МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **2**
Семестр: **4**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	32	32	часов
2	Практические занятия	24	24	часов
3	Всего аудиторных занятий	56	56	часов
4	Из них в интерактивной форме	14	14	часов
5	Самостоятельная работа	52	52	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: 4 семестр

Томск 2017

Согласована на портале № 18545

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «17» 4 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.04 Информационно-аналитические системы безопасности, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

профессор кафедра БИС	_____	Р. В. Мещеряков
инженер кафедра КИБЭВС	_____	А. Ю. Исхаков

Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

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

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

Эксперты:

доцент кафедра КИБЭВС	_____	А. А. Конев

Согласована на портале № 18545

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

приобрести навыки анализа угроз информационной безопасности

рассмотреть основные общеметодологические принципы теории информационной безопасности

изучение методов и средств обеспечения информационной безопасности

изучение методов 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 «Основы информационной безопасности» (Б1.Б.7) относится к блоку 1 (базовая часть).

Последующими дисциплинами являются: Безопасность операционных систем, Безопасность программного обеспечения.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- ОПК-5 способностью использовать нормативные правовые акты в своей профессиональной деятельности;

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 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		4 семестр
Аудиторные занятия (всего)	56	56
Лекции	32	32
Практические занятия	24	24

Согласована на портале № 18545

Из них в интерактивной форме	14	14
Самостоятельная работа (всего)	52	52
Выполнение индивидуальных заданий	15	15
Проработка лекционного материала	10	10
Написание рефератов	6	6
Подготовка к практическим занятиям, семинарам	21	21
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
4 семестр					
1 Понятие информационной безопасности, ее роль в национальной безопасности	4	0	7	11	ОК-5
2 Терминологические основы информационной безопасности	4	4	5	13	ОК-5, ОПК-5
3 Угрозы. Классификация и анализ угроз информационной безопасности	4	4	9	17	ОК-5, ОПК-5
4 Модель угроз, модель нарушителя	6	4	11	21	ОК-5, ОПК-5
5 Модели оценки угроз конфиденциальности, целостности, доступности	6	6	6	18	ОК-5, ОПК-5
6 Функции и задачи защиты информации	4	4	10	18	ОК-5, ОПК-5
7 Проблемы региональной информационной безопасности	4	2	4	10	ОК-5, ОПК-5
8 Обсуждение результатов тестового опроса по курсу «Основы информационной безопасности»	0	0	0	0	
Итого за семестр	32	24	52	108	
Итого	32	24	52	108	

Согласована на портале № 18545

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
4 семестр			
1 Понятие информационной безопасности, ее роль в национальной безопасности	Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи. Национальные интересы Российской Федерации в информационной сфере. Приоритетные направления в области защиты информации в Российской Федерации. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы. Правовое обеспечение защиты информации. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.	4	ОК-5
	Итого	4	
2 Терминологические основы информационной безопасности	Понятие информации и смежных ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление. Идентифика-ция, аутентификация, авторизация	4	ОК-5, ОПК-5
	Итого	4	
3 Угрозы. Классификация и анализ угроз информационной безопасности	Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.Характер происхождения угроз: умышленные факто-	4	ОК-5, ОПК-5

Согласована на портале № 18545

	ры, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.		
	Итого	4	
4 Модель угроз, модель нарушителя	Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные не-преднамеренные.Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.Формирование модели нарушителя.	6	ОК-5, ОПК-5
	Итого	6	
5 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. Фундаментальных требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации. Требования разделены на три группы: стратегия, подотчетность, гарантии. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.	6	ОК-5, ОПК-5
	Итого	6	
6 Функции и задачи защиты информации	Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение ин-	4	ОК-5, ОПК-5

Согласована на портале № 18545

	формации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека		
	Итого	4	
7 Проблемы региональной информационной безопасности	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	4	ОК-5, ОПК-5
	Итого	4	
Итого за семестр		32	

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
Последующие дисциплины								
1 Безопасность операционных систем			+		+	+		
2 Безопасность программного обеспечения	+	+	+	+	+	+		

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	

Согласована на портале № 18545

ОК-5	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Опрос на занятиях, Реферат, Отчет по практическому занятию
ОПК-5	+	+	+	Контрольная работа, Домашнее задание, Отчет по индивидуальному заданию, Опрос на занятиях, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

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

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

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
4 семестр			
Презентации с использованием интерактивной доски с обсуждением		2	2
Презентации с использованием слайдов с обсуждением	2	4	6
Разработка проекта	4		4
Презентации с использованием мультимедиа с обсуждением		2	2
Итого за семестр:	6	8	14
Итого	6	8	14

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
4 семестр			
2 Терминологические основы информационной безопасности	Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы.	4	ОК-5, ОПК-5
	Итого	4	
3 Угрозы. Классификация и анализ угроз информационной безопасности	Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации	4	ОК-5, ОПК-5
	Итого	4	

Согласована на портале № 18545

4 Модель угроз, модель нарушителя	Построение моделей угроз, нарушителя для выбранного объекта защиты.	4	ОК-5, ОПК-5
	Итого	4	
5 Модели оценки угроз конфиденциальности, целостности, доступности	Построение модели угроз для выбранного объекта информатизации	6	ОПК-5
	Итого	6	
6 Функции и задачи защиты информации	Оценка безопасности информации на объектах ее обработки	4	ОПК-5
7 Проблемы региональной информационной безопасности	Итого	4	ОК-5, ОПК-5
	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	2	
	Итого	2	
Итого за семестр		24	

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
4 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности	Написание рефератов	6	ОК-5	Домашнее задание, Опрос на занятиях, Реферат
	Проработка лекционного материала	1		
	Итого	7		
2 Терминологические основы информационной безопасности	Подготовка к практическим занятиям, семинарам	3	ОК-5, ОПК-5	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	5		
3 Угрозы. Классификация и анализ угроз информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ОК-5, ОПК-5	Домашнее задание, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Выполнение индивидуальных заданий	6		
	Итого	9		
4 Модель угроз, модель	Подготовка к практиче-	4	ОК-5,	Опрос на занятиях, От-

Согласована на портале № 18545

нарушителя	ским занятиям, семинарам		ОПК-5	чет по индивидуальному заданию, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Выполнение индивидуальных заданий	6		
	Итого	11		
5 Модели оценки угроз конфиденциальности, целостности, доступности	Подготовка к практическим занятиям, семинарам	4	ОК-5, ОПК-5	Контрольная работа, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
6 Функции и задачи защиты информации	Подготовка к практическим занятиям, семинарам	6	ОК-5, ОПК-5	Контрольная работа, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Выполнение индивидуальных заданий	3		
	Итого	10		
7 Проблемы региональной информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ОК-5, ОПК-5	Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		
Итого за семестр		52		
	Подготовка и сдача экзамена	36		Экзамен
Итого		88		

9.1. Темы индивидуальных заданий

1. Анализ безопасности информации
2. Создание 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
4 семестр				
Контрольная работа	10		10	20

Согласована на портале № 18545

Опрос на занятиях			5	5
Отчет по индивидуальному заданию	10	10	10	30
Отчет по практическому занятию			5	5
Реферат			10	10
Итого максимум за период	20	10	40	70
Экзамен				30
Нарастающим итогом	20	30	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. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая ли-ния-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5171

2. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-6150-4 (наличие в библиотеке ТУСУР - 21 экз.)

3. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью".

Согласована на портале № 18545

Вы-пуск 2 [Электронный ресурс] : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179 — Загл. с экрана [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5179

12.2. Дополнительная литература

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5163
2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5114

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Основы информационной безопасности: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.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. http://www.iqlib.ru - электронная интернет библиотека;
2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. http://www.elibrary.ru - научная электронная библиотека;
4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. http://www.sec.ru – каталог организаций в сфере информационной безопасности

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 лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 808. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Аудиосистема – 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор Optoma – 1 шт.; Компьютер лекционный ASUS ASRock AMD E2-1800/4 ГБ – 1 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 7 SP1; Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебно-

Согласована на портале № 18545

го оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 407. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 - 2 штуки по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E. с широкополосным доступом в Internet, – 6 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP3; Visual Studio 2010; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

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

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

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

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

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

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями	Собеседование по вопросам к зачету,	Преимущественно устная проверка

Согласована на портале № 18545

зрения	опрос по терминам	(индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 18545

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

Основы информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль): **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, кафедра безопасности информационных систем**
Курс: **2**
Семестр: **4**

Учебный план набора 2012 года

Разработчики:
- профессор кафедра БИС Р. В. Мещеряков
- инженер кафедра КИБЭВС А. Ю. Исхаков

Экзамен: 4 семестр

Томск 2017

Согласована на портале № 18545

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-5	способностью использовать нормативные правовые акты в своей профессиональной деятельности	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;
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	

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

Согласована на портале № 18545

уровень)		для выполнения простых задач	

2 Реализация компетенций

2.1 Компетенция ОПК-5

ОПК-5: способностью использовать нормативные правовые акты в своей профессиональной деятельности.

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	-сущность и понятие информационной безопасности и характеристику ее составляющих; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	- классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	профессиональной терминологией в области информационной безопасности.
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	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен;	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Отчет по практическому занятию; • Экзамен;	• Домашнее задание; • Отчет по индивидуальному заданию; • Отчет по практическому занятию; • 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 по методам защиты информации и способам их при-	• Обладает методами защиты информации;	• Способен описывать любые системы, определяя для них угрозы, а также предлагать способы защиты необ-

Согласована на портале № 18545

	менения;		ходимые и достаточные для необходимого уровня защиты информации;
Хорошо (базовый уровень)	• Знает ключевые моменты, понимает значимость защиты информации, о непрерывности процессов по защите информации;	• Обладает практическими умениями по анализу угроз и определению необходимых способов защиты;	• Способен описывать любые системы, определяя для них угрозы, а также предлагать способы защиты;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, позволяющими осуществлять первичный анализ необходимости защиты информации;	• Способен определить перечень возможных угроз системы;

2.2 Компетенция ОК-5

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

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	место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;	оценить значимость защиты информации в масштабах системы, организации, страны;	основными терминами в области информационной безопасности.
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	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Реферат;	• Контрольная работа; • Домашнее задание; • Отчет по индивидуальному заданию; • Опрос на занятиях; • Реферат;	• Домашнее задание; • Отчет по индивидуальному заданию; • Реферат; • Отчет по практическому занятию;

Согласована на портале № 18545

	• Отчет по практическому занятию; • Экзамен;	• Отчет по практическому занятию; • Экзамен;	• 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 знаниями о месте и роли информационной безопасности в рамках решения различных задач, в том числе связанных с защитой государства;	• Умеет анализировать уровень защищенности информации в масштабах системы, организации, страны;	• Владеет основными терминами в области информационной безопасности;
Хорошо (базовый уровень)	• Знает ключевые моменты в области информационной безопасности, понимает значимость защиты информации;	• Ориентируется в анализе систем информационной безопасности;	• Владеет частью основных терминов в области информационной безопасности;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, позволяющими осуществлять первичный анализ необходимости защиты информации;	• Имеет общее представление о терминах, используемых в области информационной безопасности;

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

- Структура органов государственной власти, регламентирующая деятельность по защите информации в РФ
- Современные способы идентификации и аутентификации в информационных системах
- Анализ руководящих документов по оценке защищенности автоматизированных систем

3.2 Темы домашних заданий

- Определение каналов несанкционированного доступа для личного компьютера (ноутбука)
- Построение модели нарушителя для ИСПДн

3.3 Темы индивидуальных заданий

- Одиночно стоящий компьютер в бухгалтерии.
- Сервер в бухгалтерии
- Почтовый сервер
- Веб-сервер
- Компьютерная сеть материальной группы
- Одноранговая локальная сеть без выхода в Интернет
- Одноранговая локальная сеть с выходом в Интернет
- Сеть с выделенным сервером без выхода в Интернет

Согласована на портале № 18545

– Сеть с выделенным сервером с выхода в Интернет
– Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях
– Телефонная сеть
– Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры)
– Банковские операции (внесение денег на счет и снятие)
– Операции с банковскими пластиковыми карточками
– Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия
– Компьютер, хранящий конфиденциальную информацию о разработках предприятия
– Материалы для служебного пользования на твердых носителях в производстве
– Материалы для служебного пользования на твердых носителях на закрытом предприятии
– Материалы для служебного пользования на твердых носителях в архиве
– Материалы для служебного пользования на твердых носителях в налоговой инспекции
– Комната для переговоров по сделкам на охраняемой территории
– Комната для переговоров по сделкам на неохраняемой территории
– Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.)
– Судебные материалы (твердая копия)
– Паспортный стол РОВД
– Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.)
– Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.)
– Сведения по тоталитарным сектам и другим общественно-вредным организациям
– Сведения по общественно-полезным организациям (красный крест и др.)
– Партийные списки и руководящие документы

3.4 Темы опросов на занятиях

– Понятие информации и смежных ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление. Идентифика-ция, аутентификация, авторизация

– Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.

– Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные не-преднамеренные. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Формирование модели нарушителя.

– Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к реше-

Согласована на портале № 18545

нию задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека

3.5 Темы контрольных работ

- Создание системы защиты

3.6 Экзаменационные вопросы

- Теория защиты информации. Основные направления
- Обеспечение информационной безопасности и направления защиты
- Комплексность (целевая, инструментальная, структурная, функциональная, временная)
- Требования к системе защиты информации
- Угрозы информации
- Виды угроз. Основные нарушения
- Характер происхождения угроз
- Источники угроз. Предпосылки появления угроз
- Система защиты информации
- Классы каналов несанкционированного получения информации
- Причины нарушения целостности информации
- Методы и модели оценки уязвимости информации
- Общая модель воздействия на информацию
- Общая модель процесса нарушения физической целостности информации
- Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
- Методологические подходы к оценке уязвимости информации
- Модель защиты системы с полным перекрытием
- Рекомендации по использованию моделей оценки уязвимости информации
- Допущения в моделях оценки уязвимости информации
- Методы определения требований к защите информации
- Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
- Классификация требований к средствам защиты информации
- Требования к защите, определяемые структурой автоматизированной системы обработки данных
- Требования к защите, обуславливаемые видом защищаемой информации
- Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации
- Анализ существующих методик определения требований к защите информации
- Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения
- Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации",выпущенном в 1992 году. Часть 1
- Классы защищенности средств вычислительной техники от несанкционированного доступа
- Функции защиты информации
- Стратегии защиты информации
- Способы и средства защиты информации
- Способы "абсолютной системы защиты"
- Архитектура систем защиты информации. Требования
- Общеметодологических принципов архитектуры системы защиты информации
- Построение средств защиты информации
- Ядро системы защиты

Согласована на портале № 18545

– Семирубежная модель защиты

– Средства защиты информации. Антивирусы, средства анализа защищенности, средства обнаружения вторжений

– Регуляторы в области защиты информации

3.7 Вопросы для подготовки к практическим занятиям, семинарам

– Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы.

– Оценка безопасности информации на объектах ее обработки

– Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации

– Построение модели угроз для выбранного объекта информатизации

– Построение моделей угроз, нарушителя для выбранного объекта защиты.

– Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.

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. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая ли-ния-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5171

2. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-6150-4 (наличие в библиотеке ТУСУР - 21 экз.)

3. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Вы-пуск 2 [Электронный ресурс] : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5179 — Загл. с экрана [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5179

4.2. Дополнительная литература

1. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5163 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5163

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/books/element.php?pl1_id=5114

4.3. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Основы информационной безопасности: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf

Согласована на портале № 18545

4.4. Базы данных, информационно справочные и поисковые системы

1. http://www.iqlib.ru - электронная интернет библиотека;
2. http://www.biblioclub.ru – полнотекстовая электронная библиотека;
3. http://www.elibrary.ru - научная электронная библиотека;
4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
5. http://www.sec.ru – каталог организаций в сфере информационной безопасности

Согласована на портале № 18545