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 информационных процессов в системах связи

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **4**
Семестр: **7**
Учебный план набора 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	18	18	часов
4	Всего аудиторных занятий	60	60	часов
5	Самостоятельная работа	48	48	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачет: 7 семестр

Томск 2018

Согласована на портале № 40601

Рассмотрена и одобрена на заседании кафедры
протокол № 11 от « 3 » 7 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденного 06.03.2015 года, рассмотрена и одобрена на заседании кафедры РСС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент кафедра Радиоэлектроники и систем связи (РСС) _____ Д. В. Дубинин

Заведующий обеспечивающей каф. РСС _____ А. В. Фатеев

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РСС _____ А. В. Фатеев

Эксперты:

Профессор кафедры радиоэлектроники и систем связи (РСС) _____ А. С. Задорин

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС) _____ Ю. В. Зеленецкая

Согласована на портале № 40601

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение способов защиты информационных процессов в сетях с гибридной физической средой

изучение возможностей применения программно-аппаратных средств в сетях связи для повышения их защищенности

работа в компьютерных вычислительных сетях (ВС) с применением программных средств защиты и использования существующих, встроенных в архитектуру ОС, средств связи.

1.2. Задачи дисциплины

– изучение способов создания защищенного сетевого соединения, защищенных протоколов связи, защиты от несанкционированного доступа сообщений электронной почты, сетевых ресурсов;

– изучение принципов работы брандмауэров, средств предотвращения вторжений, антивирусных программ на основе использования средств защиты информационных процессов;

– развитие навыков настройки и анализа программных средств защиты, политик безопасности, использования программных отладчиков, сетевых анализаторов

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информационных процессов в системах связи» (Б1.В.ДВ.9.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Вычислительная техника, Общая теория связи, Основы криптографии, Основы построения инфокоммуникационных систем и сетей, Сети связи и системы коммутации.

Последующими дисциплинами являются: Информационные технологии.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-15 умением разрабатывать и оформлять различную проектную и техническую документацию;

– ПК-19 готовностью к организации работ по практическому использованию и внедрению результатов исследований;

В результате изучения дисциплины обучающийся должен:

– **знать** основные подсистемы защиты средств связи в операционных системах персональных ЭВМ, основы администрирования в ОС для контроля информационных процессов в компьютерных сетях, методы и способы защиты от сетевых атак принципы построения программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере средств связи с помощью программных реализаций на высоком и на низком уровне

– **уметь** проводить анализ наличия несанкционированного доступа к компьютерам определять и оценивать вероятные угрозы информационной безопасности компьютера в системах связи осуществлять рациональный выбор программно-аппаратных средств и методов защиты информации на объектах связи

– **владеть** методами защиты информации на компьютерной технике в процессах записи, хранения и копирования, методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в системах связи методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений навыками настройки систем безопасности ОС для безопасной работы в сетях и системах связи

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр

Согласована на портале № 40601

Аудиторные занятия (всего)	60	60
Лекции	24	24
Практические занятия	18	18
Лабораторные работы	18	18
Самостоятельная работа (всего)	48	48
Оформление отчетов по лабораторным работам	18	18
Проработка лекционного материала	18	18
Подготовка к практическим занятиям, семинарам	12	12
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

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 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов.	2	4	0	4	10	ПК-15, ПК-19
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	4	0	4	6	14	ПК-15, ПК-19
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	2	2	0	4	8	ПК-15, ПК-19
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	2	0	6	8	16	ПК-15, ПК-19

Согласована на портале № 40601

5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	2	4	0	4	10	ПК-15, ПК-19
6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	2	0	0	2	4	ПК-15, ПК-19
7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации.	4	4	0	4	12	ПК-15, ПК-19
8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО.	2	0	0	1	3	ПК-15, ПК-19
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	2	0	4	5	11	ПК-15, ПК-19
10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI	2	4	4	10	20	ПК-15, ПК-19
Итого за семестр	24	18	18	48	108	
Итого	24	18	18	48	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 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты	Предмет и задачи защиты информационных процессов в системах связи, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информационных процессов в современном мире. Состав информационных процессов. Причины возникновения уязвимостей, общие принципы построения систем защиты информационных процессов. Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защи-	2	ПК-15, ПК-19

Согласована на портале № 40601

информационных процессов.	щенности (безопасности) систем связи.		
	Итого	2	
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Основные понятия, классификация задач, решаемых информационными процессами. Проблемы идентификации субъекта, понятие протокола идентификации, идентифицирующая информация в информационном процессе. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации. Протоколы идентификации с нулевой передачей знаний. Схемы идентификации Фейге-Фиата-Шамира, Гиллоу-Куискуотера и основные проблемы их реализации.	4	ПК-15, ПК-19
	Итого	4	
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Шифрование в информационном процессе, контроль доступа и разграничение доступа. Иерархический принцип доступа к файлу. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом на основе формальной модели Take-Grant и проблемы ее реализации. Способы фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Программная реализации мандатной модели доступа.	2	ПК-15, ПК-19
	Итого	2	
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	Виды аудита компьютерных систем связи. Контроль целостности данных. Программные системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS.	2	ПК-15, ПК-19
	Итого	2	
5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алгоритмов. Эфемерный ключ. Информационные процессы с компонентами криптозащиты данных. Угрозы криптографическим ключам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции средства криптозащиты систем связи.	2	ПК-15, ПК-19
	Итого	2	
6 Методы и средства	Средства ограничения доступа к компонентам ин-	2	ПК-15,

Согласована на портале № 40601

ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	формационного процесса в системах связи. Встроенная программная защита от изучения информационных процессов в системах связи. Устаревшие технические средства защиты. Программная защита от отладки, защита от дизассемблирования, защита от трассировки по аппаратным прерываниям процессорных процедур. Применение обфускации, протекторов и упаковщиков для усиления защиты системы связи. Методы, затрудняющие считывание скопированной информации. Основные функции средств защиты от копирования.		ПК-19
	Итого	2	
7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации.	Программные надстройки над ОС для защиты информационных процессов. Противоречия программных настроек и встроенных систем защиты информационных процессов в ОС. Получение многофакторная аутентификации за счет программных надстроек над операционной системой. Токены.	4	ПК-15, ПК-19
	Итого	4	
8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО.	Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие вирусной базы и тенденции формирования новых типов вирусов. Программные черви и закладки.	2	ПК-15, ПК-19
	Итого	2	
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	Средства противодействия компьютерным вирусам и их состояние в современных условиях. Маскировка вирусных программ. Способы проникновения вирусов в информационные процессы системы связи. Проблемы минимизации последствий деятельности вирусов после их удаления из системы связи.	2	ПК-15, ПК-19
	Итого	2	
10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI	Принципиальная возможность перехвата трафика в системах связи. Снифферы - назначение, состав и принцип работы. Настройки фильтров и уровни работы в информационном процессе. Возможности анализа сегментов трафика и его перехвата. Изучение свойств информационного процесса в системе связи с помощью снифера.	2	ПК-15, ПК-19
	Итого	2	
Итого за семестр		24	

Согласована на портале № 40601

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	8	9	10
Предшествующие дисциплины										
1 Вычислительная техника	+		+		+					
2 Общая теория связи				+			+		+	
3 Основы криптографии					+					
4 Основы построения инфокоммуникационных систем и сетей						+				+
5 Сети связи и системы коммутации						+		+	+	
Последующие дисциплины										
1 Информационные технологии	+	+								+

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.	
ПК-15	+	+	+	+	Отчет по лабораторной работе, Зачет, Тест, Отчет по практическому занятию
ПК-19	+	+	+	+	Отчет по лабораторной работе, Зачет, Тест, Отчет по практическому занятию

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

Согласована на портале № 40601

7 семестр			
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Исследование парольной защиты компонент связи на основе использования дизассемблеров в ручном, полуавтоматическом и автоматическом режимах.	4	ПК-15, ПК-19
	Итого	4	
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей.	4	ПК-15, ПК-19
	Маршрутизаторы. Состав, назначения свойства. Работа маршрутизатора в имитационном режиме. Удаленная настройка доступа в сеть. Основные команды.	2	
	Итого	6	
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	Исследование доступа к компьютерной системе связи с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.	4	ПК-15, ПК-19
	Итого	4	
10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI	Wireshark – анализатор сетевых протоколов, фиксация потоков в сети связи в интерактивном режиме, просмотр содержания сетевых фреймов.	4	ПК-15, ПК-19
	Итого	4	
Итого за семестр		18	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 40601

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов.	Наличие адресов физических носителей информации.Карта и структура оперативной памяти компьютера.Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.	4	ПК-15, ПК-19
	Итого	4	
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа.	2	ПК-15, ПК-19
	Итого	2	
5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.	4	ПК-15, ПК-19
	Итого	4	
7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система	Надстройки операционной системы. Отечественная система Dallas Lock 8.0 k - состав, назначение, способ установки, организация многофакторной защиты.	4	ПК-15, ПК-19
	Итого	4	

Согласована на портале № 40601

аутентификации.			
10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI	Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в модели OSI.	4	ПК-15, ПК-19
	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 Информационные процессы в системах связи, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям связи. Общие принципы построения систем защиты информационных процессов.	Подготовка к практическим занятиям, семинарам	2	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Проработка лекционного материала	2	ПК-15, ПК-19	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
3 Классификация субъектов и объектов	Подготовка к практическим занятиям, семина-	2	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест

Согласована на портале № 40601

доступа. Основные подходы к защите данных от НСД в системах связи. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	рам			
	Проработка лекционного материала	2		
	Итого	4		
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	Проработка лекционного материала	2	ПК-15, ПК-19	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	8		
5 Организация защищенного процесса шифрования. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Подготовка к практическим занятиям, семинарам	2	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Проработка лекционного материала	2	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест
	Итого	2		
7 Защита информационных процессов на основе надстроек над операционной системой. Многофакторная система аутентификации.	Подготовка к практическим занятиям, семинарам	2	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
8 Разрушающие программные воздействия (РПВ). Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО.	Проработка лекционного материала	1	ПК-15, ПК-19	Зачет, Отчет по практическому занятию, Тест
	Итого	1		

Согласована на портале № 40601

9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	Проработка лекционного материала	1	ПК-15, ПК-19	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	5		
10 Снифферы, как основной инструмент анализа информационных потоков в линии связи. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI	Подготовка к практическим занятиям, семинарам	4	ПК-15, ПК-19	Зачет, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	10		
Итого за семестр		48		
Итого		48		

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				
Зачет			25	25
Отчет по лабораторной работе	10	10	10	30
Отчет по практическому занятию	10	10	10	30
Тест	5	5	5	15
Итого максимум за период	25	25	50	100
Нарастающим итогом	25	50	100	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
< 60% от максимальной суммы баллов на дату КТ	2

Согласована на портале № 40601

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 информационных процессов в компьютерных системах [Электронный ресурс]: Учебное пособие / В. В. Пушкарёв, В. П. Пушкарев - 2012. 131 с. - Режим доступа: https://edu.tusur.ru/publications/1507 (дата обращения: 24.07.2018).

12.2. Дополнительная литература

1. Локальные компьютерные сети [Электронный ресурс]: Учебное пособие / Е. Ю. Агеев - 2012. 105 с. - Режим доступа: https://edu.tusur.ru/publications/2038 (дата обращения: 24.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информационных процессов в компьютерных системах [Электронный ресурс]: Учебно-методическое пособие по проведению практических занятий / Е. Ю. Агеев - 2012. 35 с. - Режим доступа: https://edu.tusur.ru/publications/1850 (дата обращения: 24.07.2018).
2. Компьютерное моделирование и проектирование. Лабораторный практикум. Часть 2 [Электронный ресурс]: Методические указания к лабораторным работам / Е. Ю. Агеев - 2012. 79 с. - Режим доступа: https://edu.tusur.ru/publications/2549 (дата обращения: 24.07.2018).
3. Основы компьютерных сетевых технологий [Электронный ресурс]: Методические рекомендации к организации самостоятельной работы / Е. Ю. Агеев - 2012. 12 с. - Режим доступа: https://edu.tusur.ru/publications/1657 (дата обращения: 24.07.2018).
4. Изучение сетевого протокола TCP/IP [Электронный ресурс]: Методические указания к лабораторным работам / Е. Ю. Агеев - 2012. 16 с. - Режим доступа: https://edu.tusur.ru/publications/2040 (дата обращения: 24.07.2018).

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.

Согласована на портале № 40601

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется использовать базы данных и информационно-справочные системы, к которым у ТУСУРа есть доступ https://lib.tusur.ru/ru/resursy/bazydannyh

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

Учебная лаборатория "Компьютерной радиоэлектроники"

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 412 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Компьютер Core 2 (11 шт.);
- Телевизор Samsung;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows 8 и ниже
- Mozilla Firefox
- Oracle VirtualBox
- PDFCreator
- WinDjView

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Учебная лаборатория "Компьютерной радиоэлектроники"

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 412 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Компьютер Core 2 (11 шт.);
- Телевизор Samsung;
- Комплект специализированной учебной мебели;

Согласована на портале № 40601

- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows 8 и ниже
- Mozilla Firefox
- Oracle VirtualBox
- PDFCreator
- WinDjView

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.

Согласована на портале № 40601

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:

14.1.1. Тестовые задания

1. Что можно отнести к внешним угрозам?
1) Утечки информации.
2) Вредоносные программы
3) Неавторизованный доступ.
4) Наличие сети предприятия

2. Программные закладки это какой класс программ?
1) Системный
2) Безопасный
3) Все зависит от ситуации
4) Опасный

3. Suricata это:
1) Бесплатный антивирусник
2) Межсетвой экран
3) СОВ
4) Выделенный VPN

4. Межсетевой экран:
1) Это комплекс программных или аппаратных средств, осуществляющих контроль и фильтрацию, проходящих через него сетевых пакетов в соответствии с заданными правилами
2) Это комплекс программных или аппаратных средств для СОВ
3) Это комплекс программных или аппаратных средств, осуществляющих выявление сетевых вирусов
4) Это снифер

5. Что такое VPN?
1) Виртуальная частная сеть
2) Параметр компьютерной сети
3) Одна из сетевых компьютерных служб
4) Только внутренняя сеть предприятия

6. Кольца защиты в ОС:
1) создают индивидуальную среду
2) реализуют программное разделение системного и пользовательского уровней привилегий
3) реализуют сетевое разделение системного и пользовательского уровней привилегий
4) реализуют аппаратное разделение системного и пользовательского уровней привилегий

7. Число колец защиты в операционной системе Multics
1) 2
2) 4
3) 5
4) 8

8. Причины переполнения буфера:
1) Отсутствие в программе выделенного адресного пространства
2) Удаление стека перехода в оперативной памяти
3) Запись программой буфера за пределы выделенного адресного пространства

Согласована на портале № 40601

4) Перенаправление стека памяти

9. Эксплойт это:
1) Программа, использующая уязвимость для разрушения другой программы
2) Сеть, в которой разрушается оперативная память программы
3) Тип вируса
4) Системная утилита антивирусника

10. Сплайсинг это:
1) Спрямление алгоритма в памяти
2) Новая функция защиты в СОВ
3) Метод перехвата API функций путем изменения кода целевой функции
4) Способ создания нового окна для авторизованного входа

11. Используют ли утилиты Марка Русиновича :
1) технологию перехвата
2) антивирусы
3) анализ ядра операционной системы
4) кольца защиты ОС

12. Какое бывает взаимодействие между субъектами и объектами ВС:
1) непосредственное точка-точка
2) сетевое по протоколам
3) только через один вид - виртуальный канал
4) только двух видов - с использованием и без использования виртуального канала

13. Какой протокол использует Telnet:
1) IMAP
2) всегда работает в защищенном протоколе
3) изначально не защищенный
4) с двойным кодированием

14. В интернет-поисковую систему входит
1) робот поисковик, индексатор, база данных, система обработки запросов
2) робот индексатор, база данных, система обработки запросов
3) база данных, интернет система обработки запросов
4) поисковый сервер-клиент

15. Существуют ли «хакерские» поисковые системы?
1) Да, это снифферы
2) Может быть в будущем и будут существовать
3) Нет - это серьезные технологии, им это не под силу
4) Да, конечно - Shodan, например

16. Является ли спецификация Secure IP дополнительной по отношению к протоколам IPv6 , IPv4 ?
1) Да, является, поскольку является дополнительной опцией к ним.
2) Нет конечно - это совершенно самостоятельный протокол передачи.
3) Да, поскольку предназначена для поисковых систем.
4) Нет, в ней отсутствует маршрутизация

17. На каком уровне работает IPSec :
1) На последнем седьмом
2) На пятом уровне модели OSI

Согласована на портале № 40601

3) На транспортном
4) На третьем

18. Основное и единственное назначение заголовка AH спецификации IPSec :
1) Установить уникальный адрес
2) Установить индекс защищенности сети.
3) Защита от атак.
4) Защита от мас адреса

19. Есть ли различия между "Транспортным режимом" и "Туннельным режимом" передачи данных :
1) Разница существенная - в "Туннельном режиме" шифруется весь пакет передачи данных.
2) Есть, но она небольшая и касается только заголовков пакетов - они имеют разную спецификацию.
3) Различия практически нет - просто объемы передачи данных разные.
4) Есть, но только для особых случаев

20. Какой вид сетевой атаки является наиболее опасным для IPSec :
1) Конечно атака в туннельном режиме
2) Фишинг, поскольку содержаться полные копии протоколов.
3) Сканирование портов.
4) Denial-of-Service.

14.1.2. Вопросы для подготовки к практическим занятиям, семинарам

Наличие адресов физических носителей информации.Карта и структура оперативной памяти компьютера.Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.

Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа.

Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.

Надстройки операционной системы. Отечественная система Dallas Lock 8.0 k - состав, назначение, способ установки, организация многофакторной защиты.

Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в модели OSI.

14.1.3. Зачёт

Представить карту информационного процесса в оперативной памяти ОС. Указать наличие адресов физических носителей информации. Оценить возможность переполнения памяти и воздействие этого явления на информационный процесс. Представить методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Определить общие и частные проблемы идентификации и аутентификации серверов. Представить абстрактные модели доступа, история развития. Указать основные идеи и свойства объектов и субъектов в моделях доступа. Составить логические построения и комбинации моделей доступа в системах связи.. Назначение аудита компьютерных сетей. Цели внутреннего и внешнего аудита сетей связи. Описать ручной, полуавтоматический и автоматический аудит компьютерных сетей. Представить основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI. Указать основные параметры программно-аппаратных средств шифрования. Пояснить для чего существует открытый доступ к ресурсам и как организовать его защиту в системе связи. Назвать средства ограничения доступа к системам связи. Привести основные меры защиты оперативной памяти коммуникационных устройств. Представить особенности защиты процессов записи и воспроизведения информации. Представить строение простой смарт-карты. Указать виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Назвать типовые возможно-

Согласована на портале № 40601

сти программирования смарт-карт. Пояснить процессы записи и считывания данных с смарт-карт. Показать, что радиочастотная идентификация является одним из вариантов удаленных средств доступа к объектам связи. Представить организацию периметральной защиты объектов связи на основе транспондеров и интеррогаторов. Дать описание типов вирусов. Указать основной механизм распространения. Показать базовые принципы поиска вирусов в антивирусных программах. Представить способы безопасного анализа вирусов. Показать, как определяется наличие вирусов в системах связи. Что такое Lock блокираторы функций записи-чтения в ОС. Для чего необходим UnLock деблокатор связанных программ. Указать принцип работы и использования блокираторов программ.

14.1.4. Темы лабораторных работ

Исследование парольной защиты компонент связи на основе использования дизассемблеров в ручном, полуавтоматическом и автоматическом режимах.

Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей.

Маршрутизаторы. Состав, назначения свойства. Работа маршрутизатора в имитационном режиме. Удаленная настройка доступа в сеть. Основные команды.

Исследование доступа к компьютерной системе связи с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.

Wireshark – анализатор сетевых протоколов, фиксация потоков в сети связи в интерактивном режиме, просмотр содержания сетевых фреймов.

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.

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

Согласована на портале № 40601

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 № 40601