

**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: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820  
Владелец: Троян Павел Ефимович  
Действителен: с 19.01.2016 по 16.09.2019

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Защита информационных процессов в компьютерных системах**

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: **4**  
Семестр: **7**  
Учебный план набора 2013 года

**Распределение рабочего времени**

№	Виды учебной деятельности	7 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: 7 семестр

Томск 2017

## 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 защиты информационных процессов в компьютерных сетях с гибридной физической средой

изучение возможностей применения программно-аппаратных средств для повышения их защищенности

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

### 1.2. Задачи дисциплины

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

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

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

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информационных процессов в компьютерных системах» (Б1.В.ОД.7) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика, Информационные технологии, Криптографические методы защиты информации, Основы информационной безопасности, Основы построения компьютерных сетей, Техническая защита информации.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

В результате изучения дисциплины студент должен:

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

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

– **владеть** методами защиты информации на компьютерной технике в процессах записи, хранения и копирования, методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в ОС, 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
		7 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	14	14
Подготовка к практическим занятиям, семинарам	34	34
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
7 семестр					
1 Информационные процессы в компьютерных системах, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям компьютерных сетей. Общие принципы построения систем защиты информационных процессов в компьютерах.	2	4	6	12	ПК-2
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в компьютерных системах. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	4	4	6	14	ПК-2
3 Классификация субъектов и объектов доступа в компьютере. Основные подходы к защите данных от НСД в компьютерных системах. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	2	4	4	10	ПК-2
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	2	4	6	12	ПК-2
5 Организация защищенного процесса	2	4	5	11	ПК-2

шифрования в компьютере. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.					
6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	2	4	5	11	ПК-2
7 Защита информационных процессов на основе надстроек над операционной системой компьютера. Многофакторная система аутентификации.	4	4	5	13	ПК-2
8 Разрушающие программные воздействия (РПВ) в компьютере. Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО.	2	0	1	3	ПК-2
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	2	4	5	11	ПК-2
10 Снифферы, как основной инструмент анализа информационных потоков в компьютерных сетях. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI.	2	4	5	11	ПК-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
7 семестр			
1 Информационные процессы в компьютерных системах, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям компьютерных сетей. Общие принципы построения систем защиты информационных процессов в компьютерах.	Предмет и задачи защиты информационных процессов в компьютерных системах, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты информационных процессов в современном мире. Состав информационных процессов. Причины возникновения уязвимостей, общие принципы построения систем защиты информационных процессов в компьютере. Понятие политики без-	2	ПК-2

	опасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности) компьютерных систем.		
	Итого	2	
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в компьютерных системах. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Основные понятия, классификация задач, решаемых информационными процессами в компьютере. Проблемы идентификации субъекта, понятие протокола идентификации, идентифицирующая информация в информационном процессе. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации. Протоколы идентификации с нулевой передачей знаний. Схемы идентификации Фейге-Фиата-Шамира, Гиллоу-Куискуотера и основные проблемы их реализации.	4	ПК-2
	Итого	4	
3 Классификация субъектов и объектов доступа в компьютере. Основные подходы к защите данных от НСД в компьютерных системах. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	Классификация субъектов и объектов доступа в компьютерной системе. Основные подходы к защите данных от НСД. Абстрактные модели доступа. Шифрование в информационном процессе, контроль доступа и разграничение доступа. Иерархический принцип доступа к файлу. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом на основе формальной модели Take-Grant и проблемы ее реализации. Способы фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей – RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Программная реализации мандатной модели доступа в компьютере.	2	ПК-2
	Итого	2	
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	Виды аудита компьютерных систем. Контроль целостности данных. Программные системы предотвращения и обнаружения вторжений, локальные и беспроводные - IPS IDS HIPS WIPS.	2	ПК-2
	Итого	2	
5 Организация защищенного процесса шифрования в компьютере. Построение компонент ОС для криптозащиты данных.	Генерация ключей программно-аппаратными средствами. Ключи для симметричных и несимметричных алгоритмов. Эфемерный ключ. Информа-	2	ПК-2

Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	ционные процессы с компонентами криптозащиты данных. Угрозы криптографическим ключам. Повреждение ключей. Защита алгоритма шифрования. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции средства криптозащиты компьютерных систем.		
	Итого	2	
6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Средства ограничения доступа к компонентам информационного процесса в компьютерных системах. Встроенная программная защита от изучения информационных процессов в компьютерных системах. 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 в компьютере. Основные функции средств защиты файлов от копирования.	2	ПК-2
	Итого	2	
7 Защита информационных процессов на основе надстроек над операционной системой компьютера. Многофакторная система аутентификации.	Программные надстройки над ОС для защиты информационных процессов в компьютере. Противоречия программных настроек и встроенных систем защиты информационных процессов в ОС. Получение многофакторная аутентификации за счет программных надстроек над операционной системой. Токены.	4	ПК-2
	Итого	4	
8 Разрушающие программные воздействия (РПВ) в компьютере. Классификация РПВ. Признаки наличия РПВ в информационных процессах. Возможности анализа разрушающих воздействий на ПО.	Компьютерные вирусы, как особый класс разрушающих программных воздействий. Развитие вирусной базы и тенденции формирования новых типов вирусов. Программные черви и закладки.	2	ПК-2
	Итого	2	
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	Средства противодействия компьютерным вирусам и их состояние в современных условиях. Маскировка вирусных программ. Способы проникновения вирусов в информационные процессы компьютерных систем. Пробле-	2	ПК-2

	мы минимизации последствий деятельности вирусов после их удаления из компьютерной системы.		
	Итого	2	
10 Снифферы, как основной инструмент анализа информационных потоков в компьютерных сетях. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI.	Принципиальная возможность перехвата трафика в компьютерных сетях. Снифферы - назначение, состав и принцип работы. Настройки фильтров и уровни работы в информационном процессе. Возможности анализа сегментов трафика и его перехвата. Изучение свойств информационного процесса в компьютерной сети с помощью сниффера.	2	ПК-2
	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 Криптографические методы защиты информации					+					
4 Основы информационной безопасности			+	+						
5 Основы построения компьютерных сетей							+			+
6 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-2	+	+	+	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
7 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
7 семестр			
1 Информационные процессы в компьютерных системах, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям компьютерных сетей. Общие принципы построения систем защиты информационных процессов в компьютерах.	Наличие адресов физических носителей информации. Карта и структура оперативной памяти компьютера. Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.	4	ПК-2
	Итого	4	
2 Основные понятия, классификация задач, решаемых информационными процессами в	Парольная защита компьютерных компонент на основе использования дизассемблеров в ручном, полуавтоматическом	4	ПК-2

области средств идентификации и аутентификации в компьютерных системах. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	тическом и автоматическом режимах.		
	Итого	4	
3 Классификация субъектов и объектов доступа в компьютере. Основные подходы к защите данных от НСД в компьютерных системах. Абстрактные модели доступа, их влияние на конфигурацию информационных процессов в области защиты информации.	Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа.	4	ПК-2
	Итого	4	
4 Аудит компьютерных сетей и систем связи. Классификация событий для проведения аудита.	Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей.	4	ПК-2
	Итого	4	
5 Организация защищенного процесса шифрования в компьютере. Построение компонент ОС для криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами.	Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.	4	ПК-2
	Итого	4	
6 Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.	Доступ к компьютерной системе с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.	4	ПК-2
	Итого	4	
7 Защита информационных процессов на основе надстроек над операционной системой компьютера. Многофакторная система аутентификации.	Надстройки операционной системы. Отечественная система Dallas Lock 8.0 к - состав, назначение, способ установки, организация многофакторной защиты.	4	ПК-2
	Итого	4	
9 Способы защиты от разрушающих программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	Назначение и состав вируса, полученного с сайта бесплатных рефератов. Способ безопасного изучения вируса. Первичный анализ.	4	ПК-2
	Итого	4	
10 Снифферы, как основной инструмент анализа информационных потоков в	Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в мо-	4	ПК-2

компьютерных сетях. Базовые настройки фильтров sniffеров, их уровни анализа в модели OSI.	дели OSI.		
	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
7 семестр				
1 Информационные процессы в компьютерных системах, классификация. Причины возникновения сбоев в оперативной памяти, передачи информации по линиям компьютерных сетей. Общие принципы построения систем защиты информационных процессов в компьютерах.	Подготовка к практическим занятиям, семинарам	4	ПК-2	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
2 Основные понятия, классификация задач, решаемых информационными процессами в области средств идентификации и аутентификации в компьютерных системах. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.	Подготовка к практическим занятиям, семинарам	4	ПК-2	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
3 Классификация субъектов и объектов доступа в компьютере. Основные подходы к защите данных от НСД в компьютерных системах. Абстрактные модели	Подготовка к практическим занятиям, семинарам	2	ПК-2	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		

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

программных воздействий (РПВ) в компьютерных системах связи. Недостатки антивирусных программ.	рам			
	Проработка лекционного материала	1		
	Итого	5		
10 Снифферы, как основной инструмент анализа информационных потоков в компьютерных сетях. Базовые настройки фильтров снифферов, их уровни анализа в модели OSI.	Подготовка к практическим занятиям, семинарам	4	ПК-2	Зачет, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Итого	5		
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
7 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)
65 - 69		
3 (удовлетворительно) (зачтено)	60 - 64	E (посредственно)
	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. Системы и сети связи. Демидов, А.Я.— уч. пособие — М. : ТУСУР, 2012. — 61 с. [Электронный ресурс]. - <http://e.lanbook.com/book/11030>
3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2012. — 320 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5150>
4. Защита информационных процессов в компьютерных системах: Учебное пособие / Пушкарев В. В., Пушкарев В. П. - 2012. 131 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1507>, дата обращения: 18.03.2017.

### 12.2. Дополнительная литература

1. Комплексные (интегрированные) системы обеспечения безопасности. (Серия «Обеспечение безопасности объектов»; Выпуск 7). / В.А. Ворона, В.А. Тихонов.— М. : Горячая линия-Телеком, 2013. — 160 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5136>
2. Операционные системы. Концепции построения и обеспечения безопасности. / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — М. : Горячая линия-Телеком, 2011. — 332 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5176>

### 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. Локальные компьютерные сети: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2037>, дата обращения: 18.03.2017.

## **12.5 Учебно-методические пособия**

### **12.5.1. Обязательные учебно-методические пособия**

1. Сети связи и системы коммутации: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1517>, дата обращения: 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.

**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**

**Защита информационных процессов в компьютерных системах**

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: **4**

Семестр: **7**

Учебный план набора 2013 года

Разработчики:

– доцент каф. РЗИ Н. Д. Хатьков

Зачет: 7 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-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>Должен знать основные подсистемы защиты средств связи в операционных системах персональных ЭВМ, основы администрирования в ОС для контроля информационных процессов в компьютерных сетях, методы и способы защиты от сетевых атак принципы построения программно-аппаратных систем обнаружения атак, принципы защиты информации на компьютере с помощью программных реализаций на высоком и на низком уровне;</p> <p>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 компьютера;</p> <p>Должен владеть методами защиты информации на компьютерной технике в процессах записи, хранения и копирования, методами поиска слабых мест в настройках компьютера и получения показателей уровня защищенности информации в ОС, методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений, навыками настройки систем безопасности ОС для безопасной работы в компьютерных сетях.;</p>

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-2

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

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	основные принципы защиты информационных процессов в компьютерных системах; основы организации и функционирования глобальных и локальных компьютерных сетей; способы выявления вредоносных программ и их нейтрализации	работать с программными средствами общего назначения по защите информационных процессов в компьютере, соответствующими современным требованиям;	технологией защиты информационных процессов в операционных системах компьютеров; компьютерными методами аудита систем безопасности ОС; приемами антивирусной защиты.
Виды занятий	<ul style="list-style-type: none"> <li>• Интерактивные практические занятия;</li> <li>• Интерактивные лекции;</li> <li>• Практические занятия;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные практические занятия;</li> <li>• Интерактивные лекции;</li> <li>• Практические занятия;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные практические занятия;</li> <li>• Самостоятельная работа;</li> </ul>
Используемые средства оценивания	<ul style="list-style-type: none"> <li>• Отчет по практическому занятию;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по практическому занятию;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по практическому занятию;</li> <li>• Зачет;</li> </ul>

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)	<ul style="list-style-type: none"> <li>• Знает основные тенденции развития сетей и систем связи; Анали-</li> </ul>	<ul style="list-style-type: none"> <li>• Умеет грамотно проводить анализ технической информации; Уме-</li> </ul>	<ul style="list-style-type: none"> <li>• Свободно владеет разными способами представления инфор-</li> </ul>

	зирует на основе информации поиска связи между различными компонентами ее аппаратной реализации и понятиями в этой области; Знает основные возможности поисковых систем для реализации конкурентно-способных технических решений.;	ет применять знания для решения различных связанных задач по защите информации.;	мации; Владеет методами решения связанных задач в области защиты информационных процессов.;
Хорошо (базовый уровень)	<ul style="list-style-type: none"> <li>Понимает соотношения между различными понятиями в области связи; Представляет приемы и результаты анализа технической информации.;</li> </ul>	<ul style="list-style-type: none"> <li>Умеет осуществлять поиск информации в области защиты информационных процессов, представленной в различных отечественных и зарубежных источниках; Умеет самостоятельно подбирать методы решения проблем в области безопасности компьютерных систем.;</li> </ul>	<ul style="list-style-type: none"> <li>Владеет навыками работы с литературными источниками связанными с анализом защищенности информационных процессов в компьютерных системах.;</li> </ul>
Удовлетворительно (пороговый уровень)	<ul style="list-style-type: none"> <li>Воспроизводит основные положения анализа технической информации; Дает определения основных понятий в области связи.;</li> </ul>	<ul style="list-style-type: none"> <li>Умеет работать со справочной литературой; умеет представлять результаты своей работы. ;</li> </ul>	<ul style="list-style-type: none"> <li>Способен корректно представить знания и информацию, связанную с информационными процессами в компьютерных системах.;</li> </ul>

### 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

– 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 компьютерной системе. Назвать средства ограничения доступа к компьютерным системам. Привести основные меры защиты оперативной памяти коммуникационных устройств. Представить особенности защиты процессов за-

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

### **3.2 Вопросы для подготовки к практическим занятиям, семинарам**

- Наличие адресов физических носителей информации. Карта и структура оперативной памяти компьютера. Возможность аппаратного влияния на процессы обмена информацией в оперативной памяти компьютера.
- Абстрактные модели доступа, история развития. Основные аппаратные идеи для реализации моделей доступа. Общие требования к логическим построениям в программном обеспечении при реализации различных моделей доступа.
- Программная реализация проводника в Windows и других файловых менеджеров для шифрования доступа к файлам на локальной компьютерной системе. Общие требования к службам Windows для обеспечения их безопасного использования для защиты данных.
- Надстройки операционной системы. Отечественная система Dallas Lock 8.0 k - состав, назначение, способ установки, организация многофакторной защиты.
- Работа сниффера в системах связи. Настройка фильтров для выявления паролей. Определение уровня работы в модели OSI.
- Парольная защита компьютерных компонент на основе использования дизассемблеров в ручном, полуавтоматическом и автоматическом режимах.
- Программы для ручного, полуавтоматического и автоматического аудита компьютерных сетей. Исследование состояния компьютерной сети и настройка соответствующих политик аудита этих сетей.
- Доступ к компьютерной системе с помощью тестовых утилит. Определение возможности внешнего управления интерфейсом сторонних программ.
- Назначение и состав вируса, полученного с сайта бесплатных рефератов. Способ безопасного изучения вируса. Первичный анализ.

## **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 формирования 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. Системы и сети связи. Демидов, А.Я.— уч. пособие — М. : ТУСУР, 2012. — 61 с. [Электронный ресурс]. - <http://e.lanbook.com/book/11030>
3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2012. — 320 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5150>
4. Защита информационных процессов в компьютерных системах: Учебное пособие / Пушкарев В. В., Пушкарев В. П. - 2012. 131 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1507>, свободный.

#### **4.2. Дополнительная литература**

1. Комплексные (интегрированные) системы обеспечения безопасности. (Серия «Обеспечение безопасности объектов»; Выпуск 7). / В.А. Ворона, В.А. Тихонов.— М. : Горячая линия-Телеком, 2013. — 160 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5136>
2. Операционные системы. Концепции построения и обеспечения безопасности. / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев. — М. : Горячая линия-Телеком, 2011. — 332 с. [Электронный ресурс]. - <http://e.lanbook.com/book/5176>

#### **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. Локальные компьютерные сети: Методические указания по самостоятельной работе / Агеев Е. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/2037>, дата обращения: 18.03.2017.

#### **4.5. Обязательные учебно-методические пособия**

1. Сети связи и системы коммутации: Руководство к практическим занятиям / Винокуров В. М. - 2012. 41 с. [Электронный ресурс] - Режим доступа: <https://edu.tusur.ru/publications/1517>, 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/>