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

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	46	46	часов
2	Практические занятия	26	26	часов
3	Всего аудиторных занятий	72	72	часов
4	Из них в интерактивной форме	18	18	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 6 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 3 от « 2 » 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Ассистент каф. КИБЭВС _____ А. И. Гуляев

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. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент, кандидат технических наук каф. КИБЭВС _____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Цель – дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

- Задачи дисциплины - дать основы:
- - законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;
- -понятий и видов защищаемой информации по законодательству РФ;
- - правовых режимов конфиденциальной информации;
- - правового режим защиты государственной тайны, системы защиты государственной тайны;
- - лицензирования и сертификации в области защиты информации, в том числе государственной тайны;
- -правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
- -защиты интеллектуальной собственности;
- -правовой регламентации охранной деятельности;
- -правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- - международного законодательства в области защиты информации;
- - знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.
- -угроз информационной безопасности объекта;
- -организации службы безопасности объекта;
- - подбора и работы с кадрами в сфере информационной безопасности;
- - организации и обеспечения режима конфиденциальности;
- -охраны объектов.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» (Б1.Б.16) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Основы информационной безопасности, Правоведение.

Последующими дисциплинами являются: Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-3 способностью проводить анализ защищенности автоматизированных систем;
- ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы;
- ПК-20 способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
- ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
- ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
- ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для

защиты информации ограниченного доступа;

В результате изучения дисциплины студент должен:

– **знать** − основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.

– **уметь** − применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

– **владеть** − профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами; − навыками организации и обеспечения режима секретности; − методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Аудиторные занятия (всего)	72	72
Лекции	46	46
Практические занятия	26	26
Из них в интерактивной форме	18	18
Самостоятельная работа (всего)	36	36
Проработка лекционного материала	13	13
Подготовка к практическим занятиям, семинарам	23	23
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	144	144
Зачетные Единицы	4.0	4.0

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
6 семестр					
1 Законодательство РФ в области информационной безопасности.	4	0	1	5	ПК-11, ПК-3
2 Правовые основы защиты конфиденциальной информации.	8	4	4	16	ПК-23, ПК-3
3 Правовые основы защиты государственной тайны.	6	4	6	16	ПК-20, ПК-21
4 Лицензирование и сертификация.	4	0	1	5	ПК-11, ПК-20, ПК-23
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	4	4	4	12	ПК-21, ПК-22, ПК-3
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	4	4	5	13	ПК-11, ПК-20, ПК-21, ПК-23, ПК-3
7 Средства и методы физической защиты объектов.	4	4	3	11	ПК-21, ПК-22, ПК-23
8 Организация службы безопасности и работа с кадрами.	4	2	6	12	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
9 Организация и обеспечения режима секретности.	4	2	3	9	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
10 Организация пропускного и внутри объектового режима.	4	2	3	9	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
Итого за семестр	46	26	36	108	
Итого	46	26	36	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
6 семестр			

1 Законодательство РФ в области информационной безопасности.	Понятие и структура информационной безопасности. Основные задачи системы информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Субъекты и объекты правоотношений в области информационной безопасности. Отрасли законодательства, регламентирующие деятельность по защите информации.	4	ПК-11, ПК-3
	Итого	4	
2 Правовые основы защиты конфиденциальной информации.	Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.	8	ПК-23, ПК-3
	Итого	8	
3 Правовые основы защиты государственной тайны.	Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.	6	ПК-20, ПК-21
	Итого	6	
4 Лицензирование и сертификация.	Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты	4	ПК-11, ПК-20, ПК-23
	Итого	4	
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной	4	ПК-21, ПК-22, ПК-3

	информации. Экспертиза компьютерных преступлений. Административные правонарушения.		
	Итого	4	
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Задачи организационного обеспечения информационной безопасности. Роль нормативных документов в защите информации. Инвентаризация информационных ресурсов организации. Построение моделей документооборота и информационных систем. Модели нарушителя информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.	4	ПК-11, ПК-20, ПК-21, ПК-3
	Итого	4	
7 Средства и методы физической защиты объектов.	Структура системы физической защиты. Система охраны периметра. Система сигнализации, видеонаблюдения, контроля доступа: классификация, сферы применения.	4	ПК-21, ПК-22, ПК-23
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.	4	ПК-11, ПК-20, ПК-21
	Итого	4	
9 Организация и обеспечения режима секретности.	Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров.	4	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3

	Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества. Организация режима и охраны объектов в процессе транспортировки.		
	Итого	4	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.	4	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
	Итого	4	
Итого за семестр		46	

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 Основы информационной безопасности	+	+					+	+	+	+
2 Правоведение	+	+	+	+	+			+	+	
Последующие дисциплины										

1 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-3	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях
ПК-11	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях
ПК-20	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях
ПК-21	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях
ПК-22	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях
ПК-23	+	+	+	Отчет по индивидуальному заданию, Отчет по лабораторной работе, Опрос на занятиях

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
6 семестр			
IT-методы	2	6	8

Работа в команде	2		2
Решение ситуационных задач	2		2
Мини-лекция		6	6
Итого за семестр:	6	12	18
Итого	6	12	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
6 семестр			
2 Правовые основы защиты конфиденциальной информации.	Работа с конфиденциальной информацией. Защита коммерческой тайны.	4	ПК-23, ПК-3
	Итого	4	
3 Правовые основы защиты государственной тайны.	Работа с государственной тайной.	4	ПК-20, ПК-21
	Итого	4	
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Нарушение законодательства в сфере информационных технологий. Компьютерные преступления.	4	ПК-21, ПК-22, ПК-3
	Итого	4	
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Описание структуры защищаемой организации и видов защищаемой информации.	4	ПК-11, ПК-21, ПК-23, ПК-3
	Итого	4	
7 Средства и методы физической защиты объектов.	Определение угроз автоматизированной системе, обрабатывающей информацию ограниченного доступа, и требований к работе сотрудника с этой информацией.	4	ПК-21, ПК-22, ПК-23
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Разработка структуры службы безопасности организации.	2	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
	Итого	2	
9 Организация и обеспечения режима секретности.	Выбор способов и методов защиты информации и автоматизированной	2	ПК-11, ПК-20,

	системы.		ПК-21, ПК-22, ПК-23, ПК-3
	Итого	2	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима в организации.	2	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3
	Итого	2	
Итого за семестр		26	

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
6 семестр				
1 Законодательство РФ в области информационной безопасности.	Проработка лекционного материала	1	ПК-11, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Итого	1		
2 Правовые основы защиты конфиденциальной информации.	Подготовка к практическим занятиям, семинарам	2	ПК-23, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Итого	4		
3 Правовые основы защиты государственной тайны.	Подготовка к практическим занятиям, семинарам	4	ПК-20, ПК-21	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Итого	6		
4 Лицензирование и сертификация.	Проработка лекционного материала	1	ПК-11, ПК-20, ПК-23	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Итого	1		
5 Нормы ответственности за правонарушения в сфере компьютерных	Подготовка к практическим занятиям, семинарам	3	ПК-21, ПК-22, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по
	Проработка лекционного	1		

технологий.	материала			лабораторной работе
	Итого	4		
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Подготовка к практическим занятиям, семинарам	4	ПК-11, ПК-20, ПК-21, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Итого	5		
7 Средства и методы физической защиты объектов.	Подготовка к практическим занятиям, семинарам	2	ПК-21, ПК-22, ПК-23	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Итого	3		
8 Организация службы безопасности и работа с кадрами.	Подготовка к практическим занятиям, семинарам	4	ПК-11, ПК-20, ПК-21	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	2		
	Итого	6		
9 Организация и обеспечения режима секретности.	Подготовка к практическим занятиям, семинарам	2	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Итого	3		
10 Организация пропускного и внутри объектового режима.	Подготовка к практическим занятиям, семинарам	2	ПК-11, ПК-20, ПК-21, ПК-22, ПК-23, ПК-3	Опрос на занятиях, Отчет по индивидуальному заданию, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

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

6 семестр				
Опрос на занятиях	5	7	8	20
Отчет по индивидуальному заданию		10	10	20
Отчет по лабораторной работе	10	10	10	30
Итого максимум за период	15	27	28	70
Экзамен				30
Нарастающим итогом	15	42	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 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. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 1. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 214[2] с. : табл. - ISBN 978-5-91191-053-5 (наличие в библиотеке ТУСУР - 81 экз.)

2. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 2. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 194[2] с. : табл. - ISBN 978-5-91191-054-5 (наличие в библиотеке ТУСУР - 81 экз.)

12.2. Дополнительная литература

1. Информационная безопасность предприятия : Учебное пособие / А. А. Садердинов, В. А. Трайнёв, А. А. Федулов ; Международная академия информации,информационных процессов и технологий. - 3-е изд. - М. : Дашков и К°, 2006. - 335[1] с. : ил., табл. - Библиогр.: с. 326-331. - ISBN 5-94798-918-2 (наличие в библиотеке ТУСУР - 19 экз.)
2. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 1. - Томск : ТУСУР, 2005. - 221 с. (наличие в библиотеке ТУСУР - 83 экз.)
3. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 2. - Томск : ТУСУР, 2005. - 180 с. : ил. - Библиогр.: с. 179-180. (наличие в библиотеке ТУСУР - 82 экз.)
4. Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие для вузов / А. А. Стрельцов [и др.] ; ред. А. А. Стрельцов. - М. : Академия, 2008. - 256 с. : табл. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 242-245. - ISBN 978-5-7695-4240-4 (наличие в библиотеке ТУСУР - 1 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2506, дата обращения: 02.03.2017.

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. Ресурсы сети Интернет

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

1. 1. Справочно-правовая система (СПС) КонсультантПлюс.
2. 2. Справочно-правовая система (СПС) ГАРАНТ.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Мультимедийная лекционная аудитория. корпус УЛК, ауд. 401

13.1.2. Материально-техническое обеспечение для практических занятий

Компьютерный класс с выходом в Интернет. корпус УЛК, ауд. 402

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Компьютерный класс с выходом в Интернет. корпус УЛК, ауд. 402

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

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **6**

Учебный план набора 2012 года

Разработчики:

- Ассистент каф. КИБЭВС А. И. Гуляев

Экзамен: 6 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-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Должен знать − основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах. ; Должен уметь − применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации. ; Должен владеть − профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами; − навыками организации и обеспечения режима секретности; − методами организации и управления деятельностью служб
ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
ПК-20	способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	
ПК-3	способностью проводить анализ защищенности автоматизированных систем	

		защиты информации на предприятии; - методами формирования требований по защите информации. ;

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-23

ПК-23: способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

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	− основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;	− применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;	− профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами;
Виды занятий	• Интерактивные	• Интерактивные	• Интерактивные

	практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • 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)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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 завершения 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.;

2.2 Компетенция ПК-22

ПК-22: способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	− правовые основы организации защиты государственной тайны и конфиденциальной	− разрабатывать проекты нормативных и организационно-распорядительных	− навыками организации и обеспечения режима секретности;

	информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	документов, регламентирующих работу по защите информации.	
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 оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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 завершения 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.;

2.3 Компетенция ПК-21

ПК-21: способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.

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

представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	− организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	− применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	− методами организации и управления деятельностью служб защиты информации на предприятии;
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 оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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 завершения 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.;

2.4 Компетенция ПК-20

ПК-20: способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	− правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.	− применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	-методами организации и управления деятельностью служб защиты информации на предприятии;
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная	• Интерактивные практические занятия; • Самостоятельная работа;

	работа;	работа;	
Используемые средства оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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 завершения 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. ;

2.5 Компетенция ПК-11

ПК-11: способностью разрабатывать политику информационной безопасности автоматизированной системы.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 11.

Таблица 11 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные	− применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных	- методами формирования требований по защите информации.

	методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.	документов, регламентирующих работу по защите информации.	
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 оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 12.

Таблица 12 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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 завершения 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.;

2.6 Компетенция ПК-3

ПК-3: способностью проводить анализ защищенности автоматизированных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 13.

Таблица 13 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	− основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты	− применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	− профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами; − навыками организации и обеспечения режима секретности; − методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.

	информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.		
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 оценивания	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Экзамен;	• Отчет по лабораторной работе; • Отчет по индивидуальному заданию; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 14.

Таблица 14 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в 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	• Обладает диапазоном практических умений, требуемых для решения	• Берет ответственность за завершения задач в

	пределах изучаемой области.;	определенных проблем в области исследования.;	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 индивидуальных заданий

– Задание №1. Каждый студент для своего индивидуального задания по дисциплине «Комплексное обеспечение информационной безопасности» должен представить обоснование использования или разработки выбранной системы. Должны быть рассмотрены следующие вопросы: 1) Перечень нормативно-правовых актов: 1.1) перечень законов; 1.2) перечень подзаконных актов. 2) Лицензирование и сертификация: 2.1) обоснование проведения лицензирования и сертификации (аттестации); 2.2) перечень контролирующих, сертифицирующих, аттестующих организаций; 3) Нормы ответственности за нарушение нормативно-правовых актов: 3.1) перечень статей; 3.2) перечень санкций согласно статьям. Задание №2. Индивидуальное задание №2 включает в себя самостоятельное изучение раздела курса, посвященного компьютерным правонарушениям. В задании необходимо привести не менее 4-5 примеров преступлений в сфере компьютерной информации, как в РФ, так и в зарубежных странах. Привести признаки и элементы состава преступления, расследование компьютерного преступления, особенности основных следственных действий. Описать какие статьи каких законов были нарушены, какую ответственность понесло лицо или группа лиц, совершивших преступление. Дать свои оценки преступлениям. Оценить проблемы судебного преследования за преступления в сфере компьютерной информации. Задание №3 Индивидуальное задание №3 включает в себя разработку проектов нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. Каждый студент для своего индивидуального задания по дисциплине «Комплексное обеспечение информационной безопасности» должен представить в дополнение к Индивидуальному заданию №1 следующий перечень документов: 1) Перечень сведений конфиденциального характера. 2) Перечень лиц допущенных к сведениям конфиденциального характера. 3) Матрица разграничения доступа. 4) Регламент доступа лиц к сведениям ограниченного доступа.

3.2 Темы опросов на занятиях

– Понятие и структура информационной безопасности. Основные задачи системы информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Субъекты и объекты правоотношений в области информационной безопасности. Отрасли законодательства, регламентирующие деятельность по защите информации.

– Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.

– Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной

тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.

– Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты

– Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений. Административные правонарушения.

– Задачи организационного обеспечения информационной безопасности. Роль нормативных документов в защите информации. Инвентаризация информационных ресурсов организации. Построение моделей документооборота и информационных систем. Модели нарушителя информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.

– Структура системы физической защиты. Система охраны периметра. Система сигнализации, видеонаблюдения, контроля доступа: классификация, сферы применения.

– Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.

– Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров. Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества. Организация режима и охраны объектов в процессе транспортировки.

– Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.

3.3 Экзаменационные вопросы

– 1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. 2. Конституционные гарантии прав граждан на информацию и механизм их реализации. 3. Понятие и виды защищаемой информации по законодательству РФ. 4. Государственная тайна как особый вид защищаемой информации. 5. Конфиденциальная информация. 6.Система защиты государственной тайны. 7.Правовой режим защиты государственной тайны. 8. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации. 9. Правовые режимы конфиденциальной информации. 10. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны. 11. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.). 12. Защита интеллектуальной собственности. 13. Правовая регламентация охранной деятельности. 14. Международное законодательство в области защиты информации. 15. Преступления в сфере компьютерной информации. 16. Экспертиза преступлений в области компьютерной информации. 17. Криминалистические аспекты проведения расследований.

3.4 Темы лабораторных работ

– 1. Методика изучения персонала, допущенного к работе с конфиденциальной информацией 2. Порядок изучение материальных и финансовых ценностей, как объекта защиты 3. Защита информации на предприятии 4. Разглашение информации, способы и методы их предотвращения 5. Утечка информации, способы НСД к конфиденциальной информации 6. Предупреждение утечки информации, способы и методы 7. Мероприятия по восстановлению утерянной информации 8. Организационные мероприятия по защите территории и объектов 9. Порядок использования аппаратуры, предназначенной для обработки конфиденциальной информации 10. Масштабность защитных мероприятий (объектовая, индивидуальная) их характеристика и организация проведения.

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. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 1. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 214[2] с. : табл. - ISBN 978-5-91191-053-5 (наличие в библиотеке ТУСУР - 81 экз.)

2. Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 2. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 194[2] с. : табл. - ISBN 978-5-91191-054-5 (наличие в библиотеке ТУСУР - 81 экз.)

4.2. Дополнительная литература

1. Информационная безопасность предприятия : Учебное пособие / А. А. Садердинов, В. А. Трайнёв, А. А. Федулов ; Международная академия информации,информационных процессов и технологий. - 3-е изд. - М. : Дашков и К°, 2006. - 335[1] с. : ил., табл. - Библиогр.: с. 326-331. - ISBN 5-94798-918-2 (наличие в библиотеке ТУСУР - 19 экз.)

2. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 1. - Томск : ТУСУР, 2005. - 221 с. (наличие в библиотеке ТУСУР - 83 экз.)

3. Организационное обеспечение информационной безопасности : курс лекций для студентов специальности 090105 "Комплексное обеспечение информационной безопасности АС" / Г. А. Праскурин ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005 - . Ч. 2. - Томск : ТУСУР, 2005. - 180 с. : ил. - Библиогр.: с. 179-180. (наличие в библиотеке ТУСУР - 82 экз.)

4. Организационно-правовое обеспечение информационной безопасности [Текст] :

учебное пособие для вузов / А. А. Стрельцов [и др.] ; ред. А. А. Стрельцов. - М. : Академия, 2008. - 256 с. : табл. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 242-245. - ISBN 978-5-7695-4240-4 (наличие в библиотеке ТУСУР - 1 экз.)

4.3. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2506, свободный.

4.4. Ресурсы сети Интернет

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Справочно-правовая система (СПС) КонсультантПлюс.
2. 2. Справочно-правовая система (СПС) ГАРАНТ.