МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	60	60	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	48	48	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 5 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «24» 1 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. РЗИ _____ Н. Д. Хатьков

Заведующий обеспечивающей каф.
РЗИ _____ А. С. Задорин

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперты:

старший преподаватель каф. РЗИ _____ Ю. В. Зеленецкая

1. Цели и задачи дисциплины

1.1. Цели дисциплины

изучение способов программно-аппаратной защиты информации в сетях с гибридной физической средой

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

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

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, аппаратных 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 информации» (Б1.Б.16) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика, Информационные технологии, Основы информационной безопасности, Основы построения компьютерных сетей.

Последующими дисциплинами являются: Криптографические методы защиты информации, Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

В результате изучения дисциплины студент должен:

– **знать** основные подсистемы защиты в операционных системах персональных ЭВМ, основы администрирования в ОС для контроля информационных процессов в компьютерных сетях, методы и способы программно-аппаратной защиты от сетевых атак, принципы построения программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере 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, осуществлять рациональный выбор программно-аппаратных средств и методов защиты информации в компьютерных системах.

– **владеть** программно-аппаратными методами защиты информации на компьютерной технике, методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в компьютерных системах, методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений, навыками настройки систем безопасности ОС для безопасной работы в компьютерных сетях.

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
		5 семестр

Аудиторные занятия (всего)	60	60
Лекции	24	24
Практические занятия	36	36
Из них в интерактивной форме	20	20
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	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	2	0	2	4	ПК-1
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	4	4	4	12	ПК-1
3 Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	4	4	6	14	ПК-1
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита. Аппаратные функции для аудита событий.	2	4	6	12	ПК-1
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструк-	2	4	4	10	ПК-1

тура 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.	2	8	6	16	ПК-1
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	2	4	6	12	ПК-1
8 WiFi сети. Оборудование доступа. Программное обеспечение особенности установки. Настройка модемов и роутеров.	2	0	2	4	ПК-1
9 Использование микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи. Автоматическое формирование одноразовых паролей для персонала с помощью микроконтроллеров.	2	4	6	12	ПК-1
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах с помощью программно-аппаратных средств.	2	4	6	12	ПК-1
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
5 семестр			
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Предмет и задачи защиты информации в компьютерных сетях с помощью программно-аппаратных средств, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты компьютерной информации в современном мире. Причины возникновения аппаратных и программных уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопас-	2	ПК-1

	ности) компьютерных сетей.		
	Итого	2	
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. 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.	4	ПК-1
	Итого	4	
3 Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Основные аппаратные подходы к защите данных от НСД. Абстрактные модели 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-1
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита. Аппаратные функции для аудита событий.	Виды аудита компьютерных систем 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.	2	ПК-1
	Итого	2	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент	Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алго-	2	ПК-1

криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	ритмов. Эфемерный ключ. Программно-аппаратные средства шифрования в реальном времени, построение аппаратных компонент криптозащиты данных. Угрозы криптографическим ключам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты.		
	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 компьютерных системах. 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 компьютерной системы. Методы, затрудняющие считывание скопированной информации. Основные функции средств защиты от копирования в компьютерах. Аппаратные приемы противодействия динамическим способам снятия защиты программ от копирования.	2	ПК-1
	Итого	2	
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.	2	ПК-1
	Итого	2	
8 WiFi сети. Оборудование доступа. Программное обеспечение особенности установки. Настройка	Базовые принципы радиочастотной передачи информации в WiFi сетях. Структура и функционирование систем	2	ПК-1

модемов и роутеров.	WiFi сетей. Понятие каналов в WiFi сетях. Виды шифрования трафика в радиочастотных сетях связи. Брутфорс атаки на радиочастотные сети. Применение WiFi сетей для связи между объектами.		
	Итого	2	
9 Использование микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи. Автоматическое формирование одноразовых паролей для персонала с помощью микроконтроллеров.	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-аппаратные средства противодействия компьютерным вирусам и их состояние в современных условиях.	2	ПК-1
	Итого	2	
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах 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 компьютерных системах.	2	ПК-1
	Итого	2	
Итого за семестр		24	

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 Информатика	+									
2 Информационные технологии		+		+				+		
3 Основы информационной безопасности			+			+	+			
4 Основы построения компьютерных сетей								+	+	+
Последующие дисциплины										
1 Криптографические методы защиты информации					+					

2 Техническая защита информации									+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ПК-1	+	+	+	Зачет, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
5 семестр			
Презентации с использованием слайдов с обсуждением	12	8	20
Итого за семестр:	12	8	20
Итого	12	8	20

7. Лабораторные работы

Не предусмотрено РУП

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
5 семестр			
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие	Изучение программных средств, обеспечивающих поиск информации - броузеры. Аутентификация с помощью этих средств в компьютерных системах.	4	ПК-1
	Итого	4	

протокола идентификации, идентифицирующая информация.			
3 Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Исследование широко распространенности на рынке программных средств абстрактных моделей доступа. Достоинства и недостатки их применимости на практике.	4	ПК-1
	Итого	4	
4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита. Аппаратные функции для аудита событий.	Получение навыков работы с программой XVID32. Ознакомление с синтаксисом языка программирования Assembler. Поиск пароля в программной утилите.	4	ПК-1
	Итого	4	
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Поиск и встраивание кода для замены защищенного пароля в программной утилите с помощью дизассемблера XVID32.	4	ПК-1
	Итого	4	
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Использование дизассемблера OllyDbg для поиска невидимого защищенного пароля, формы и встраивания кода в программной утилите.	4	ПК-1
	Встраивание кода и внешнее управление объектами с помощью программных утилит. Влияние уровня наследования классов на глубину проникновения в программное обеспечение.	4	
	Итого	8	
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Установка и анализ работы программно-аппаратной системы защиты Dallas Lock 8.0 k. Назначение токена.	4	ПК-1
	Итого	4	
9 Использование микроконтроллеров и одноплатных микрокомпьютеров для доступа в защищенные сети связи. Автоматическое формирование одноразовых паролей для персонала с помощью микроконтроллеров.	Программное обеспечение микроконтроллерной техники - установка, настройка. Изучение содержания библиотек программ микроконтроллеров. Структура базового загрузчика микроконтроллера. ОС одноплатных микрокомпьютеров - утилиты, порты ввода-вывода (разъем GPIO). Программное обеспечение микроконтроллерной техники - установка, настройка. Изучение содержания библиотек программ микроконтроллеров. Структура базового	4	ПК-1

	загрузчика микроконтроллера. ОС одноплатных микрокомпьютеров - утилиты, порты ввода-вывода (разъем GPIO).		
	Итого	4	
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах с помощью программно-аппаратных средств.	Анализ структуры вирусной программы. Выявление способов определения ее назначения и классификации.	4	ПК-1
	Итого	4	
Итого за семестр		36	

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
5 семестр				
1 Архитектура программно-аппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Проработка лекционного материала	2	ПК-1	Зачет
	Итого	2		
2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		
3 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	4	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		

4 Виды аудита компьютерных сетей и систем связи с помощью программно-аппаратных средств, классификация событий для проведения аудита. Аппаратные функции для аудита событий.	Подготовка к практическим занятиям, семинарам	4	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
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-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		
6 Программно-аппаратные методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Подготовка к практическим занятиям, семинарам	2	ПК-1	Зачет, Отчет по практическому занятию
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Итого	6		
7 Применение смарт-карт для аппаратной защиты данных, их классификация. Аппаратные компоненты смарт-карт. Программное обеспечение для смарт-карт.	Подготовка к практическим занятиям, семинарам	4	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
8 WiFi сети. Оборудование доступа. Программное обеспечение особенности установки. Настройка модемов и роутеров.	Проработка лекционного материала	2	ПК-1	Зачет
	Итого	2		
9 Использование микроконтроллеров и одноплатных микрокомпьютеров для	Подготовка к практическим занятиям, семинарам	4	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного	2		

доступа в защищенные сети связи. Автоматическое формирование одноразовых паролей для персонала с помощью микроконтроллеров.	материала			
	Итого	6		
10 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах с помощью программно-аппаратных средств.	Подготовка к практическим занятиям, семинарам	4	ПК-1	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
Итого за семестр		48		
Итого		48		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
5 семестр				
Зачет	15	15	20	50
Отчет по практическому занятию	15	15	20	50
Итого максимум за период	30	30	40	100
Нарастающим итогом	30	60	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)

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]. - http://e.lanbook.com/book/5135

2. Михальченко, С.Г. Аппаратное и программное обеспечение ЭВМ. М. : ТУСУР, 2007. — 103 с. [Электронный ресурс]. - https://e.lanbook.com/book/private/11524

3. Голиков, А.М. Основы информационной безопасности.— М. : ТУСУР, 2007. — 201 с. [Электронный ресурс]. - http://e.lanbook.com/book/10927

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]. - http://e.lanbook.com/journal/issue/298339

2. Голиков, А.М. Сети и системы радиосвязи и средства их информационной защиты. — М. : ТУСУР, 2007. — 34 с. [Электронный ресурс]. - http://e.lanbook.com/book/11406

3. 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]. - http://e.lanbook.com/book/5114

4. 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]. - http://e.lanbook.com/journal/issue/296034

12.3. Литература для практических занятий

1. Защита информационных процессов в компьютерных системах: Учебно-методическое пособие по проведению практических занятий / Агеев Е. Ю. - 2012. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1850, дата обращения: 18.03.2017.

12.4. Литература для самостоятельной работы.

1. Основы компьютерных сетевых технологий: Методические рекомендации к организации самостоятельной работы / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1657, дата обращения: 18.03.2017.

12.5 Учебно-методические пособия

12.5.1. Обязательные учебно-методические пособия

1. Средства коммутации систем мобильной связи (СКСМС): Руководство к практическим занятиям и самостоятельной работе студентов / Винокуров В. М. - 2014. 42 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3817, дата обращения: 18.03.2017.

12.5.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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.

12.6. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://www.rambler.ru/
2. http://www.sputnik.ru/
3. https://www.yandex.ru/

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория 418, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74, 4 этаж, ауд. 412. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения

общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Программно-аппаратные средства защиты информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5**

Учебный план набора 2013 года

Разработчики:
- доцент каф. РЗИ Н. Д. Хатьков

Зачет: 5 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Должен знать основные подсистемы защиты в операционных системах персональных ЭВМ, основы администрирования в ОС для контроля информационных процессов в компьютерных сетях, методы и способы программно-аппаратной защиты от сетевых атак, принципы построения программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере с помощью программных реализаций на высоком и на низком уровне модели OSI; Должен уметь проводить анализ наличия несанкционированного доступа к компьютерам, определять и оценивать вероятные угрозы информационной безопасности компьютера, осуществлять рациональный выбор программно-аппаратных средств и методов защиты информации в компьютерных системах.; Должен владеть программно-аппаратными методами защиты информации на компьютерной технике, методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в компьютерных системах, методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений, навыками настройки систем безопасности ОС для безопасной работы в компьютерных сетях. ;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы

Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-1

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Должен знать принципы построения компьютерных сетей и систем, их связь с аппаратной частью; основы защиты информации в компьютере, основные методы расчета параметров компонентов компьютерных устройств и их внедрению в практику, анализ и мониторинг компьютерных сетей от внешних и внутренних вредных воздействий; основные положения по проектированию компьютерных сетей; классификацию и типы вирусных программ: основы многофакторной аппаратной системы защиты информации включая криптографию.	Должен уметь применять на практике политику настроек ПО компьютерных сетей различного назначения; осуществлять грамотный выбор вида безопасной передачи информационных сообщений в зависимости от внутренних и внешний условий вредных воздействий; осуществлять грамотный выбор технологии в области аппаратных компьютерных средств защиты и методов использования антивирусного ПО; применять на практике эффективные методы настройки политики безопасности компьютеров и определения места и характера возникновения вредоносных воздействий; определять на основе мониторинга компьютерных сетей основные показатели их защищенности	Должен владеть навыками формирования топологий компьютерных защищенных сетей, их адресации на основе применения современных коммуникационных компонентов сетей; навыками проектирования защиты компьютерных систем, использования в них криптографических компонентов; навыками работы с антивирусными программами и средствами мониторинга компьютерного ПО, а также набором свойств настроек программно-аппаратной политики безопасности; навыками работы с оборудованием, использующем средства многофакторной аутентификации и идентификации с помощью токенов.
Виды занятий	• Интерактивные прак-	• Интерактивные прак-	• Интерактивные прак-

	тические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	тические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	тические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по практическому занятию; • Зачет;	• Отчет по практическому занятию; • Зачет;	• Отчет по практическому занятию; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает основные тенденции развития инфокоммуникационных компьютерных технологий в области использования защиты информационных процессов; Анализирует связи между различными понятиями в области построения программно-аппаратной защиты ПО и др. оборудования. Знает основные параметры, используемые в компьютерной технике для защиты ОС, цифровой подписи и почтовых сообщений. ;	• Умеет грамотно проводить анализ технической информации; Умеет применять знания для решения различных связных задач по защите информации в том числе и с помощью аппаратных средств.;	• Свободно владеет разными способами представления информации; Владеет методами решения связных задач в области программно-аппаратной защиты компьютеров.;
Хорошо (базовый уровень)	• Понимает связи между различными понятиями в области программно-аппаратной защиты компьютера; Представляет приемы и результаты анализа технической информации в различных комбинациях применения компьютерных компонентов. ;	• Умеет осуществлять поиск информации в области использования компьютерных компонент для защиты информации, представленной в различных отечественных и зарубежных источниках; Умеет самостоятельно подбирать методы решения проблем в области компьютерной безопасности. ;	• Владеет навыками работы с литературными источниками связанными с анализом защищенности ПО компьютера и его компонентов.;
Удовлетворительно (пороговый уровень)	• Воспроизводит основные положения анализа технической	• Умеет работать со справочной литературой; умеет представлять	• Способен корректно представить знания и информацию, связан-

	информации по вредоносным воздействиям на компьютерные компоненты; Дает определения основных понятий в области проведения технических мероприятий, связанных с программно-аппаратной защитой компьютера . ;	результаты своей работы.;	ную с применением аппаратных средств защиты в компьютерных системах. ;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Зачёт

– 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 компьютерных сетей. Представить топологии компьютерных сетей в зависимости от их назначения. Указать основные идеи построения сетей WiFi, представить их топологию. Цели внутреннего и внешнего аудита программно-аппаратной защиты компьютерных систем. 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 компьютерным ресурсам и как организовать его защиту. Назвать средства ограничения доступа к компьютерным системам. Привести основные меры защиты оперативной памяти компьютерных устройств. Представить особенности аппаратной защиты процессов записи и воспроизведения информации. Представить строение простой смарт-карты. Показать возможности микроконтроллеров и одноплатных микрокомпьютеров для защиты сетей связи. Указать виды доступа к сетям WiFi. Пояснить процессы записи и считывания данных с смарт-карт. Показать, что радиочастотная идентификация является одним из вариантов удаленных средств доступа к компьютерным системам. 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 компьютерных системах. Указать принцип работы и использования программно-аппаратных микроконтроллерных блокираторов программ.

3.2 Вопросы для подготовки к практическим занятиям, семинарам

– Изучение программных средств, обеспечивающих поиск информации - броузеры. Аутентификация с помощью этих средств в компьютерных системах.

– Исследование широко распространенности на рынке программных средств абстрактных моделей доступа. Достоинства и недостатки их применимости на практике.

– Получение навыков работы с программой XVID32. Ознакомление с синтаксисом языка программирования Assembler. Поиск пароля в программной утилите.

– Поиск и встраивание кода для замены защищенного пароля в программной утилите с помощью дизассемблера XVID32.

– Использование дизассемблера OllyDbg для поиска невидимого защищенного пароля, формы и встраивания кода в программной утилите.

– Встраивание кода и внешнее управление объектами с помощью программных утилит.

Влияние уровня наследования классов на глубину проникновения в программное обеспечение.

– Установка и анализ работы программно-аппаратной системы защиты Dallas Lock 8.0 k. Назначение токена.

– Анализ структуры вирусной программы. Выявление способов определения ее назначения и классификации.

– Программное обеспечение микроконтроллерной техники - установка, настройка. Изучение содержания библиотек программ микроконтроллеров. Структура базового загрузчика микроконтроллера. ОС одноплатных микрокомпьютеров - утилиты, порты ввода-вывода (разъем GPIO). Программное обеспечение микроконтроллерной техники - установка, настройка. Изучение содержания библиотек программ микроконтроллеров. Структура базового загрузчика микроконтроллера. ОС одноплатных микрокомпьютеров - утилиты, порты ввода-вывода (разъем GPIO).

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. 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]. - http://e.lanbook.com/book/5135

2. Михальченко, С.Г. Аппаратное и программное обеспечение ЭВМ. М. : ТУСУР, 2007. — 103 с. [Электронный ресурс]. - https://e.lanbook.com/book/private/11524

3. Голиков, А.М. Основы информационной безопасности.— М. : ТУСУР, 2007. — 201 с. [Электронный ресурс]. - http://e.lanbook.com/book/10927

4.2. 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]. - http://e.lanbook.com/journal/issue/298339

2. Голиков, А.М. Сети и системы радиосвязи и средства их информационной защиты. — М. : ТУСУР, 2007. — 34 с. [Электронный ресурс]. - http://e.lanbook.com/book/11406

3. 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]. - http://e.lanbook.com/book/5114

4. 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]. - http://e.lanbook.com/journal/issue/296034

4.3. Литература для практических занятий

1. Защита информационных процессов в компьютерных системах: Учебно-методическое пособие по проведению практических занятий / Агеев Е. Ю. - 2012. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1850, дата обращения: 18.03.2017.

4.4. Литература для самостоятельной работы.

1. Основы компьютерных сетевых технологий: Методические рекомендации к организации самостоятельной работы / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1657, дата обращения: 18.03.2017.

4.5. Обязательные учебно-методические пособия

1. Средства коммутации систем мобильной связи (СКСМС): Руководство к практическим занятиям и самостоятельной работе студентов / Винокуров В. М. - 2014. 42 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3817, свободный.

4.6. Базы данных, информационно справочные и поисковые системы

1. http://www.rambler.ru/
2. http://www.sputnik.ru/
3. https://www.yandex.ru/