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

Основы защиты информационных процессов в операционных системах

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **5**
Семестр: **10**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	60	60	часов
4	Самостоятельная работа	48	48	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачет: 10 семестр

Томск 2018

Согласована на портале № 37865

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) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 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

Согласована на портале № 37865

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение способов защиты информационных процессов в сетях с гибридной физической средой

изучение возможностей применения стандартных настроек 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

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

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы защиты информационных процессов в операционных системах» (Б1.В.ДВ.8.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Компьютерные сети, Криптографические методы защиты информации, Программно-аппаратные средства обеспечения информационной безопасности, Сети и системы передачи информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-12.2 способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия;

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 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 средств и методов защиты информации на объектах связи;

– **владеть** программными 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 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр

Согласована на портале № 37865

Аудиторные занятия (всего)	60	60
Лекции	24	24
Практические занятия	36	36
Самостоятельная работа (всего)	48	48
Проработка лекционного материала	20	20
Подготовка к практическим занятиям, семинарам	28	28
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	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр					
1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	2	2	6	10	ПСК-12.2
2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	2	4	6	12	ПСК-12.2
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа.	2	4	6	12	ПСК-12.2
4 Виды аудита компьютерных сетей и систем связи, классификация событий.	2	4	6	12	ПСК-12.2
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI.	2	4	4	10	ПСК-12.2
6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанк-	2	4	4	10	ПСК-12.2

Согласована на портале № 37865

ционированного копирования.					
7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	2	4	4	10	ПСК-12.2
8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID.	4	4	4	12	ПСК-12.2
9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ.	2	4	4	10	ПСК-12.2
10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи.	4	2	4	10	ПСК-12.2
Итого за семестр	24	36	48	108	
Итого	24	36	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
10 семестр			
1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Предмет и задачи защиты информационных процессов в сетях и системах связи, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информации в современном мире. Причины возникновения уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности) компьютерных сетей и системы связи.	2	ПСК-12.2
	Итого	2	
2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации. Идентификация субъекта, 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.	2	ПСК-12.2
	Итого	2	

Согласована на портале № 37865

3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа.	Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом. Анализ систем дискреционного разграничения доступа на основе формальной модели Take-Grant. Доступ к данным со стороны процесса. Способы фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей – RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Механизмы реализации мандатной модели доступа. Защита файлов от изменения. Субъект и диспетчер допуска, особенности реализации. Средства управления доступом, используемые в современных операционных системах.	2	ПСК-12.2
	Итого	2	
4 Виды аудита компьютерных сетей и систем связи, классификация событий.	Виды аудита, классификация событий. Контроль целостности данных, использование цифровой подписи. Средства аудита, реализованные в современных сетях и системах связи. Системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS.	2	ПСК-12.2
	Итого	2	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI.	Генерация ключей. Ключи для симметричных и несимметричных алгоритмов. Обмен ключами, алгоритм Диффи-Хеллмана. Эфемерный ключ. Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI. Угрозы криптографическим ключам. Усечение ключевого множества. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты систем связи.	2	ПСК-12.2
	Итого	2	
6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от	Классификация методов защиты информационных процессов в сетях и системах связи. Методы и средства ограничения доступа к компонентам ЭВМ, защиты программ от несанкционированного копирования. Программные и технические средства защиты. Защита программ от излучения. Устаревшие технические средства защиты. Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям. Применение обфускации, протекторов и упаковщиков для усиле-	2	ПСК-12.2

Согласована на портале № 37865

несанкционированного копирования.	ния защиты системы связи. Методы, затрудняющие считывание скопированной информации. Пароли и ключи, организация хранения ключей. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Приемы противодействия динамическим способам снятия защиты программ от копирования.		
	Итого	2	
7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Классификация и архитектура 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.	2	ПСК-12.2
	Итого	2	
8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID.	Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID. Передача данных в системах RFID, способы кодирования. Считыватели и транспондеры, электронные компоненты систем RFID, стандартизация. Обеспечение безопасности данных. Примеры применения: идентификация товаров, транспортных средств, иммобилайзерные системы, идентификация животных.	4	ПСК-12.2
	Итого	4	
9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ.	Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы, как особый класс РПВ. Развитие вирусной базы и тенденции формирования новых типов вирусов. Способы заражения локальных компьютеров и сетей. Программные черви и закладки. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды. Средства противодействия компьютерным вирусам и их состояние в современных условиях.	2	ПСК-12.2
	Итого	2	
10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи.	Защита от разрушающих программных воздействий (РПВ). Проблема восстановления операционной системы после воздействия РПВ и применения средств противодействия в системах связи.	4	ПСК-12.2
	Итого	4	
Итого за семестр		24	

Согласована на портале № 37865

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 Компьютерные сети	+	+	+	+	+	+				
2 Криптографические методы защиты информации						+				
3 Программно-аппаратные средства обеспечения информационной безопасности					+	+	+	+	+	+
4 Сети и системы передачи информации				+						+
Последующие дисциплины										
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		+		+	+	+	+			
2 Преддипломная практика	+	+	+	+	+	+	+	+	+	+

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.	Сам. раб.	
ПСК-12.2	+	+	+	Конспект самоподготовки, Зачет, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 37865

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Карта информационного процесса в оперативной памяти ОС. Наличие адресов физических носителей информации. Возможность переполнения памяти и воздействие этого явления на информационный процесс.	2	ПСК-12.2
	Итого	2	
2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Общие и частные проблемы идентификации и аутентификации серверов.	4	ПСК-12.2
	Итого	4	
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа.	Абстрактные модели доступа, история развития. Основные идеи и свойства объектов и субъектов в моделях доступа. Логические построения и комбинации моделей доступа в системах связи..	4	ПСК-12.2
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи, классификация событий.	Аудит компьютерных сетей. Внутренний и внешний аудит. Ручной, полуавтоматический и автоматический аудит компьютерных сетей. Основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI.	4	ПСК-12.2
	Итого	4	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления	Программно-аппаратные средства шифрования - основные параметры. Открытый доступ к ресурсам и вопросы его защиты в системе связи.	4	ПСК-12.2
	Итого	4	

Согласована на портале № 37865

сертификатами, логическая структура и компоненты PKI.			
6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Средства ограничения доступа к системам связи. Основные меры защиты оперативной памяти коммуникационных устройств. Особенности защиты процессов записи и воспроизведения информации.	4	ПСК-12.2
	Итого	4	
7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Строение простой смарт-карты. Виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Возможности программирования смарт-карт. Запись и считывание данных с смарт-карт.	4	ПСК-12.2
	Итого	4	
8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID.	Радиочастотная идентификация, как один из вариантов удаленных средств доступа к объектам связи. Организация периметральной защиты объектов связи на основе транспондеров и интеррогаторов.	4	ПСК-12.2
	Итого	4	
9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ.	Описание типов вирусов. Основной механизм распространения. Базовые принципы поиска вирусов в антивирусных программах. Способы безопасного анализа вирусов. Наличие вирусов в системах связи.	4	ПСК-12.2
	Итого	4	
10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи.	Lock блокираторы функций записи-чтения в ОС. UnLock деблокатор связанных программ. Принцип работы и использования.	2	ПСК-12.2
	Итого	2	
Итого за семестр		36	

9. Самостоятельная работа

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

Согласована на портале № 37865

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).	Подготовка к практическим занятиям, семинарам	4	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	6		
2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Подготовка к практическим занятиям, семинарам	4	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	6		
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа.	Подготовка к практическим занятиям, семинарам	4	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	6		
4 Виды аудита компьютерных сетей и систем связи, классификация событий.	Подготовка к практическим занятиям, семинарам	4	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	6		
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		

Согласована на портале № 37865

сертификатами, логическая структура и компоненты PKI.				
6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
7 Классификация и архитектура смарт-карт. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
8 Базовые принципы радиочастотной идентификации. Классификация средств RFID, структура и функционирование систем RFID.	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
9 Классификация разрушающих программных воздействий (РПВ). компьютерные Вирусы как особый класс РПВ.	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
10 Защита от разрушающих программных воздействий (РПВ) в компьютерных системах связи.	Подготовка к практическим занятиям, семинарам	2	ПСК-12.2	Конспект самоподготовки, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
Итого за семестр		48		
Итого		48		

Согласована на портале № 37865

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
10 семестр				
Зачет	10	10	10	30
Конспект самоподготовки	3	3	4	10
Отчет по практическому занятию	10	10	10	30
Тест	10	10	10	30
Итого максимум за период	33	33	34	100
Нарастающим итогом	33	66	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

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)

Согласована на портале № 37865

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. [Электронный ресурс]: Горячая линия-Телеком, 2013. — 272 с. - Режим доступа: http://e.lanbook.com/book/5135 (дата обращения: 07.07.2018).
2. Системы и сети связи. Демидов, А.Я.— уч. пособие — М. [Электронный ресурс]: ТУСУР, 2012. — 61 с. - Режим доступа: http://e.lanbook.com/book/11030 (дата обращения: 07.07.2018).
3. Защита информационных процессов в компьютерных системах [Электронный ресурс]: Учебное пособие / Пушкарёв В. В., Пушкарев В. П. - 2012. 131 с. - Режим доступа: https://edu.tusur.ru/publications/1507 (дата обращения: 07.07.2018).

12.2. Дополнительная литература

1. Комплексные (интегрированные) системы обеспечения безопасности. (Серия «Обеспечение безопасности объектов»; Выпуск 7). / В.А. Ворона, В.А. Тихонов.— М. [Электронный ресурс]: Горячая линия-Телеком, 2013. — 160 с. - Режим доступа: http://e.lanbook.com/book/5136 (дата обращения: 07.07.2018).
2. Операционные системы. Концепции построения и обеспечения безопасности. / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — М. [Электронный ресурс]: Горячая линия-Телеком, 2011. — 332 с. - Режим доступа: http://e.lanbook.com/book/5176 (дата обращения: 07.07.2018).
3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова. — М. [Электронный ресурс]: Горячая линия-Телеком, 2012. — 550 с. - Режим доступа: http://e.lanbook.com/book/5114 (дата обращения: 07.07.2018).
4. Финкенцеллер, К. RFID-технологии [Электронный ресурс] [Электронный ресурс]: справочное пособие / К. Финкенцеллер. — Электрон. дан. — Москва ДМК Пресс, 2010. — 489 с. - Режим доступа: https://e.lanbook.com/book/61013 (дата обращения: 07.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы построения коммутационных полей систем коммутации (ОПКПСК) [Электронный ресурс]: Руководство к лабораторным занятиям и самостоятельной работе студентов / Винокуров В. М. - 2012. 115 с. - Режим доступа: https://edu.tusur.ru/publications/2500 (дата обращения: 07.07.2018).
2. Сети связи и системы коммутации [Электронный ресурс]: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. - Режим доступа: https://edu.tusur.ru/publications/1517 (дата обращения: 07.07.2018).
3. Методы моделирования и оптимизации телекоммуникационных систем и сетей [Электронный ресурс]: Учебно-методическое пособие к практическим занятиям и самостоятельной работы / Демидов А. Я. - 2012. 55 с. - Режим доступа: https://edu.tusur.ru/publications/2840 (дата обращения: 07.07.2018).
4. Локальные компьютерные сети [Электронный ресурс]: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. - Режим доступа: https://edu.tusur.ru/publications/2037 (дата обращения: 07.07.2018).

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 № 37865

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

13.1.3. 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.;

Согласована на портале № 37865

- 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
Какой протокол использует Telnet:
IMAP
всегда работает в защищенном протоколе
изначально не защищенный
с двойным кодированием
Вопрос 2
В интернет-поисковую систему входит
робот поисковик, индексатор, база данных, система обработки запросов
робот индексатор, база данных, система обработки запросов
база данных, интернет система обработки запросов
поисковый сервер-клиент
Вопрос 3
Существуют ли «хакерские» поисковые системы?
Да, это снифферы

Согласована на портале № 37865

Может быть в будущем и будут существовать
Нет - это серьезные технологии, им это не под силу
Да, конечно - Shodan, например
Вопрос 4
Является ли спецификация Secure IP дополнительной по отношению к протоколам IPv6 , IPv4 ?
Да, является, поскольку является дополнительной опцией к ним.
Нет конечно - это совершенно самостоятельный протокол передачи.
Да, поскольку предназначена для поисковых систем.
Нет, в ней отсутствует маршрутизация
Вопрос 5
На каком уровне работает IPSec :
На последнем седьмом
На пятом уровне модели OSI
На транспортном
На третьем
Вопрос 6
Основное и единственное назначение заголовка AH спецификации IPSec :
Установить уникальный адрес
Установить индекс защищенности сети.
Защита от атак.
Защита от мас адреса
Вопрос 7
Есть ли различия между "Транспортным режимом" и "Туннельным режимом" передачи данных :
Разница существенная - в "Туннельном режиме" шифруется весь пакет передачи данных.
Есть, но она небольшая и касается только заголовков пакетов - они имеют разную спецификацию.
Различия практически нет - просто объемы передачи данных разные.
Есть, но только для особых случаев
Вопрос 8
Какой вид сетевой атаки является наиболее опасным для IPSec :
Конечно атака в туннельном режиме
Фишинг, поскольку содержаться полные копии протоколов.
Сканирование портов.
Denial-of-Service.
Вопрос 9
Что можно отнести к внешним угрозам?
Утечки информации.
Вредоносные программы
Не авторизованный доступ.
Наличие сети предприятия
Вопрос 10
Программные закладки это какой класс программ?
Системный
Безопасный
Все зависит от ситуации
Опасный
Вопрос 11
Suricata это:
Бесплатный антивирусник
Межсетевой экран
СОВ
Выделенный VPN

Согласована на портале № 37865

Вопрос 12

Межсетевой экран:

Это комплекс программных или аппаратных средств, осуществляющих контроль и фильтрацию, проходящих через него сетевых пакетов в соответствии с заданными правилами

Это комплекс программных или аппаратных средств для СОВ

Это комплекс программных или аппаратных средств, осуществляющих выявление сетевых вирусов

Это снифер

Вопрос 13

Что такое VPN:

Виртуальная частная сеть

Параметр компьютерной сети

Одна из сетевых компьютерных служб

Только внутренняя сеть предприятия

Вопрос 14

Кольца защиты в ОС:

создают индивидуальную среду

реализуют программное разделение системного и пользовательского уровней привилегий

реализуют сетевое разделение системного и пользовательского уровней привилегий

реализуют аппаратное разделение системного и пользовательского уровней привилегий

Вопрос 15

Число колец защиты в операционной системе Multics

2

4

5

8

Вопрос 16

Причины переполнения буфера:

Отсутствие в программе выделенного адресного пространства

Удаление стека перехода в оперативной памяти

Запись программой буфера за пределы выделенного адресного пространства

Перенаправление стека памяти

Вопрос 17

Эксплойт это:

Программа, использующая уязвимость для разрушения другой программы

Сеть, в которой разрушается оперативная память программы

Тип вируса

Системная утилита антивируса

Вопрос 18

Сплайсинг это:

Спрямление алгоритма в памяти

Новая функция защиты в СОВ

Метод перехвата API функций путем изменения кода целевой функции

Способ создания нового окна для авторизованного входа

Вопрос 19

Используют ли утилиты Марка Русиновича :

технологию перехвата

антивирусы

анализ ядра операционной системы

кольца защиты ОС

Вопрос 20

Какое бывает взаимодействие между субъектами и объектами ВС:

непосредственное точка-точка

сетевое по протоколам

Согласована на портале № 37865

только через один вид - виртуальный канал

только двух видов - с использованием и без использования виртуального канала

14.1.2. 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 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.

Что такое Lock блокираторы функций записи-чтения в ОС. Для чего необходим UnLock деблокатор связанных программ. Указать принцип работы и использования блокираторов программ.

14.1.3. 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

Карта информационного процесса в оперативной памяти ОС. Наличие адресов физических носителей информации. Возможность переполнения памяти и воздействие этого явления на информационный процесс.

Методы входа в сетевые сервера различного типа: почтовый, файловый, веб-сервер, сервер баз данных, коммуникационный сервер связи, сервер - принтер и виртуальные сервера. Общие и частные проблемы идентификации и аутентификации серверов.

Абстрактные модели доступа, история развития. Основные идеи и свойства объектов и

Согласована на портале № 37865

субъектов в моделях доступа. Логические построения и комбинации моделей доступа в системах связи..

Аудит компьютерных сетей. Внутренний и внешний аудит. Ручной, полуавтоматический и автоматический аудит компьютерных сетей. Основные политики настроек в программном обеспечении, возможность проверок на нижнем уровне модели OSI.

Программно-аппаратные средства шифрования - основные параметры. Открытый доступ к ресурсам и вопросы его защиты в системе связи.

Средства ограничения доступа к системам связи. Основные меры защиты оперативной памяти коммуникационных устройств. Особенности защиты процессов записи и воспроизведения информации.

Строение простой смарт-карты. Виды доступа к информационным процессам смарт-карт в том числе с помощью удаленных устройств связи. Возможности программирования смарт-карт. Запись и считывание данных с смарт-карт.

Радиочастотная идентификация, как один из вариантов удаленных средств доступа к объектам связи. Организация периметральной защиты объектов связи на основе транспондеров и интеррогаторов.

Описание типов вирусов. Основной механизм распространения. Базовые принципы поиска вирусов в антивирусных программах. Способы безопасного анализа вирусов. Наличие вирусов в системах связи.

Lock блокираторы функций записи-чтения в ОС. UnLock деблокатор связанных программ. Принцип работы и использования.

14.1.5. Методические рекомендации

Оценка степени сформированности заявленных в рабочей программе дисциплины компетенций ПСК-12.2 осуществляется как в рамках промежуточной, так и текущей аттестации, в т. ч. при сдаче дифференцированного зачета, 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:

Согласована на портале № 37865

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

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

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

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 37865