и декодирования циклических кодов. Коды БЧХ, коды Рида-Соломона. Сверточные коды (СК). Пороговое декодирование. Декодирование по методу Витерби. Декодирование с мягким решением. Группирование ошибок, перемежение символов при кодировании, применение циклических и сверточных кодов. Предельные возможности помехоустойчивого кодирования. Помехоустойчивость систем с обратной связью (ОС). Теоретико-информационная концепция криптозащиты сообщений в телекоммуникационных системах. Модель и основные понятия секретной связи. Алгоритмика классических криптосистем с секретными ключами. Двухключевая теоретико-числовая криптосистема RSA.

Основы теории информации. Собственная информация, энтропия. Избыточность и ее роль. Кодирование в цифровых каналах без помех. Коды Шеннона-Фано, Хафмана, Лемпела-Зива. Цифровые каналы с помехами. Скорость создания и скорость передачи информации. Пропускная способность двоичного симметричного канала. Теоремы Шеннона о кодировании в дискретном канале с помехами. Информация в непрерывных сигналах. Дифференциальная энтропия непрерывного отсчета. Пропускная способность непрерывного канала с аддитивным белым гауссовским шумом, формула Шеннона.

Оптимальный прием сигналов и основы теории помехоустойчивости. Когерентные и некогерентные системы передачи информации. Решающая схема, построенная по правилу максимума апостериорной вероятности. Оптимальный прием в канале с постоянными параметрами при наличии аддитивного белого шума, вероятность ошибки. Относительная фазовая модуляция. Вероятность ошибки при приеме многопозиционных сигналов. Разнесенный прием. Регенерация цифрового сигнала в ретрансляторах. Среднеквадратическая ошибка при приеме отсчетов непрерывного сигнала, неравенство Рао-Крамера, аномальные ошибки.

Методы многоканальной связи и многостанционного доступа. Основные положения теории разделения сигналов в системах многоканальной связи. Многостанционный доступ с

ЧРК, ВРК, кодовым разделением каналов. Междуканальные помехи. Синхронный и асинхронный методы передачи в цифровых многоканальных системах. Иерархии цифровых систем.

Принципы распределения информации. Сети и системы обмена информацией. Классификация сетей, каналов, линий. Структуры сетей. Кабельные сети и сети радиосвязи: релейная передача, электромагнитная совместимость, принцип повторного использования частот, общая синхронизация. Коммутация каналов и коммутация пакетов: сравнительный анализ. Классификация гибридных методов. Современные технологии синхронного и асинхронного обмена информацией в сетях: контейнерная передача, виртуальные каналы и виртуальные пути, маршрутизация и коммутация, защита от ошибок. Примеры: ATM , Frame Relay. Основные положения теории массового обслуживания. Структура систем распределения информации. Многоуровневая архитектура связи и протоколы.

Рекомендуемая литература.

1. Теория электрической связи: Учебник для вузов/ Зюко А.Г., Кловский Д.Д., Коржик В.И., Назаров М.В. - М.: Радио и связь, 1999. - 432 с.

3. Акулиничев Ю.П. Теория электрической связи. Часть 1: Учебное пособие. - Томск, ТМЦДО, 2005. – 127 с.

3.4. Перечень вопросов по дисциплине «Передача дискретных сообщений»

Краткая характеристика преобразований, которым подвергаются сигналы в процессе их передачи в цифровых системах передачи информации (ЦСПИ). Основные отличия цифровых и аналоговых методов передачи. Обзор содержания курса.

Форматирование и узкополосная модуляция. Преобразование неэлектрических сигналов в электрические. Коды, применяемые для кодирования текстов. АЦП и ЦАП. Компандирование аналогового сигнала. Способы передачи сигналов с ИКМ. Искажения в канале, межсимвольная интерференция. Прием М-ичного сигнала на фоне белого шума, корреляционный метод приема, битовая вероятность ошибки. Роль отношения сигнал/шум. Симплексные, ортогональные и биортогональные системы сигналов.

Кодирование источника. Коды Шеннона-Фано, Хафмана, Лемпела-Зива. Модифицированный код Хафмана. Предельные характеристики при квантовании непрерывного источника. Спектральное кодирование источника. Дифференциальная ИКМ с предсказанием, дельта-модуляция. Модельное кодирование сигнала, вокодер, кодирование речи в сотовых системах стандарта GSM. Кодирование видеоизображения, MPEG-2.

Шифрование. Цели и классификация. Методы подстановки и перестановки. Методы шифрования в системах непосредственного телевизионного вещания. Псевдослучайные цифровые последовательности, методы генерирования, свойства. Гаммирование как скоростной метод поточного шифрования. Шифрование речи в сотовых системах стандартов GSM и CDMA. Асимметричные системы шифрования. Алгоритмы DES, PGP, Диффи-Хеллмана и RSA.

Канальное кодирование. Назначение и способы. Кодирование без введения избыточности. Оптимальные коды для передачи в постоянном канале с белым шумом. Симплексные коды, коды Адамара, биортогональные коды. Кодирование с введением избыточности. Линейные блочные коды. Циклические коды, техника кодирования и декодирования. Коды Хэмминга, БЧХ, Рида-Соломона. Объединение кодов: композиционные и каскадные коды, турбо-коды. Перемежение символов при наличии пакетов ошибок. Сверточные коды. Техника кодирования. Древовидная и решетчатая диаграммы. Методы декодирования: пороговый, последовательный, максимума правдоподобия. Алгоритм декодирования Витерби.

Многостанционный доступ (МД). Способы разделения каналов при МД: частотный, временной, кодовый. Методы МД в сотовых системах стандартов NMT-450, GSM и CDMA, а также в спутниковых системах Intelsat, Iridium, Globalstar.

Расширение спектра. Цели и методы, типичные заблуждения. Метод прямой последовательности. Методы скачкообразной перестройки частоты. Роль синхронизации приемника сигнала с расширенным спектром. Многоканальные цифровые системы передачи с ИКМ. Европейский и американский варианты плезиохронной цифровой иерархии. ИКМ-30, структура кадра, метод согласования скоростей цифровых потоков. ИКМ-120, ИКМ-480, ИКМ-1920. Оборудование линейного тракта, обслуживаемые и необслуживаемые регенераторные пункты. Системы передачи по волоконно-оптическому кабелю. Принципы построения, методы модуляции оптического сигнала. SONET/SDH. Передающие и приемные оптические модули. Волновое уплотнение: WDM, DWDM. Отечественные волоконно-оптические системы пере-

дачи. Радиорелейные системы передачи. Общие сведения. Антенно-волноводные тракты. Отечественные радиорелейные системы передачи.

Рекомендуемая литература.

1. **Ск**ляр Б. Цифровая связь. Теоретические основы и практическое применение, 2-е издание. : Пер. с англ. – М.: Изд. дом “Вильямс”, 2003. – 1104 с.

2. Прокис Дж. Цифровая связь. Пер. с англ. / Под ред. Д.Д. Кловского. – М: Радио и связь, 2000. – 800 с.

ПРИЛОЖЕНИЕ А

УТВЕРЖДЕНО
приказом ректора ТУСУРа
от 02.05.2005 г. №3968

ПОЛОЖЕНИЕ

ОБ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ ТОМСКОГО ГОСУДАРСТВЕННОГО НИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУРа)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целями итоговой аттестации являются:

- определение уровня подготовки выпускника, претендующего на получение соответствующей квалификации, и соответствия его подготовки требованиям государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) по конкретному направлению (специальности);
- принятие решения о присвоении соответствующей квалификации (степени) и выдаче выпускнику диплома государственного образца;
- разработка рекомендаций, направленных на совершенствование подготовки студентов в ТУСУРе;
- выдача рекомендаций о целесообразности дальнейшего обучения выпускника в ТУСУРе.

1.2 К итоговым аттестационным испытаниям, входящим в состав итоговой государственной аттестации, допускается лицо, успешно завершившее в полном объёме освоение основной образовательной программы по направлению подготовки (специальности) высшего профессионального образования, разработанной ТУСУРом в соответствии с требованиями ГОС высшего профессионального образования.

При условии успешного прохождения всех установленных форм итоговых аттестационных испытаний, входящих в итоговую государственную аттестацию, выпускнику ТУСУ-

Ра присваивается соответствующая квалификация (степень) и выдаётся диплом государственного образца.

1.3. Лица, обучающиеся в не имеющих государственной аккредитации высших учебных заведениях или успешно окончившие их, имеют право на текущую и итоговую аттестацию в ТУСУРе на условиях экстерната.

2. ФОРМА ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Итоговая аттестация проводится в форме ***защиты выпускной квалификационной работы (ВКР) и итогового государственного экзамена (ГЭ).***

2.2. Выпускные квалификационные работы выполняются для квалификации (степени) бакалавр - в форме бакалаврской работы;

для квалификации «дипломированный специалист» - в форме дипломной работы (проекта);

для квалификации (степени) магистр - в форме магистерской диссертации.

Защита ВКР имеет целью дать оценку способности выпускника к профессиональной деятельности в современных условиях.

2.2.1. Выпускная квалификационная работа - **бакалаврская работа** - выполняется в форме анализа известного технического решения, изделия, технологического процесса, программного продукта, общественно-политического процесса, социального процесса и т.д., раскрывающего знания выпускника, приобретённые им в процессе изучения общепрофессиональных и специальных дисциплин. Работы могут основываться на обобщении выполненных курсовых работ и проектов и подготавливаться к защите в завершающий период теоретического обучения.

2.2.2. Выпускная квалификационная работа - **дипломная работа или дипломный проект** (для инженерных специальностей) должна представлять собой решения поставленной задачи, оформленные в виде конструкторских, технологических, программных и других проектных документов или содержать результаты теоретических и (или) экспериментальных исследований по определённой теме. В ВКР, как правило, должна быть отражена совокупность целенаправленных действий выпускника в следующей последовательности: постановка задачи, поиск инновационных вариантов, теоретический анализ, инженерные расчёты, разработка конструкций, схем и структур, решение вопросов тех-

нологического, организационного, эргонометрического, экономического, экологического обоснования, выявление последствий внедрения разработки или программного продукта.

2.2.3. Выпускная квалификационная работа - **магистерская диссертация** - должна раскрыть знания выпускника, приобретённые в ходе освоения профессиональной программы по направлению, аналитические и творческие способности, развитые при разработке темы диссертации, информационно-системные и организационные навыки, полученные при выполнении программ научно-исследовательской и педагогической практики.

2.3. Темы ВКР определяются профилирующей кафедрой и могут включать темы (задания), предложенные заинтересованными учреждениями, организациями, предприятиями. Тема ВКР с обоснованием целесообразности и (или) необходимости её разработки может быть предложена самим выпускником.

2.3.1. Тема ВКР, её руководитель, консультанты (при необходимости) определяются не позднее, чем за полгода до начала итоговой аттестации. Критерии оценки ВКР разрабатываются группой экспертов с учётом рекомендаций учебно-методических объединений по направлениям (специальностям), утверждаются деканом факультета и доводятся до сведения выпускников не позднее, чем за полгода до начала итоговой аттестации. Руководитель ВКР должен иметь квалификацию не ниже дипломированного специалиста и по завершении ВКР должен составить письменный отзыв (с оценкой) на выполненную студентом работу.

2.3.2. Тема магистерской диссертации, её руководитель, консультанты определяются непосредственно после начала реализации образования по магистерской программе. По завершении работы руководитель должен составить письменный отзыв на выполненную соискателем работу.

2.3.3. ВКР - дипломный проект (работа), магистерская диссертация - подлежат рецензированию. Рецензентами назначаются высококвалифицированные специалисты предприятий, НИИ или вузов. Рецензентом ВКР, в порядке исключения, может быть сотрудник ТУСУРа из числа ведущих специалистов, не являющийся сотрудником выпускающей кафедры по данной специальности. В рецензии (с оценкой) на ВКР даётся заключение о возможности присвоения выпускнику соответствующей квалификации (степени).

2.4. Государственный экзамен (ГЭ) имеет целью определение знаний, умений и навыков студентов в конце теоретического курса обучения по комплексу общекультур-

ных, экологических, социально-экономических, естественно-научных, общепрофессиональных и специальных знаний по профессиональной образовательной программе.

Программа ГЭ по специальности (направлению) разрабатывается группой экспертов с учётом рекомендаций учебно-методических объединений по специальности (направлению), утверждается деканом факультета и доводится до сведения выпускников не позднее, чем **за месяц** до проведения экзамена у бакалавров и не позднее, чем за **три месяца** до проведения экзамена у дипломированных специалистов и магистров. Форма экзамена (письменный, устный или др.) выбирается выпускающей кафедрой.

2.5. На сдачу ГЭ, подготовку ВКР и её защиту в учебных планах отводится по совокупности не менее **шести недель** для бакалавров, не менее **16 недель** - для дипломированных специалистов, и не менее **14 недель** – для магистров.

2.6. Итоговые аттестационные испытания **не могут** быть заменены оценкой качества освоения образовательных программ путём осуществления текущего контроля успеваемости и промежуточной аттестации студента.

3. СТРУКТУРА ГОСУДАРСТВЕННОЙ АТТЕСТАЦИОННОЙ КОМИССИИ

3.1. Итоговая аттестация осуществляется Государственной аттестационной комиссией (ГАК) по специальности или группе специальностей (направлению) со сроком полномочий в течение текущего календарного года.

Председатель ГАК утверждается Федеральным Агентством по образованию. Председатель ГАК должен иметь учёную степень доктора наук (учёное звание профессора) или быть ведущим специалистом предприятия, организации, учреждения соответствующего профиля и не должен быть сотрудником ТУСУРа. При необходимости председатель ГАК должен отвечать требованиям, предъявляемым к специалистам, связанным с работами по закрытой тематике.

3.2. ГАК состоит из экзаменационных комиссий (ЭК) по защите ВКР и по приёму ГЭ, которые формируются приказом ректора (после утверждения председателей ГАК в соответствии с пунктом 3.1 настоящего положения) по каждой основной образовательной программе не позднее, чем за **два месяца** до начала их работы. Комиссии формируются в университете, филиалах или, в случае необходимости, на предприятиях, являющихся потребителями кадров данного профиля специалистов. В состав ГАК филиала ТУСУРа в качестве

заместителя входит представитель университета.

3.3. В состав ЭК по защите ВКР (в количестве не менее пяти человек) и ЭК по приему ГЭ (в количестве не менее трёх человек) включаются преподаватели выпускающей кафедры, общетехнических и естественнонаучных кафедр и кафедр социально-экономического цикла, ведущие специалисты производства по профилю специальности.

3.4. Председателями ЭК по защите ВКР и по приёму ГЭ назначаются ведущие специалисты вузов, научно-исследовательских и проектно-конструкторских центров и организаций, предприятий соответствующих направлений деятельности.

Председателем ЭК по приёму ГЭ по специальности (направлению), в порядке исключения, может быть утверждён сотрудник ТУСУРа из числа ведущих специалистов данного направления, не являющийся сотрудником выпускающей кафедры по данной специальности.

Председатель ГАК может быть председателем ЭК, а также принимать участие в работе любой из них на правах её члена. Председатели ЭК являются заместителями председателя ГАК. Председатель ГАК организует и контролирует деятельность всех ЭК, обеспечивает единство требований, предъявляемых выпускникам.

4. ПОРЯДОК ПРОВЕДЕНИЯ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

4.1. График работы ГАК утверждается приказом ректора по представлению выпускающей кафедры не позднее, чем за **один месяц** до начала её работы и доводится до сведения студентов.

4.2. Итоговый государственный экзамен должен предшествовать защите ВКР и проводиться после завершения теоретического курса обучения.

Выпускающая кафедра, не позднее чем за **полгода** до начала работы ГАК**,** знакомит студентов с порядком проведения итоговой аттестации, за два месяца до начала консультаций по подготовке к итоговому ГЭ и за месяц до начала работы ЭК по защите ВКР объявляет графики их проведения.

4.3. К итоговой аттестации допускаются студенты, завершившие полный курс обучения по профессиональной образовательной программе и успешно прошедшие все предусмотренные учебным планом аттестационные испытания. Допуск к итоговой аттестации в ГАК производится распоряжением декана факультета.

4.4. К защите ВКР допускаются студенты, успешно сдавшие ГЭ по специальности (направлению).

4.5. На каждого студента, допущенного к защите ВКР, руководство выпускающей кафедры представляет сведения о результатах изучения всех циклов профессиональной образовательной программы, сертификаты по дополнительным образовательным программам, включая участие в НИРС, сведения об участии в научных конференциях, конкурсах, о степени знания иностранного языка, отзывы руководителя и рецензента о выполненной ВКР, а также предложения о целесообразности продолжения обучения в университете.

4.6. Все решения ГАК (ЭК) о результатах сдачи ГЭ, защиты ВКР, о присвоении соответствующей квалификации и выдаче диплома принимаются простым большинством голосов членов комиссии при обязательном присутствии председателя комиссии или его заместителя. В случае равенства голосов «за» и «против» председателю ГАК (ЭК) предоставляется право окончательного решения. Особые мнения членов комиссии фиксируются в протоколе ГАК (ЭК).

4.7. Все заседания и решения ГАК (ЭК) протоколируются. Протоколы сохраняются в деканатах до окончания производства дел, после чего сдаются в архив ТУСУРа на постоянный срок храпения.

4.8. Оценка итоговой аттестации осуществляется по четырёхбальной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». ГАК (ЭК) может принять решение о выдаче ***диплома с отличием*** выпускнику, достигшему особых успехов в освоении профессиональной образовательной программы и прошедшему все виды текущих аттестационных испытаний с оценкой «отлично» не менее 75%, остальные - не ниже оценок «хорошо», а также итоговые аттестационные испытания с оценкой «отлично».

Результаты любого из видов аттестационных испытаний объявляются в день заседания экзаменационной комиссии.

4.9. Результаты сдачи ГЭ и защиты ВКР записываются в приложение к диплому раздельно.

4.10. Студентам, не сдавшим ГЭ или не защитившим ВКР, предоставляется право повторной защиты или сдачи экзамена не ранее чем через три месяца и не более чем через пять лет после прохождения итоговой государственной аттестации впервые. Студентам, не защитившим ВКР, может быть выдана академическая справка установленного образца или,

по их просьбе, диплом о высшем профессиональном образовании предыдущего уровня.

Повторные итоговые аттестационные испытания не могут назначаться более двух раз.

4.11. В случае неявки студента для сдачи ГЭ или на защиту ВКР по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтверждённых), по заявлению студента ГАК (ЭК) рассматривает и решает вопрос о новых сроках заседания для проведения аттестации в период действия своих полномочий, но не позднее четырёх месяцев после подачи заявления.

4.12. Все спорные вопросы, связанные с организацией проведения итоговой аттестации, разрешаются ректором ТУСУРа.

4.13. В отчётах председателей ЭК по сдаче ГЭ должна быть дана оценка уровня теоретической и практической подготовки выпускника к самостоятельной профессиональной деятельности относительно общих требований к уровню его образования, определяемому ГОСами соответствующего направления.

В отчётах председателей ЭК по защите ВКР должен содержаться анализ результатов защит ВКР с оценкой способности выпускников к профессиональной деятельности в современных условиях.

В итоговом отчёте о работе ГАК по всем видам аттестационных испытаний должна содержаться характеристика общего уровня подготовки студентов по данному направлению, недостатки в подготовке студентов и рекомендации по устранению отмеченных недостатков.

Итоговые отчеты о работе ГАК должны быть обсуждены на заседаниях советов факультетов.

Итоговые отчеты председателей ГАК составляются в течение пяти дней после проведения заседаний по всем видам аттестационных испытаний и представляются вместе с планом по устранению отмеченных недостатков, подписанном заведующим выпускающей кафедрой, в двух экземплярах в учебное управление ТУСУРа.

4.14. Учебное управление ТУСУРа, на основании итоговых отчётов председателей ГАК, готовит сводный отчёт о результатах проведения итоговой государственной аттестации выпускников ТУСУРа и представляет его в Федеральное агентство по образованию в двухмесячный срок после завершения итоговой аттестации.