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

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

Защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **27.03.04 Управление в технических системах**
Направленность (профиль): **Управление в технических системах**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**
Курс: **4**
Семестр: **8**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	22	22	часов
2	Лабораторные работы	22	22	часов
3	Всего аудиторных занятий	44	44	часов
4	Из них в интерактивной форме	12	12	часов
5	Самостоятельная работа	64	64	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Дифференцированный зачет: 8 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «22» 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 27.03.04 Управление в технических системах, утвержденного 20 октября 2015 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

Ассистент преподавателя каф.
КИБЭВС _____ И. Г. Ганюшкин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

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

Декан ФВС _____ Л. А. Козлова

Заведующий выпускающей каф.
КСУП _____ Ю. А. Шурыгин

Эксперт:

Доцент ТУСУР ИСИБ КИБЭВС _____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, рассмотреть основные методологические принципы теории информационной безопасности, изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

1.2. Задачи дисциплины

– ознакомление студентов с терминологией информационной безопасности, развитие мышления студентов, изучение методов и средств обеспечения информационной безопасности, обучение определению причин, видов, каналов утечки и искажения информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» (Б1.В.ДВ.3.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Базы данных, Вычислительные машины, системы и сети, Информатика, Информационные сети и телекоммуникации, Информационные технологии, Программирование, Процессы коммуникации в современном обществе, Системное программное обеспечение.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-9 способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности;

В результате изучения дисциплины студент должен:

– **знать** сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

– **уметь** классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.

– **владеть** профессиональной терминологией в области информационной безопасности.

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
		8 семестр
Аудиторные занятия (всего)	44	44
Лекции	22	22
Лабораторные работы	22	22
Из них в интерактивной форме	12	12
Самостоятельная работа (всего)	64	64
Выполнение расчетных работ	6	6
Подготовка к контрольным работам	6	6
Выполнение домашних заданий	12	12
Выполнение индивидуальных заданий	8	8

Оформление отчетов по лабораторным работам	24	24
Самостоятельное изучение тем (вопросов) теоретической части курса	8	8
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	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Понятие информационной безопасности, ее роль в национальной безопасности.	4	0	4	8	ОПК-9
2 Терминологические основы информационной безопасности.	2	0	2	4	ОПК-9
3 Угрозы.	2	0	4	6	ОПК-9
4 Классификация и анализ угроз информационной безопасности.	2	0	4	6	ОПК-9
5 Модель угроз, модель нарушителя.	2	0	4	6	ОПК-9
6 Модели оценки угроз конфиденциальности, целостности, доступности.	4	0	6	10	ОПК-9
7 Функции и задачи защиты информации.	4	22	32	58	ОПК-9
8 Проблемы региональной информационной безопасности.	2	0	8	10	ОПК-9
Итого за семестр	22	22	64	108	
Итого	22	22	64	108	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
8 семестр			

1 Понятие информационной безопасности, ее роль в национальной безопасности.	Понятие информационной безопасности. Информационное право в теории государства и права. Информация как объект правового регулирования. Национальные интересы Российской Федерации в информационной сфере. Правовое обеспечение защиты информации.	4	ОПК-9
	Итого	4	
2 Терминологические основы информационной безопасности.	Основные термины и определения. Общедоступная информация и информация ограниченного доступа.	2	ОПК-9
	Итого	2	
3 Угрозы.	Угрозы. Уязвимости. Факторы. Характер происхождения угроз.	2	ОПК-9
	Итого	2	
4 Классификация и анализ угроз информационной безопасности.	Виды угроз. Источники угроз. Предпосылки появления угроз.	2	ОПК-9
	Итого	2	
5 Модель угроз, модель нарушителя.	Классы каналов несанкционированного получения информации. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Архитектура систем защиты информации.Семирубежная модель защиты информации.	2	ОПК-9
	Итого	2	
6 Модели оценки угроз конфиденциальности, целостности, доступности.	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования к вычислительным системам, которые используются для обработки конфиденциальной информации.	4	ОПК-9
	Итого	4	
7 Функции и задачи защиты информации.	Методы формирования функций защиты. Управление системой защиты информации. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии.	4	ОПК-9

	Итого	4	
8 Проблемы региональной информационной безопасности.	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	2	ОПК-9
	Итого	2	
Итого за семестр		22	

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
Предшествующие дисциплины								
1 Базы данных	+	+	+			+		+
2 Вычислительные машины, системы и сети		+	+		+		+	
3 Информатика		+						
4 Информационные сети и телекоммуникации			+					
5 Информационные технологии							+	+
6 Программирование			+	+				
7 Процессы коммуникации в современном обществе					+			
8 Системное программное обеспечение							+	

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	Лабораторные работы	Самостоятельная работа	

ОПК-9	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Расчетная работа, Выступление (доклад) на занятии, Реферат, 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 лабораторные занятия	Интерактивные лекции	Всего
8 семестр			
Презентации с использованием мультимедиа с обсуждением		1	1
Выступление студента в роли обучающего		1	1
IT-методы	10		10
Итого за семестр:	10	2	12
Итого	10	2	12

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
7 Функции и задачи защиты информации.	Администрирование учетных записей пользователей в операционной системе	4	ОПК-9
	Работа с локальной групповой политикой в операционной системе	4	
	Мандатный механизм разграничения доступа к файловым объектам	4	
	Дискреционный механизм разграничения доступа к файловым объектам	6	
	Аутентификация в операционных системах при помощи физического объекта	4	
	Итого	22	
Итого за семестр		22	

8. Практические занятия (семинары)

Не предусмотрено РУП

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности.	Подготовка к контрольным работам	4	ОПК-9	Контрольная работа
	Итого	4		
2 Терминологические основы информационной безопасности.	Подготовка к контрольным работам	2	ОПК-9	Контрольная работа
	Итого	2		
3 Угрозы.	Выполнение домашних заданий	4	ОПК-9	Домашнее задание, Опрос на занятиях
	Итого	4		
4 Классификация и анализ угроз информационной безопасности.	Выполнение домашних заданий	4	ОПК-9	Домашнее задание, Опрос на занятиях
	Итого	4		
5 Модель угроз, модель нарушителя.	Выполнение домашних заданий	4	ОПК-9	Домашнее задание, Опрос на занятиях
	Итого	4		
6 Модели оценки угроз конфиденциальности, целостности, доступности.	Выполнение расчетных работ	6	ОПК-9	Отчет по практическому занятию, Расчетная работа
	Итого	6		
7 Функции и задачи защиты информации.	Самостоятельное изучение тем (вопросов) теоретической части курса	8	ОПК-9	Выступление (доклад) на занятии, Домашнее задание, Отчет по лабораторной работе, Реферат
	Оформление отчетов по лабораторным работам	24		
	Итого	32		
8 Проблемы региональной информационной безопасности.	Выполнение индивидуальных заданий	8	ОПК-9	Домашнее задание, Защита отчета, Опрос на занятиях, Отчет по индивидуальному заданию
	Итого	8		
Итого за семестр		64		
Итого		64		

9.1. Темы для самостоятельного изучения теоретической части курса

1. Виды криптографических преобразований;
2. Виды запутывающих преобразований.

9.2. Темы индивидуальных заданий

1. Анализ защищенности локального объекта;
2. Система с полным перекрытием.

9.3. Темы домашних заданий

1. Анализ возможных угроз информации
2. Классификация каналов несанкционированного получения информации
3. Классификация угроз информации

9.4. Темы расчетных работ

1. Парольные системы защиты

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
8 семестр				
Выступление (доклад) на занятии		2	2	4
Домашнее задание	3	4	2	9
Защита отчета	4	6	2	12
Контрольная работа	5		5	10
Опрос на занятиях	6	2		8
Отчет по индивидуальному заданию			10	10
Отчет по лабораторной работе	4	6	2	12
Отчет по практическому занятию	3	4	2	9
Расчетная работа		10	10	20
Реферат		3	3	6
Итого максимум за период	25	37	38	100
Нарастающим итогом	25	62	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. Шелупанов А.А., Сопов М.А. и др. Основы защиты информации. Учебное пособие. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

12.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс]. - https://edu.tusur.ru/publications/2261

2. Безопасность операционных систем: Методические указания по выполнению лабораторных работ, часть 2 / Конев А.А. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-lab.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.

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

1. Не предусмотрены

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 используется мультимедийная лекционная аудитория, с количеством посадочных мест не менее 55-60, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 4 этаж, ауд. 405. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8Г-Гц. - 14 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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, 4 этаж, ауд. 405. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron 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 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

Защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **27.03.04 Управление в технических системах**
Направленность (профиль): **Управление в технических системах**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**
Курс: **4**
Семестр: **8**

Учебный план набора 2016 года

Разработчик:
- Ассистент преподавателя каф. КИБЭВС И. Г. Ганюшкин

Дифференцированный зачет: 8 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
ОПК-9	способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	Должен знать сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ; Должен уметь классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. ; Должен владеть профессиональной терминологией в области информационной безопасности.;

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	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми	Работает при прямом наблюдении

уровень)		для выполнения простых задач	

2 Реализация компетенций

2.1 Компетенция ОПК-9

ОПК-9: способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности.

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 сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	Должен уметь классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	Должен владеть профессиональной терминологией в области информационной безопасности.
Виды занятий	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Отчет по лабораторной работе; • Опрос на занятиях; • Расчетная работа;	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Отчет по лабораторной работе; • Опрос на занятиях; • Расчетная работа;	• Домашнее задание; • Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Расчетная работа; • Выступление (доклад) на занятии;

	• Выступление (доклад) на занятии; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет;	• Выступление (доклад) на занятии; • Реферат; • Отчет по практическому занятию; • Дифференцированный зачет;	• Реферат; • Отчет по практическому занятию; • Дифференцированный 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)	• 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;

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 Темы рефератов

- Виды криптографических преобразований;
- Виды запутывающих преобразований.

3.2 Темы домашних заданий

- Анализ возможных угроз информации
- Анализ защищенности локального объекта;
- Система с полным перекрытием.
- Виды криптографических преобразований;
- Виды запутывающих преобразований.
- Классификация каналов несанкционированного получения информации
- Классификация угроз информации

3.3 Темы индивидуальных заданий

- Анализ защищенности локального объекта;
- Система с полным перекрытием.

3.4 Темы опросов на занятиях

- Анализ возможных угроз информации

– Анализ защищенности локального объекта;
– Система с полным перекрытием.
– Классификация каналов несанкционированного получения информации
– Классификация угроз информации

3.5 Темы докладов

– Виды криптографических преобразований;
– Виды запутывающих преобразований.

3.6 Темы контрольных работ

– Термины и определения нормативно-правовой базы информационной безопасности

3.7 Вопросы для подготовки к практическим занятиям, семинарам

– Парольные системы защиты

3.8 Темы расчетных работ

– Парольные системы защиты

3.9 Темы лабораторных работ

– Администрирование учетных записей пользователей в операционной системе
– Работа с локальной групповой политикой в операционной системе
– Мандатный механизм разграничения доступа к файловым объектам
– Дискреционный механизм разграничения доступа к файловым объектам
– Аутентификация в операционных системах при помощи физического объекта

3.10 Вопросы дифференцированного зачета

– 1. Теория защиты информации. Основные направления. 2. Обеспечение
– информационной безопасности и направления защиты. 3. Комплексность (целевая,
– инструментальная, структурная, функциональная, временная). 4. Требования к системе защиты
– информации. 5. Угрозы информации. 6. Виды угроз. Основные нарушения. 7. Характер
– происхождения угроз. 8. Источники угроз. Предпосылки появления угроз. 9. Система защиты
– информации. 10. Классы каналов несанкционированного получения информации. 11. Причины
– нарушения целостности информации:. 12. Методы и модели оценки уязвимости информации. 13.
– Общая модель воздействия на информацию. 14. Общая модель процесса нарушения физической
– целостности информации. 15. Структурированная схема потенциально возможных
– злоумышленных действий в автоматизированных системах обработки данных. 16.
– Методологические подходы к оценке уязвимости информации. 17. Модель защиты системы с
– полным перекрытием. 18. Рекомендации по использованию моделей оценки уязвимости
– информации. 19. Допущения в моделях оценки уязвимости информации. 20. Методы определения
– требований к защите информации. 21. Факторы, обуславливающие конкретные требования к
– защите, обусловленные спецификой автоматизированной обработки информации. 22.
– Классификация требований к средствам защиты информации. 23. Требования к защите,
– определяемые структурой автоматизированной системы обработки данных. 24. Требования к
– защите, обуславливаемые видом защищаемой информации. 25. Требования, обуславливаемые,
– взаимодействием пользователя с комплексом средств автоматизации. 26. Анализ суще-

ствующих
– методик определения требований к защите информации. 27. Стандарт США "Критерии оценки
– гарантировано защищенных вычислительных систем в интересах министерства обороны США".
– Основные положения. 28. Руководящем документе Гостехкомиссии России "Классификация
– автоматизированных систем и требований по защите информации", выпущенном в 1992 году.
– Часть 1. 29. Классы защищенности средств вычислительной техники от несанкционированного
– доступа. 30. Факторы, влияющие на требуемый уровень защиты информации. 31. Функции и
– задачи защиты информации. Основные положения механизмов непосредственной защиты и
– механизмы управления механизмами непосредственной защиты. 32. Методы формирования
– функций защиты. 33. События, возникающие при формировании функций защиты. 34. Классы
– задач функций защиты. 35. Класс задач функций защиты 1 — уменьшение степени распознавания
– объектов 36. Класс задач функций защиты 2 — защита содержания обрабатываемой, хранимой и
– передаваемой информации. 37. Класс задач функций защиты 3 — защита информации от
– информационного воздействия. 38. Функции защиты информации. 39. Стратегии защиты
– информации. 40. Способы и средства защиты информации. 41. Способы "абсолютной системы
– защиты". 42. Архитектура систем защиты информации. Требования. 43. Общеметодологических
– принципов архитектуры системы защиты информации. 44. Построение средств защиты
– информации. 45. Ядро системы защиты. 46. Семирубежная модель защиты.

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. Шелупанов А.А., Сопов М.А. и др. Основы защиты информации. Учебное пособие. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

4.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информацион-

ной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

4.3. Обязательные учебно-методические пособия

1. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс]. - https://edu.tusur.ru/publications/2261
2. Безопасность операционных систем: Методические указания по выполнению лабораторных работ, часть 2 / Конев А.А. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-lab.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрены