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

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты сетей и систем 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: **8**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	32	32	часов
2	Практические занятия	20	20	часов
3	Лабораторные работы	20	20	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 8 семестр

Томск 2018

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 каф. РСС	_____	Н. Д. Хатьков
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:

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС)	_____	Ю. В. Зеленецкая
Профессор кафедры радиоэлектроники и систем связи (РСС)	_____	А. С. Задорин

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 аппаратных средств защиты

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

2. Место дисциплины в структуре ОПОП

Дисциплина «Программно-аппаратные средства защиты сетей и систем связи» (Б1.В.ОД.13) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Вычислительная техника и информационные технологии, Общая теория связи, Основы криптографии, Сети связи и системы коммутации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-12 готовностью к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам;

– ПК-18 способностью организовывать и проводить экспериментальные испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов;

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 модели OSI

– **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** программно-аппаратными методами защиты информации на компьютерной технике 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 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр

Аудиторные занятия (всего)	72	72
Лекции	32	32
Практические занятия	20	20
Лабораторные работы	20	20
Самостоятельная работа (всего)	36	36
Оформление отчетов по лабораторным работам	14	14
Проработка лекционного материала	10	10
Подготовка к практическим занятиям, семинарам	12	12
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр						
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	2	4	0	3	9	ПК-12, ПК-18
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	2	0	4	3	9	ПК-12, ПК-18
3 Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	4	4	0	3	11	ПК-12, ПК-18
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	4	0	4	3	11	ПК-12, ПК-18
5 Программно-аппаратные средства	2	4	0	3	9	ПК-12, ПК-18

шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.						
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	4	0	4	3	11	ПК-12, ПК-18
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	4	0	0	1	5	ПК-12, ПК-18
8 Радиочастотная идентификация - пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	4	4	0	3	11	ПК-12, ПК-18
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	4	4	4	9	21	ПК-12, ПК-18
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	2	0	4	5	11	ПК-12, ПК-18
Итого за семестр	32	20	20	36	108	
Итого	32	20	20	36	108	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем	Предмет и задачи защиты информации в сетях и системах связи с помощью программно-аппаратных средств, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информации в современном мире. Причины возникновения аппаратных и программных уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопас-	2	ПК-12, ПК-18

защиты (triple functions).	ности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности) компьютерных сетей и системы связи.		
	Итого	2	
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Основные понятия, классификация задач, решаемых программно- аппаратными средствами идентификации и аутентификации. Идентификация субъекта с помощью аппаратных средств, понятие протокола идентификации, идентифицирующая информация. 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 при их аппаратно-программной реализации.	2	ПК-12, ПК-18
	Итого	2	
3 Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа. Программно-аппаратное шифрование, контроль доступа и разграничение доступа. Иерархический принцип доступа к файлу. Аппаратная защита сетевого файлового ресурса. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом на основе формальной модели Take-Grant и проблемы при ее аппаратной реализации. Способы программно-аппаратной 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.	4	ПК-12, ПК-18
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Виды аудита компьютерных систем связи с помощью программно-аппаратных средств. Контроль целостности данных, использование цифровой подписи с защитой аппаратными средствами. Программные системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS.	4	ПК-12, ПК-18
	Итого	4	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных.	Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алгоритмов. Эфемерный ключ. Программно-аппаратные средства шифрования в реальном времени, построение аппаратных компонент криптозащиты данных. Угрозы криптографическим клю-	2	ПК-12, ПК-18

Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	чам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты систем связи.		
	Итого	2	
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Программно-аппаратные методы и средства ограничения доступа к компонентам ЭВМ, защиты программ от несанкционированного копирования. Программные и технические средства защиты информации в системах связи. Встроенная аппаратная защита программ от излучения. 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. Аппаратные приемы противодействия динамическим способам снятия защиты программ от копирования.	4	ПК-12, ПК-18
	Итого	4	
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт. Контактные и бесконтактные смарт – карты с соответствующими интерфейсами ISO – 7816, USB (RuToken, eToken), ISO/ IEC 14443.. Интеллектуальные карты. Жизненный цикл смарт-карт. Выпускаемые серийно интегральные схемы смарт-карт. Инфраструктура поддержки смарт-карт. Проблемы безопасности смарт-карт. Классификация атак на смарт-карты.	4	ПК-12, ПК-18
	Итого	4	
8 Радиочастотная идентификация - пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Базовые принципы радиочастотной идентификации. Структура и функционирование систем RFID. Удаленная передача данных в системах RFID, способы кодирования. Считыватели и транспондеры, электронные и программные компоненты систем RFID, стандартизация. Примеры применения: идентификация товаров, транспортных средств, иммобилайзерные системы, идентификация животных.	4	ПК-12, ПК-18
	Итого	4	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных	Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие программно-аппаратной вирусной базы и тенденции формирования новых типов вирусов, поддерживаемых аппаратным способом. Способы заражения локальных компьютеров с помощью микроконтроллеров и одноплатных компьютеров. Программные черви и закладки. Программно-аппарат-	4	ПК-12, ПК-18

микрокомпьютеров для доступа в защищенные сети связи.	ные средства противодействия компьютерным вирусам и их состояние в современных условиях.		
	Итого	4	
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	Программно-аппаратная защита от разрушающих программных воздействий (РПВ). Проблема восстановления аппаратных настроек операционной системы после воздействия РПВ и применения средств противодействия в системах связи.	2	ПК-12, ПК-18
	Итого	2	
Итого за семестр		32	

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 и информационные технологии	+		+		+					
2 Общая теория связи				+				+		
3 Основы криптографии					+					
4 Сети связи и системы коммутации							+	+	+	

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-12	+	+	+	+	Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Тест, Отчет по практическому занятию
ПК-18	+	+	+	+	Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, 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
8 семестр			
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами 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-12, ПК-18
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, 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-12, ПК-18
	Итого	4	
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Исследование доступа к компьютерной системе связи с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.	4	ПК-12, ПК-18
	Итого	4	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные	Изучение и анализ работы снифера. Настройка фильтров на разных уровнях модели OSI при передачи трафика. Выделение информации, связанной с доступом в сеть связи.	4	ПК-12, ПК-18
	Итого	4	

сети связи.			
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	Антивирусные программы и основные настройки политики безопасности. Специализированные программы защиты от несанкционированного доступа. Многофакторная защита доступа аппаратными средствами.	4	ПК-12, ПК-18
	Итого	4	
Итого за семестр		20	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Наличие адресов физических носителей информации. Карта и структура оперативной памяти компьютера.Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.	4	ПК-12, ПК-18
	Итого	4	
3 Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части 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.	4	ПК-12, ПК-18
	Итого	4	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления	Программная реализация проводника в Windows и других файловых менедлжеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.	4	ПК-12, ПК-18
	Итого	4	

сертификатами.			
8 Радиочастотная идентификация - пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Радиочастотная идентификация, как один из вариантов аппаратных средств защиты доступа удаленным способом. Транспондеры и интеррогаторы в мониторинговых системах доступа к объектам связи.	4	ПК-12, ПК-18
	Итого	4	
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Способы организации разрушающих программных воздействий с помощью микроконтроллеров. Защита доступа в системы связи с помощью микроконтроллера. Одноплатные компьютеры, как существенная угроза системам доступа. Наличие необходимых свойств одноплатных компьютеров для несанкционированного доступа. Виды удаленных атак на системы связи с помощью одноплатных компьютеров.	4	ПК-12, ПК-18
	Итого	4	
Итого за семестр		20	

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
8 семестр				
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Подготовка к практическим занятиям, семинарам	2	ПК-12, ПК-18	Конспект самоподготовки, Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации в сетях связи. Многофакторная идентификация субъекта, понятие	Проработка лекционного материала	1	ПК-12, ПК-18	Конспект самоподготовки, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	3		

протокола идентификации, идентифицирующая информация.				
3 Классификация субъектов и объектов доступа. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Подготовка к практическим занятиям, семинарам	2	ПК-12, ПК-18	Конспект самоподготовки, Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита.	Проработка лекционного материала	1	ПК-12, ПК-18	Конспект самоподготовки, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	3		
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Подготовка к практическим занятиям, семинарам	2	ПК-12, ПК-18	Конспект самоподготовки, Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Проработка лекционного материала	1	ПК-12, ПК-18	Конспект самоподготовки, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	2		
	Итого	3		
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Проработка лекционного материала	1	ПК-12, ПК-18	Конспект самоподготовки, Экзамен
	Итого	1		

8 Радиочастотная идентификация - пример удаленной защиты данных с помощью аппаратных средств. Классификация средств RFID, структура и функционирование систем RFID.	Подготовка к практическим занятиям, семинарам	2	ПК-12, ПК-18	Конспект самоподготовки, Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
9 Разрушающие программные воздействия с помощью программно-аппаратных средств. Способы использования микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи.	Подготовка к практическим занятиям, семинарам	4	ПК-12, ПК-18	Конспект самоподготовки, Отчет по лабораторной работе, Отчет по практическому занятию, Экзамен
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	4		
	Итого	9		
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи с помощью программно-аппаратных средств.	Проработка лекционного материала	1	ПК-12, ПК-18	Конспект самоподготовки, Отчет по лабораторной работе, Экзамен
	Оформление отчетов по лабораторным работам	4		
	Итого	5		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
8 семестр				
Конспект самоподготовки	8	8	10	26
Отчет по лабораторной работе	5	5	6	16
Отчет по практическому занятию	9	9	10	28

Итого максимум за период	22	22	26	70
Экзамен				30
Нарастающим итогом	22	44	70	100

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

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

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Системы контроля и управления доступом. (Серия «Обеспечение безопасности объектов»; Выпуск 2). / В.А. Ворона, В.А. Тихонов. — М. : Горячая линия-Телеком, 2013. — 272 с. [Электронный ресурс] - Режим доступа: http://e.lanbook.com/book/5135 (дата обращения: 05.07.2018).

2. Величко, В.В. Телекоммуникационные системы и сети: В 3 томах. Том 3. - Мультисервисные сети [Электронный ресурс] : учебное пособие / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев ; под ред. Шувалова В.П. Москва : Горячая линия-Телеком, 2015. — 592 с. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/64092 (дата обращения: 05.07.2018).

12.2. Дополнительная литература

1. Т.В. Вахний, С.Ю. Кузьмин. Разработка аппаратно-программного средства защиты от уязвимости badusb. — // Математические структуры и моделирование. — 2016. — № 2. — С. 116-125. [Электронный ресурс] - Режим доступа: http://e.lanbook.com/journal/issue/298339 (дата обращения: 05.07.2018).

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — М. : Горячая линия-Телеком, 2012. — 550 с. [Электронный ресурс] - Режим доступа: http://e.lanbook.com/book/5114

(дата обращения: 05.07.2018).

3. Башмаков, А.В. Выбор оптимального подхода к построению защищенных беспроводных локальных сетей.// Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2015. — № 1. — С. 222-228. [Электронный ресурс] - Режим доступа: http://e.lanbook.com/journal/issue/296034 (дата обращения: 05.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Сети связи и системы коммутации: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1517 (дата обращения: 05.07.2018).
2. Локальные компьютерные сети: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2037 (дата обращения: 05.07.2018).
3. Изучение сетевого протокола TCP/IP: Методические указания к лабораторным работам / Агеев Е. Ю. - 2012. 16 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2040 (дата обращения: 05.07.2018).
4. Методы моделирования и оптимизации телекоммуникационных систем и сетей: Учебно-методическое пособие к практическим занятиям и самостоятельной работы / Демидов А. Я. - 2012. 55 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2840 (дата обращения: 05.07.2018).
5. Использование командных файлов: Методические указания к лабораторной работе / Агеев Е. Ю. - 2012. 14 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2034 (дата обращения: 05.07.2018).

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.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. База данных ТУСУРа:
2. https://lib.tusur.ru/ru/resursy/bazy-dannyh
3. Проф. база данных - http://protect.gost.ru/
4. Информационная система - https://lib.tusur.ru/ru/resursy/bazy-dannyh/uis-rossiya
5. Информационно-аналитическая система Science Index РИНЦ:
6. https://elibrary.ru/defaultx.asp
7. Информационная система - http://www.tehnorma.ru/

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, те-

кущего 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
- LibreOffice
- Microsoft Windows 8 и ниже
- Mozilla Firefox
- Oracle VirtualBox
- PTC Mathcad13, 14
- Qucs
- Scilab

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;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Keysight Electromagnetic Professional (EMPro)
- LibreOffice
- Microsoft Windows 8 и ниже
- Mozilla Firefox
- Oracle VirtualBox
- PTC Mathcad13, 14
- Qucs
- Scilab

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы),

расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

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

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

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

14.1.1. Тестовые задания

Вопрос 1

Отказ в обслуживании это:

состояние информационной системы при котором блокируется доступ к некоторому ее ресурсу

отсутствие доступа к назначенным ресурсам

отсутствие полного доступа ко всем ресурсам

Прекращение работы КС

Вопрос 2

Информационная среда общества это:

Определенный набор информационных компонентов, предназначенных для объектов и субъектов

Совокупность информационных ресурсов и системы формирования, распространения и использования информации

Информационные компоненты субъектов, обладающие способностью к записи, воспроизведения и обработки информации.

Социальные сети

Вопрос 3

Электронный документ это:

любая информация записанная в файлах с расширением doc

любая информация записанная в файлах с расширением txt

информация содержащая печать и реквизиты предприятия произвольной формы собственности

информация зафиксированная электронной цифровой подписью

Вопрос 4

ЭЦП это:

электронный цифровой поток для субъекта

электронный цифровой пакет субъекта

электронная цифровая подпись

энцефалограмма пакета данных

Вопрос 5

Когда был принят федеральный закон о защите информации в РФ?

1974г.

1995г.

1975г

2000г.

Вопрос 6

Какими особенностями обладает информация?

Ее можно передавать на расстояние

Она подвижна.

Она не уничтожима

Она не материальна

Вопрос 7

Какими особенностями обладает информация?

Она всегда доступна.

Она не уничтожима

Она хранится и передается с помощью материальных носителей.

Она может быть преобразована.

Вопрос 8

Когда доступна информация?

Если она содержится на материальном носителе

Всегда, если использовать соответствующие средства.

Только, когда ее разрешают брать

Если имеется пароль на нее

Вопрос 9

Имеет ли информация ценность?

Имеет ценность алфавит, на котором она написана.

Нет не имеет, поскольку она не материальна.

Имеет, если за нее платят.

Имеет, если она полезна для владельца

Вопрос 10

Подтверждение подлинности ЭЦП это:

положительный результат проверки принадлежности ЭЦП владельцу закрытого ключа ЭЦП и отсутствие искажений в электронном документе

положительный результат проверки принадлежности ЭЦП владельцу открытого ключа ЭЦП

характеристика надежности проверки ЭЦП ее владельца

дополнительный параметр ЭЦП
Вопрос 11
При какой политике безопасности используется модель Белла- Лападула:
Системная
Доверительная
Избирательная
Полномочная
Вопрос 12
В интересах кого была разработана полномочная политика безопасности:
В интересах бизнеса
В интересах МО США
В интересах режимных российских предприятий
В интересах сетевых сообществ
Вопрос 13
Модель разработанная Гогеном и Мисгаером называется:
Системным набором
Парольной защитой
Информационной базой
Потоковой
Вопрос 14
Три кита на, которых строится защита информации:
Субъекты и объекты с информационными потоками
Программно-аппаратное управление доступом и потоками
Избирательное и полномочное управление доступом и потоками
Парольный доступ, шифрование, разграничение сред пользователей.
Вопрос 15
Идентификация это:
Процесс распознавания элемента системы
Проверка процесса, создаваемого субъектом
Анализ и получение сведений об объекте системы
Это использование пароля
Вопрос 16
Авторизация это:
Вход в систему.
Представление субъекту прав на доступ к объекту
Проверка идентификации пользователя, процесса
Представление субъекту прав на доступ к объекту
Вопрос 17
Указать в каких сервисах присутствуют процедуры аутентификации:
Электронная почта, веб-форумы, интернет - банкинг
Электронная почта, веб-форумы, социальные сети, интернет - банкинг, платежные системы, корпоративные сайты, интернет магазины
Интернет - банкинг, корпоративные сайты, интернет магазины
Только при входе в компьютер
Вопрос 18
Чем обеспечивается надежность дайджест аутентификации в интернет:
кодированием трафика
отсутствует логин пользователя при обработке
при соединении не используются методы Post и Get
при каждом соединении генерируется новый хэш пароль
Вопрос 19
Что позволяет делать протокол HTTPS в среде интернет:
Передавать зашифрованные заголовки пакетов данных
Шифровать данные в системе интернет магазинов и банкинга.

Шифрует все данные, включая имена пользователей и их пароли.
Шифровать конфиденциальные данные
Вопрос 20
Один из самых надежных методов многофакторной идентификации является:
Применение токенов
Применение логина и пароля
Применение парольной защиты к каждому элементу системы
Управление доступом голосом

14.1.2. Экзаменационные вопросы

Определить порты ввода вывода информации для связи с объектами ОС в зависимости от их назначения. Указать наличие адресов физических носителей информации. Оценить возможность создания блокирующих и не блокирующих сокетов с недокументированным доступом. 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 аппаратной идентификации и аутентификации сетей связи. Представить топологии сетей связи в зависимости от их назначения. Указать основные идеи и свойства объектов и субъектов в условиях ограниченного доступа к ним. Составить логические построения и комбинации моделей доступа в системах связи. Цели внутреннего и внешнего аудита сетей связи. Описать ручной, полуавтоматический и автоматический аудит компьютерных сетей с помощью программно-аппаратных средств. 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 аппаратной 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 возможности 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. Указать принцип работы и использования программно-аппаратных блокираторов программ.

14.1.3. Вопросы на самоподготовку

Способы предотвращения выполнения данных с помощью встроенных средств ОС. Изучить Dáta Execútion Prevéntion, DEP — функции безопасности, встроенной в Linux, Mac OS X, Android и Windows. Получить информацию по токенам в проблеме многофакторной аутентификации. Определить способы установки и виды доступа в систему связи. Провести анализ совмещенных систем защиты доступа в одной и той же ОС на примере Windows. Осуществить анализ возможностей поисковых серверов в области технической IP адресации для сетевого и другого оборудования. Получить последние новости по работе вирусов в мировой практике, новые способы исследования. Привести материалы по повышению устойчивости парольной защиты компонент связи к сетевым атакам.

14.1.4. 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 менедлжеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.

Радиочастотная идентификация, как один из вариантов аппаратных средств защиты доступа удаленным способом. Транспондеры и интеррогаторы в мониторинговых системах доступа к объектам связи.

Способы организации разрушающих программных воздействий с помощью микроконтроллеров. Защита доступа в системы связи с помощью микроконтроллера. Одноплатные компьютеры, как существенная угроза системам доступа. Наличие необходимых свойств одноплатных компьютеров для несанкционированного доступа. Виды удаленных атак на системы связи с помощью одноплатных компьютеров.

14.1.5. 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.

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

Изучение и анализ работы снифера. Настройка фильтров на разных уровнях модели OSI при передачи трафика. Выделение информации, связанной с доступом в сеть связи.

Антивирусные программы и основные настройки политики безопасности. Специализированные программы защиты от несанкционированного доступа. Многофакторная защита доступа аппаратными средствами.

14.1.6. Методические рекомендации

Оценка степени сформированности заявленных в рабочей программе дисциплины компетенций ПК-12, ПК-18 осуществляется как в рамках промежуточной, так и текущей аттестации, в т. ч. при сдаче экзамена, проведении лабораторных и практических. занятий. Порядок оценки для текущих видов контроля определяется в методических указаниях по проведению лабораторных и практических занятий, организации самостоятельной работы.

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 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.