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.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Теоретические основы компьютерной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2014 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	64	64	часов
4	Из них в интерактивной форме	18	18	часов
5	Самостоятельная работа	80	80	часов
6	Всего (без экзамена)	144	144	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е

Экзамен: 10 семестр

Томск 2017

Согласована на портале № 18495

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «14» 4 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16 ноября 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

инженер каф. КИБЭВС	_____	А. О. Исхакова
доцент каф. БИС	_____	О. О. Евсютин

Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

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

Декан ФБ	_____	Е. М. Давыдова
Заведующий выпускающей каф. БИС	_____	Р. В. Мещеряков

Эксперты:

доцент каф. КИБЭВС	_____	А. А. Конев

Согласована на портале № 18495

1. Цели и задачи дисциплины

1.1. Цели дисциплины

обучение студентов комплексному подходу к обеспечению информационной безопасности;

формирование у них представлений об использовании специального математического аппарата для анализа защищенности автоматизированных систем.

1.2. Задачи дисциплины

– получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;

– изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;

– изучить методологию проектирования и построения защищенных автоматизированных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Теоретические основы компьютерной безопасности» (Б1.В.ОД.13) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Администрирование сетей ЭВМ, Безопасность операционных систем, Дискретная математика, Защита информации в компьютерных сетях, Защита информации в системах беспроводной связи, Информационная безопасность телекоммуникационных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-5 способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов;

В результате изучения дисциплины студент должен:

– **знать** методологические и технологические основы комплексного обеспечения безопасности АС; угрозы и методы нарушения безопасности АС; формальные модели, лежащие в основе систем защиты АС; стандарты по оценке защищенных систем и их теоретические основы; методы и средства реализации защищенных АС; средства и методы верификации и анализа надежности защищенных АС.

– **уметь** проводить анализ АС с точки зрения обеспечения компьютерной безопасности; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС; реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС.

– **владеть** работой с АС распределенных вычислений и обработки информации; управлением процессами функционирования систем защиты; навыками работы с документацией АС; использованием критериев оценки защищенности АС; навыками построения формальных моделей систем защиты информации АС.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Аудиторные занятия (всего)	64	64
Лекции	28	28
Практические занятия	36	36

Согласована на портале № 18495

Из них в интерактивной форме	18	18
Самостоятельная работа (всего)	80	80
Выполнение расчетных работ	1	1
Выполнение домашних заданий	9	9
Выполнение индивидуальных заданий	14	14
Оформление отчетов по лабораторным работам	7	7
Проработка лекционного материала	14	14
Самостоятельное изучение тем (вопросов) теоретической части курса	2	2
Подготовка к практическим занятиям, семинарам	33	33
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	180	180
Зачетные Единицы	5.0	5.0

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
10 семестр					
1 Основные положения теории защиты информации	2	2	4	8	ПК-5
2 Математическое моделирование в информационной безопасности	4	4	9	17	ПК-5
3 Классификация угроз безопасности информации	2	4	9	15	ПК-5
4 Дискреционное разграничение доступа	4	4	8	16	ПК-5
5 Мандатное разграничение доступа	6	4	8	18	ПК-5
6 Ролевое разграничение доступа	6	2	5	13	ПК-5
7 Изолированная программная среда	4	2	4	10	ПК-5
8 Защита индивидуальных заданий	0	14	33	47	ПК-5
Итого за семестр	28	36	80	144	
Итого	28	36	80	144	

Согласована на портале № 18495

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Основные положения теории защиты информации	Субъектно-объектное представление автоматизированной системы. Понятие доступа. Информационная безопасность автоматизированных систем.	2	ПК-5
	Итого	2	
2 Математическое моделирование в информационной безопасности	Математические модели в информационной безопасности. Применение моделей при проектировании систем безопасности.	4	ПК-5
	Итого	4	
3 Классификация угроз безопасности информации	Угрозы конфиденциальности, целостности и доступности информации. Угроза раскрытия параметров автоматизированной системы. Классификационные признаки угроз безопасности информации.	2	ПК-5
	Итого	2	
4 Дискреционное разграничение доступа	Матрица доступов. Классическая модель Take-Grant. Расширенная модель Take-Grant.	4	ПК-5
	Итого	4	
5 Мандатное разграничение доступа	Модель Белла-ЛаПадула. Модель Биба. Модель систем военных сообщений.	6	ПК-5
	Итого	6	
6 Ролевое разграничение доступа	Понятие роли. Модель ролевого разграничения доступа.	6	ПК-5
	Итого	6	
7 Изолированная программная среда	Монитор безопасности объектов. Монитор безопасности. Изолированная программная среда.	4	ПК-5
	Итого	4	
Итого за семестр		28	

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.

Согласована на портале № 18495

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
Предшествующие дисциплины								
1 Администрирование сетей ЭВМ			+					
2 Безопасность операционных систем			+				+	
3 Дискретная математика	+	+						
4 Защита информации в компьютерных сетях	+	+	+	+	+	+	+	
5 Защита информации в системах беспроводной связи	+	+	+	+	+	+	+	
6 Информационная безопасность телекоммуникационных систем	+	+	+	+	+	+	+	

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-5	+	+	+	Домашнее задание, Отчет по индивидуальному заданию, Конспект самоподготовки, Собеседование, Опрос на занятиях, Выступление (доклад) на занятии, Расчетная работа

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
10 семестр			
Мини-лекция	3		3
Выступление студента в роли	1		1

Согласована на портале № 18495

обучающего			
Решение ситуационных задач	4		4
Презентации с использованием интерактивной доски с обсуждением		2	2
Презентации с использованием раздаточных материалов с обсуждением	2	2	4
Презентации с использованием слайдов с обсуждением		4	4
Итого за семестр:	10	8	18
Итого	10	8	18

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
10 семестр			
1 Основные положения теории защиты информации	Субъектно-объектное представление автоматизированной системы.	2	ПК-5
	Итого	2	
2 Математическое моделирование в информационной безопасности	Функциональные модели автоматизированных систем	2	ПК-5
	Математические модели автоматизированных систем	2	
	Итого	4	
3 Классификация угроз безопасности информации	Противодействие угрозам конфиденциальности, целостности и доступности информации в автоматизированных системах	4	ПК-5
	Итого	4	
4 Дискреционное разграничение доступа	Работа с матрицей доступов	2	ПК-5
	Модель Take-Grant	2	
	Итого	4	
5 Мандатное разграничение доступа	Мандатное разграничение прав доступа пользователей	2	ПК-5
	Модель Белла-ЛаПадула	2	
	Итого	4	
6 Ролевое разграничение доступа	Ролевое разграничение прав доступа	2	ПК-5

Согласована на портале № 18495

	пользователей		
	Итого	2	
7 Изолированная программная среда	Построение изолированной программной среды	2	ПК-5
	Итого	2	
8 Защита индивидуальных заданий	Защита индивидуальных заданий	14	ПК-5
	Итого	14	
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
10 семестр				
1 Основные положения теории защиты информации	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Опрос на занятиях
	Проработка лекционного материала	2		
	Итого	4		
2 Математическое моделирование в информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ПК-5	Выступление (доклад) на занятии, Домашнее задание, Опрос на занятиях
	Подготовка к практическим занятиям, семинарам	3		
	Проработка лекционного материала	2		
	Выполнение домашних заданий	2		
	Итого	9		
3 Классификация угроз безопасности информации	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Конспект самоподготовки, Опрос на занятиях
	Самостоятельное изучение тем (вопросов) теоретической части курса	2		
	Проработка лекционного материала	3		
	Выполнение домашних заданий	2		

Согласована на портале № 18495

	Итого	9		
4 Дискреционное разграничение доступа	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Опрос на занятиях, Отчет по индивидуальному заданию, Расчетная работа
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Выполнение домашних заданий	1		
	Выполнение расчетных работ	1		
	Итого	8		
5 Мандатное разграничение доступа	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Опрос на занятиях, Отчет по индивидуальному заданию, Собеседование
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Выполнение домашних заданий	2		
	Итого	8		
6 Ролевое разграничение доступа	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Опрос на занятиях, Расчетная работа
	Проработка лекционного материала	2		
	Выполнение домашних заданий	1		
	Итого	5		
7 Изолированная программная среда	Подготовка к практическим занятиям, семинарам	2	ПК-5	Домашнее задание, Опрос на занятиях, Расчетная работа
	Проработка лекционного материала	1		
	Выполнение домашних заданий	1		
	Итого	4		
8 Защита индивидуальных заданий	Подготовка к практическим занятиям, семинарам	12	ПК-5	Отчет по индивидуальному заданию, Собеседование
	Оформление отчетов по	7		

Согласована на портале № 18495

	лабораторным работам			
	Выполнение индивидуальных заданий	14		
	Итого	33		
Итого за семестр		80		
	Подготовка и сдача экзамена	36		Экзамен
Итого		116		

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
10 семестр				
Домашнее задание	4	4	2	10
Конспект самоподготовки	1	1		2
Опрос на занятиях	2	2	2	6
Отчет по индивидуальному заданию	12	24	6	42
Расчетная работа	4	4	2	10
Итого максимум за период	23	35	12	70
Экзамен				30
Нарастающим итогом	23	58	70	100

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный	Оценка (ECTS)

Согласована на портале № 18495

	экзамен	
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. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и инфор-мационными потоками: учебное пособие для вузов. — 2-е изд., испр. и доп. — М.: Горячая линия – Телеком, 2013. — 338 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63235/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63235/

12.2. Дополнительная литература

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: учебное пособие для студентов специальности 075500 / Р. В. Мещеряков, Г. А. Праскурин. — 2-е изд., перераб. и доп. — Томск: В-Спектр, 2007. — 343 с. (наличие в библиотеке ТУСУР - 53 экз.)

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах.— М.: Радио и связь, 2006. — 175 с. (наличие в библиотеке ТУСУР - 60 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: методические указания по выполнению практических работ и самостоятельной работе для студентов специальностей 10.05.02 «Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности» // Р.В. Мещеряков, Г.А. Праскурин, А.А. Шелупанов [Электронный ресурс] — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/praskurin_tokb_lab_srs.pdf [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/praskurin_tokb_lab_srs.pdf

12.3.2 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.

Согласована на портале № 18495

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

1. Не предусмотрено

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 мультимедийная лекционная аудитория.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется компьютерный класс на 20 компьютеров с выходом в Интернет (минимальный размер оперативной памяти компьютеров: 512 МБ).

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 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	Тесты, письменные самостоятельные	Преимущественно письменная

Согласована на портале № 18495

слуха	работы, вопросы к зачету, контрольные работы	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.

Согласована на портале № 18495

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

Теоретические основы компьютерной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль): **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**

Учебный план набора 2014 года

Разработчики:
- инженер каф. КИБЭВС А. О. Исхакова
- доцент каф. БИС О. О. Евсютин

Экзамен: 10 семестр

Томск 2017

Согласована на портале № 18495

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-5	способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов	Должен знать методологические и технологические основы комплексного обеспечения безопасности АС; угрозы и методы нарушения безопасности АС; формальные модели, лежащие в основе систем защиты АС; стандарты по оценке защищенных систем и их теоретические основы; методы и средства реализации защищенных АС; средства и методы верификации и анализа надежности защищенных АС. ; Должен уметь проводить анализ АС с точки зрения обеспечения компьютерной безопасности; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС; реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС. ; Должен владеть работой с АС распределенных вычислений и обработки информации; управлением процессами функционирования систем защиты; навыками работы с документацией АС; использованием критериев оценки защищенности АС; навыками построения формальных моделей систем защиты информации АС.;

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

Согласована на портале № 18495

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-5

ПК-5: способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов.

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	- методологические и технологические основы комплексного обеспечения безопасности АС; - угрозы и методы нарушения безопасности АС; - формальные модели, лежащие в основе систем защиты АС; - стандарты по оценке защищенных систем и их теоретические основы; - методы и средства реализации защищенных АС; - средства и методы верификации и анализа надежности защищенных АС;	- проводить анализ АС с точки зрения обеспечения компьютерной безопасности; - разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; - применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС; - реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;	- работой с АС распределенных вычислений и обработки информации; - управлением процессами функционирования систем защиты; - навыками работы с документацией АС; - использованием критериев оценки защищенности АС; - навыками построения формальных моделей систем защиты информации АС.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценива-	• Домашнее задание; • Отчет по индивиду-	• Домашнее задание; • Отчет по индивиду-	• Домашнее задание; • Отчет по индивиду-

Согласована на портале № 18495

ния	альному заданию; • Конспект самоподготовки; • Собеседование; • Опрос на занятиях; • Выступление (доклад) на занятии; • Расчетная работа; • Экзамен;	альному заданию; • Конспект самоподготовки; • Собеседование; • Опрос на занятиях; • Выступление (доклад) на занятии; • Расчетная работа; • Экзамен;	альному заданию; • Выступление (доклад) на занятии; • Расчетная работа; • Экзамен;

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 методы и средства реализации защищенных автоматизированных систем, ориентируется в моделях защищенных автоматизированных систем, средствах и методах верификации и анализа надежности защищенных автоматизированных систем;	• Умеет моделировать политику безопасности, используя известные подходы и методы. Имеет навык создания системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС.;	• В полном объеме владеет навыками построения моделей систем защиты информации АС, управления процессами работы систем защиты, использования критериев оценки защищенности АС, работы с соответствующей документацией;
Хорошо (базовый уровень)	• Ориентируется в реализации защищенных автоматизированных систем, моделях защищенных автоматизированных систем, средствах и методах верификации и анализа надежности защищенных автоматизированных систем;	• Умеет реализовывать политику безопасности АС, используя известные подходы и методы, а также системы защиты информации в АС на их основе.;	• Владеет основными методами построения моделей систем защиты информации АС, управления процессами работы систем защиты, использования критериев оценки защищенности АС;
Удовлетворительно (пороговый уровень)	• Имеет представление об основных методах и средствах реализации защищенных автоматизированных систем, моделях защищенных автоматизированных систем.;	• Умеет различать сферы применения методов моделирования систем защиты информации в АС.;	• На базовом уровне владеет методами построения моделей систем защиты информации АС, использования критериев оценки защищенности АС;

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 Вопросы на самоподготовку

– Классификация угроз безопасности информации в АС (в графическом виде).

Согласована на портале № 18495

3.2 Темы домашних заданий

– Термины и положения в области теории защиты компьютерных систем. Применение математических моделей построения защищенных АС. Определение актуальных угроз АС. Примеры применения мандатного разграничения доступа, достоинства, недостатки применения для выбранной АС. Примеры применения ролевого разграничения доступа, достоинства, недостатки применения для выбранной АС. Примеры реализации ИПС для выбранной АС.

3.3 Темы индивидуальных заданий

– Парольные системы защиты. Целостность данных. Модель Кларка-Вилсона. Стеганография. Криптография. Шифрование. Криптография. Электронно-цифровая подпись и хеширование. Субъект-объектная модель. Изолированная программная среда. Работа с матрицей доступов. Домены безопасности. Модель Take-Grant. Нарушение дискреционной политики безопасности программой «Троянский конь». Мандатные политики безопасности. Стандарты в области защиты информации в компьютерных системах.

3.4 Вопросы на собеседование

– Основные положения теории защиты информации Математическое моделирование в информационной безопасности Классификация угроз безопасности информации Дискреционное разграничение доступа Мандатное разграничение доступа Ролевое разграничение доступа Изолированная программная среда

3.5 Темы опросов на занятиях

– Субъектно-объектное представление автоматизированной системы. Понятие доступа. Информационная безопасность автоматизированных систем.

– Математические модели в информационной безопасности. Применение моделей при проектировании систем безопасности.

– Угрозы конфиденциальности, целостности и доступности информации. Угроза раскрытия параметров автоматизированной системы. Классификационные признаки угроз безопасности информации.

– Матрица доступов. Классическая модель Take-Grant. Расширенная модель Take-Grant.

– Модель Белла-ЛаПадула. Модель Биба. Модель систем военных сообщений.

– Понятие роли. Модель ролевого разграничения доступа.

– Монитор безопасности объектов. Монитор безопасности. Изолированная программная среда.

3.6 Темы докладов

– Парольная система защиты ОС Windows; Парольная система защиты ОС семейства Unix; Парольные системы защиты различных служб Интернета (Web-сервера, электронная почта, FTP и т.д.); Парольные системы защиты архиваторов; История (хронология) разработки и создания стандартов в области защиты информации в компьютерных системах; Сравнение стандартов: Руководящие документы ГТК и TCSEC; Сравнение стандартов: Руководящие документы ГТК и Единые критерии безопасности информационных технологий; Пример профиля защиты некоторой системы. (Посмотреть на сайте www.fstec.ru в разделе "Материалы, предназначенные для предприятий и организаций, получивших лицензии ФСТЭК России").

3.7 Экзаменационные вопросы

– 1. Что является важнейшими особенностями информации? 2. Что входит в автоматизированные системы обработки информации? 3. Дайте определение информационной безопасности автоматизированной системы. 4. Дайте определение субъекта доступа. 5. Сформулируйте основную теорему безопасности информации в АС. 6. На каком уровне иерархии модели OSI/ISO нельзя использовать модели безопасности информации? 7. На основе чего строится ценность информации в аддитивной модели? 8. Как определяется ценность информации в модель анализа риска? 9. На чем основывается порядковая шкала ценностей? 10. В каких случаях применяется модель решетки ценностей? 11. MLS-решетка. 12. Дайте определение конфиденциальности информации. 13. Дайте определение целостности информации. 14. Дайте определение доступности информации. 15. На какие уровни разделяется доступ к информации применительно к автоматизированным системам?

Согласована на портале № 18495

16. Перечислите основные принципы обеспечения информационной безопасности в АС. 17. Чем, согласно основным принципам, должна обеспечиваться информационная безопасность в АС? 18. Чем, согласно основным принципам, является оценка эффективности обеспечения информационной безопасности в АС? 19. Приведите примеры несанкционированного копирования носителей информации. 20. Приведите примеры не информационных каналов утечки информации. 21. Какого доступа к данным машинных носителей информации не существует? 22. Дайте определение идентификации и аутентификации. 23. На чем основаны парольные системы защиты? 24. Приведите примеры угроз нарушения конфиденциальности. 25. Приведите примеры угроз нарушения целостности. 26. Приведите примеры угроз отказа служб. 27. Зачем необходим принцип системности. 28. Для чего в системе защиты информации используется принцип комплексности? 29. Приведите пример идентификации. 30. Приведите пример аутентификации. 31. Как называют процедуру аутентификации, если в ней (помимо основных сторон) участвует сервер аутентификации (арбитр)? 32. С помощью какого вредоносного программного обеспечения может быть создана атака на систему аутентификации? 33. Дайте определение пароля пользователя. 34. Каких атак на пароли не существует? 35. Перечислите компоненты парольной системы защиты. 36. Какие элементы затрудняют появление угроз парольным системам? 37. Какова зависимость между мощностью алфавита паролей и скоростью перебора паролей? 38. Какова зависимость параметров парольной системы защиты от длины пароля? 39. Как расшифровывается аббревиатура СКЗИ? 40. Какие существуют системы шифрования? 41. Для чего необходимо шифрование? 42. Для чего необходима электронно-цифровая подпись? 43. Дайте определение стеганографии. 44. Приведите примеры стеганографических приемов защиты информации. 45. В чем заключается сертификация средств СКЗИ? 46. Какие стандарты защиты информации на данный момент действуют в Российской Федерации? 47. В чем заключается требование корректности транзакций? 48. В чем заключается принцип минимизации привилегий? 49. Что подразумевает разграничение функциональных обязанностей в АС? 50. Для чего необходим аудит произошедших событий в АС? 51. В каких случаях требуется обеспечение непрерывной работы защитных механизмов АС? 52. В чем заключается требование простоты использования защитных механизмов? 53. Каково назначение модели Кларка – Вилсона? 54. Перечислите правила модели Кларка-Вилсона. 55. Для чего используются барьерные адреса? Варианты назначения барьерных адресов. 56. Позволяет ли использование сегментов оперативной памяти защитить код программ друг от друга? 57. Позволяет ли использование сегментов оперативной памяти обеспечить доступ нескольких программ к одному участку оперативной памяти? 58. Чем обеспечивается отказоустойчивость программного обеспечения (ПО) АС? 59. Дайте определение политики безопасности. 60. Между какими элементами системы существуют потоки информации? 61. При каком условии возможно порождение субъекта? 62. Какое действие называется доступом субъекта S к объекту O? 63. Какой из специальных субъектов системы является механизмом реализации заданной политики безопасности системы? 64. Перечислите типы политик безопасности. 65. Какой тип политик безопасности может противостоять атакам типа «Троянский конь» ? 66. Какими свойствами определяется дискреционное управление доступом? 67. Какими свойствами определяется мандатное управление доступом? 68. Как определяется корректность субъектов друг относительно друга? 69. Каково назначение Монитора безопасности субъектов и Монитора безопасности объектов? 70. Какие специальные субъекты обязательно входят в состав Изолированной программной среды? 71. Для чего используются модели политик безопасности? 72. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих дискреционное управление доступом? 73. Какие из известных Вам моделей политик безопасности используются для представления систем, реализующих мандатное управление доступом? 74. В чем состоит основная задача дискреционных политик безопасности? 75. В чем состоит основная задача мандатных политик безопасности? 76. Какие операции преобразования матрицы доступов используются в модели HRU? 77. Возможна ли проверка безопасности произвольной системы, представленной моделью матрицы доступов HRU? 78. Какая система в модели HRU называется монооперационной? 79. Что является основой политики MLS? 80. При каком условии согласно политике MLS разрешен доступ субъекта S к объекту O? 81. При помощи чего в модели Take-Grant описывается функционирование системы? 82. Какие команды преобразования графа доступов используются в модели Take-Grant? 83. В каком случае возможно похищение прав доступа согласно модели Take-Grant? 84. Каково назначение расширенной модели Take-Grant?

Согласована на портале № 18495

85. Можно ли применять правила де-юре к мнимым дугам в расширенной модели Take-Grant? 86. С помощью каких свойств определяется безопасность системы в модели Белла-Лападула? 87. Что является основной задачей стандартов информационной безопасности? 88. Укажите назначение профиля защиты. 89. Перечислите виды оценок согласно РД «Общие критерии».

3.8 Темы расчетных работ

– Дискреционное разграничение доступа. Ролевое разграничение доступа. Изолированная программная среда.

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. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и инфор-мационными потоками: учебное пособие для вузов. — 2-е изд., испр. и доп. — М.: Горячая линия – Телеком, 2013. — 338 с. [Электронный ресурс]. — Режим доступа: http://e.lanbook.com/view/book/63235/ [Электронный ресурс]. - http://e.lanbook.com/view/book/63235/

4.2. Дополнительная литература

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: учебное пособие для студентов специальности 075500 / Р. В. Мещеряков, Г. А. Праскурин. — 2-е изд., перераб. и доп. — Томск: В-Спектр, 2007. — 343 с. (наличие в библиотеке ТУСУР - 53 экз.)

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах.— М.: Радио и связь, 2006. — 175 с. (наличие в библиотеке ТУСУР - 60 экз.)

4.3. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: методические указания по выполнению практических работ и самостоятельной работе для студентов специальностей 10.05.02 «Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности» // Р.В. Мещеряков, Г.А. Праскурин, А.А. Шелупанов [Электронный ресурс] — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/praskurin_tokb_lab_srs.pdf [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/praskurin_tokb_lab_srs.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрено

Согласована на портале № 18495