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

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **4**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	16	16	часов
2	Практические занятия	24	24	часов
3	Всего аудиторных занятий	40	40	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	32	32	часов
6	Всего (без экзамена)	72	72	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Экзамен: 4 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «24» 1 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. РЗИ _____ А. В. Лячин

Заведующий обеспечивающей каф.
РЗИ _____ А. С. Задорин

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

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперты:

Старший преподаватель каф. РЗИ _____ Ю. В. Зеленецкая

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование у студентов ТУСУР целостного представления о сущности и значении информационной безопасности и защиты информации, их места в системе национальной безопасности;

определение моделей, стратегий и систем обеспечения безопасности информации;

классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

1.2. Задачи дисциплины

– раскрытие понятийного аппарата в области информационной безопасности и защиты информации;

– раскрытие базовых содержательных положений в области информационной безо-пасности и защиты информации;

– раскрытие современной доктрины информационной безопасности;

– определение целей и принципов защиты информации;

– установление факторов, влияющих на защиту информации;

– раскрытие методов определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам;

– установление структуры угроз защищаемой информации;

– установление и раскрытие сущности компонентов защиты информации;

– раскрытие назначения, сущности и структуры систем защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» (Б1.Б.14) относится к блоку 1 (базовая часть).

Последующими дисциплинами являются: Комплексные системы защиты информации на предприятии, Организационное и правовое обеспечение информационной безопасности, Организация и управление службой защиты информации на предприятии, Техническая защита информации, Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

В результате изучения дисциплины студент должен:

– **знать** место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы организационной защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации.

– **уметь** анализировать и оценивать угрозы информационной безопасности для различных объектов.

– **владеть** профессиональной терминологией, методами и средствами выявления угроз безопасности автоматизированным системам; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		4 семестр
Аудиторные занятия (всего)	40	40

Лекции	16	16
Практические занятия	24	24
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	32	32
Проработка лекционного материала	8	8
Подготовка к практическим занятиям, семинарам	24	24
Всего (без экзамена)	72	72
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
4 семестр					
1 Место информационной безопасности в системе национальной безопасности	4	8	10	22	ОПК-7
2 Теория информационной безопасности	2	4	5	11	ОПК-7
3 Классификация защищаемой информации	2	2	3	7	ОПК-7
4 Параметры уязвимости защищаемой информации	4	4	6	14	ОПК-7
5 Компоненты и системы защиты информации	4	6	8	18	ОПК-7
Итого за семестр	16	24	32	72	
Итого	16	24	32	72	

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 Место информационной безопасности в системе национальной безопасности	Понятие национальной безопасности. Виды безопасности.Сущность и понятие информационной безопасности, характеристика ее составляющих.Информационная безопасность в системе национальной безопасности.Государственная информационная политика. Современная концепция информационной безопасности.	4	ОПК-7
	Итого	4	
2 Теория информационной безопасности	Основные понятия, общеметодологические принципы теории информационной безопасности.Анализ угроз информационной безопасности.Методы и средства обеспечения информационной безопасности.	2	ОПК-7
	Итого	2	
3 Классификация защищаемой информации	Виды защищаемой информации.Критерии, условия и принципы отнесения информации к защищаемой.Носители защищаемой информации.	2	ОПК-7
	Итого	2	
4 Параметры уязвимости защищаемой информации	Методы нарушения конфиденциальности, целостности и доступности информации. Понятие и структура угроз защищаемой информации; источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. Виды уязвимости информации и формы ее проявления. Каналы и методы несанкционированного доступа к конфиденциальной информации.	4	ОПК-7
	Итого	4	
5 Компоненты и системы защиты информации	Основы комплексного обеспечения информационной безопасности: методологические подходы к защите информации и принципы ее организации.- Объекты защиты. Виды защиты. Классификация методов и средств защиты информации. Модели, стратегии и системы обеспечения информационной безопасности: кадровое и ресурсное обеспечение защиты информации; системы защиты информации.Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	4	ОПК-7
	Итого	4	
Итого за семестр		16	

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
Последующие дисциплины					
1 Комплексные системы защиты информации на предприятии					+
2 Организационное и правовое обеспечение информационной безопасности	+	+			+
3 Организация и управление службой защиты информации на предприятии		+	+	+	+
4 Техническая защита информации			+	+	+
5 Управление информационной безопасностью	+	+	+	+	+

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	
ОПК-7	+	+	+	Отчет по индивидуальному заданию, Экзамен, Коллоквиум, Опрос на занятиях, Выступление (доклад) на занятии

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			
Мозговой штурм	2	2	4
Решение ситуационных задач	4	2	6

Презентации с использованием мультимедиа с обсуждением		2	2
Работа в команде	2		2
Case-study (метод конкретных ситуаций)	2	2	4
Разработка проекта	2		2
Итого за семестр:	12	8	20
Итого	12	8	20

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Место информационной безопасности в системе национальной безопасности	Анализ терминов и определений информационной безопасности. Доктрина информационной безопасности РФ	2	ОПК-7
	Концепция национальной безопасности РФ. Виды безопасности. Место информационной безопасности в системе национальной безопасности	2	
	Информационный ресурс и государственная информационная политика. Информационная война и информационное оружие	2	
	Проблемы информационной безопасности в сфере регионального и муниципального управления	2	
	Итого	8	
2 Теория информационной безопасности	Законодательство РФ в сфере информационной безопасности и защиты информации	2	ОПК-7
	Каналы несанкционированного доступа к защищаемой информации	2	
	Итого	4	
3 Классификация защищаемой информации	Виды информации	2	ОПК-7
	Итого	2	
4 Параметры уязвимости защищаемой информации	Угрозы информации. Уязвимость информации	2	ОПК-7
	Методы и модели оценки уязвимости	2	

	информации. Модели нейтрализации угроз		
	Итого	4	
5 Компоненты и системы защиты информации	Функции и задачи защиты информации. Стратегии, способы и средства защиты информации	2	ОПК-7
	Классификация автоматизированных систем обработки информации по классу защиты информации	2	
	Архитектура систем защиты информации	2	
	Итого	6	
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 Место информационной безопасности в системе национальной безопасности	Подготовка к практическим занятиям, семинарам	2	ОПК-7	Выступление (доклад) на занятии, Коллоквиум, Опрос на занятиях, Экзамен
	Подготовка к практическим занятиям, семинарам	2		
	Подготовка к практическим занятиям, семинарам	2		
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Итого	10		
2 Теория информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ОПК-7	Выступление (доклад) на занятии, Коллоквиум, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	1		

	Итого	5		
3 Классификация защищаемой информации	Подготовка к практическим занятиям, семинарам	2	ОПК-7	Выступление (доклад) на занятии, Коллоквиум, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
4 Параметры уязвимости защищаемой информации	Подготовка к практическим занятиям, семинарам	2	ОПК-7	Выступление (доклад) на занятии, Коллоквиум, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Итого	6		
5 Компоненты и системы защиты информации	Подготовка к практическим занятиям, семинарам	2	ОПК-7	Выступление (доклад) на занятии, Коллоквиум, Опрос на занятиях, Отчет по индивидуальному заданию, Экзамен
	Подготовка к практическим занятиям, семинарам	2		
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	2		
	Итого	8		
Итого за семестр		32		
	Подготовка и сдача экзамена	36		Экзамен
Итого		68		

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				
Выступление (доклад) на занятии	5	5	5	15
Коллоквиум	10	10		20

Опрос на занятиях	5	5	5	15
Отчет по индивидуальному заданию			20	20
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	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. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с. (наличие в библиотеке ТУСУР - 51 экз.)

2. Информационная безопасность и защита информации: Учебное пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; ред.: С.А. Клейменов. – М.: Academia, 2006. – 330 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.2. Дополнительная литература

1. Методологические, организационные и правовые основы информационной безопасности: В 3 ч. / В.Н. Ильюшенко [и др.]; ред.: В.Н. Ильюшенко. – Томск: Изд-во Института оптики атмосферы СО РАН, 2005. – 474 с. (наличие в библиотеке ТУСУР - 37 экз.)

2. Технические средства защиты информации: Курс лекций / Волегов К. А., Бацула А. П., Литвинов Р. В. - 2006. 169 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/949, дата обращения: 21.03.2017.

3. Основы информационной безопасности: Учебное пособие / Голиков А. М. - 2007. 201 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1024, дата обращения: 21.03.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Технические средства защиты информации: Учебное пособие / Титов А. А. - 2010. 194 с. (данное издание рекомендовано к СРС) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/653, дата обращения: 21.03.2017.
2. Инженерно-техническая защита информации: Учебное пособие / Титов А. А. - 2010. 195 с. (данное издание рекомендовано к СРС) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/654, дата обращения: 21.03.2017.
3. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (данное издание рекомендовано для практических занятий) (наличие в библиотеке ТУСУР - 25 экз.)
4. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. (данное издание рекомендовано для практических занятий) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, дата обращения: 21.03.2017.

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

1. Научно-образовательный портал ТУСУР: https://edu.tusur.ru/.
2. Специального программного обеспечения не требуется.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебная аудитория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 74. Состав оборудования: Учебная мебель, с количеством посадочных мест не менее 22-24; доска магнитно-маркерная -1шт.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компью-

теры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

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

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

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

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

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

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

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

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

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

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

- в печатной форме;
- в печатной форме с увеличенным шрифтом;

– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

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

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **4**

Учебный план набора 2013 года

Разработчики:
- доцент каф. РЗИ А. В. Лячин

Экзамен: 4 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Должен знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы организационной защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации.; Должен уметь анализировать и оценивать угрозы информационной безопасности для различных объектов.; Должен владеть профессиональной терминологией, методами и средствами выявления угроз безопасности автоматизированным системам; навыками организации и обеспечения режима секретности; 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 ОПК-7

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы

безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

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	угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	определять информационные ресурсы, подлежащие защите; определять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	способностью определять информационные ресурсы, подлежащие защите; способностью определять угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
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 индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Коллоквиум; • Экзамен;	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Коллоквиум; • Экзамен;	• Отчет по индивидуальному заданию; • Выступление (доклад) на занятии; • Коллоквиум; • 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)	• Все виды и формы информационных ресурсов, подлежащих защите;; • виды угроз безопасности информации и возможные методы и пути реализации угроз;; • методы анализа структуры и содержания информационных	• Определять виды и формы информационных ресурсов, подлежащих защите;; • анализировать возможные методы и пути реализации угроз информации;; • проводить анализ структуры и содержания информационных	• Способностью определять виды и формы информационных ресурсов, подлежащих защите;; • способностью определять виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информа-

	процессов объекта защиты;; • способы определения особенностей функционирования объекта защиты.;	процессов предприятия;; • определять особенностей функционирования объекта защиты.;	ционных процессов предприятия и особенностей функционирования объекта защиты. ;
Хорошо (базовый уровень)	• Представляет все виды и формы информационных ресурсов, подлежащих защите и пути реализации возможных угроз;; • понимает возможности всех методов анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;; • имеет глубокое представление о положениях предметной области знания.;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования;; • применяет изученные методы решения задач в незнакомых ситуациях;; • умеет корректно выражать и аргументированно обосновывать положения предметной области знания. ;	• Приспосабливает свои действия к обстоятельствам в решении проблем;; • критически осмысливает полученные знания;; • компетентен в различных ситуациях;; • владеет разными способами представления информации.;
Удовлетворительно (пороговый уровень)	• воспроизводит основные положения предметной области знания;; • дает определения основных понятий;; • знает основные методы анализа угроз информации и умеет их применять на практике.; • Распознает виды и формы информационных ресурсов, подлежащих защите и пути реализации возможных угроз;;	• Умеет работать со справочной литературой;; • умеет представлять результаты своей работы;; • обладает основными умениями, требуемыми для выполнения простых задач. ;	• Работает при прямом наблюдении; ; • владеет терминологией предметной области знания;; • способен корректно представить знания и результаты своей деятельности.;

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 коллоквиумов

– Коллоквиум по курсу Основы информационной безопасности Билет № 3 1. Что такое Доктрина информационной безопасности РФ? Для чего она предназначена? 2. ФЗ «Об информации, информационных технологиях и о защите информации». Что регулирует данный закон в сфере информационных отношений? 3. Дайте определение следующему термину: «Техника защиты информации».

3.2 Темы индивидуальных заданий

– Индивидуальные задания состоят из двух частей, взаимосвязанных друг с другом по

объекту защиты информации. Объект необходимо исследовать таким образом, чтобы можно было применить все основные элементы защиты информации, т.е. определяя местоположение, внешние и внутренние характеристики с учетом естественных событий. Однако уточнение характеристик не должно приводить к абсолютной конкретизации объекта, т.к. в этом случае будет затруднен анализ объекта. Сдача индивидуальных заданий происходит в конце семестра на последних практических занятиях. Первое задание Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам: 1. виды угроз; 2. характер происхождения угроз; 3. классы каналов несанкционированного получения информации; 4. источники появления угроз; 5. причины нарушения целостности информации; 6. потенциально возможные злоумышленные действия; 7. определить класс защиты информации. Второе задание Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам: 1. определить требования к защите информации; 2. классифицировать автоматизированную систему; 3. определить факторы, влияющие на требуемый уровень защиты информации; 4. выбрать или разработать способы и средства защиты информации; 5. построить архитектуру систем защиты информации; 6. сформулировать рекомендации по увеличению уровня защищенности. Примеры наименования объекта защиты информации: 1. Телефонная сеть. 2. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры). 3. Банковские операции (внесение денег на счет и снятие). 4. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия. 5. Компьютер, хранящий конфиденциальную информацию о разработках предприятия. 6. Материалы для служебного пользования на твердых носителях в производстве. 7. Материалы для служебного пользования на твердых носителях в архиве. 8. Комната для переговоров по сделкам на охраняемой территории. 9. Судебные материалы (твердая копия). 10. Паспортный стол РОВД. 11. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.). 12. Партийные списки и руководящие документы. Наименование объекта защиты информации может быть предложено студентом и согласовано с преподавателем.

3.3 Темы опросов на занятиях

– Понятие национальной безопасности. Виды безопасности. Сущность и понятие информационной безопасности, характеристика ее составляющих. Информационная безопасность в системе национальной безопасности. Государственная информационная политика. Современная концепция информационной безопасности.

– Основные понятия, общеметодологические принципы теории информационной безопасности. Анализ угроз информационной безопасности. Методы и средства обеспечения информационной безопасности.

– Виды защищаемой информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации.

– Методы нарушения конфиденциальности, целостности и доступности информации. Понятие и структура угроз защищаемой информации; источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. Виды уязвимости информации и формы ее проявления. Каналы и методы несанкционированного доступа к конфиденциальной информации.

– Основы комплексного обеспечения информационной безопасности: методологические подходы к защите информации и принципы ее организации. Объекты защиты. Виды защиты. Классификация методов и средств защиты информации. Модели, стратегии и системы обеспечения информационной безопасности: кадровое и ресурсное обеспечение защиты информации; системы защиты информации. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

3.4 Темы докладов

– 1. Доктрина информационной безопасности РФ. 2. Определение информационной безопасности согласно «ДИБ РФ» 4. Национальные интересы РФ в информационной сфере. 5. Интересы личности, общества и государства в информационной сфере. 6. Виды угроз ИБ РФ. В чем они заключаются? 7. Основные задачи по обеспечению информационной безопасности РФ. 8. Методы обеспечения информационной безопасности РФ. 9. Особенности обеспечения ИБ РФ в различных сферах. 10. Государственная политика обеспечения информационной безопасности РФ. 11.

Основные функции системы обеспечения информационной безопасности РФ. 12. Основные элементы системы обеспечения информационной безопасности РФ. Их функции и обязанности.

– 1. Законы, устанавливающие правила и процедуры обеспечения информационной безопасности.

– 1. Перечислите основные виды информации. 2. Сформулируйте основные свойства информации. 3. Дайте определение конфиденциальной информации. 4. Дайте определение и перечислите уровни секретности государственной тайны. 5. Раскройте сущность информации как объекта права собственности. 6. Раскройте сущность объекта защиты. 7. Составьте классификацию угроз информационной безопасности. 8. Раскройте основные группы классификации. 9. На основании чего строится модель нарушителя информационной безопасности? 10. Перечислите возможные каналы неправомерного и несанкционированного доступа к защищаемой информации.

– 1. Дайте определение понятию защита информации. 2. Что понимается под термином безопасность информации? 3. Что включает в себя защита информации? 4. Какие цели преследует защита информации? 5. Работы, в каких направлениях необходимы для достижения целей защиты информации на объектах защиты? 6. Что представляет собой политика безопасности организации? Какие мероприятия она подразумевает? 7. Какие мероприятия подразумевает процедура анализа рисков? 8. Что необходимо учитывать при оценивании рисков? 9. Что представляет собой программа безопасности организации? Какие меры должны быть в ней предусмотрены? 10. Какие группы процедурных мер Вы знаете? 11. Какие механизмы программно-технического уровня Вы знаете?

– 1. Основные принципы построения системы защиты информации. 2. Основные методы защиты информации. 3. Метод минимизации ущерба от случайных факторов. 4. Метод дублирования информации. Способы его реализации. 5. Метод повышения надёжности информационной системы. 6. Метод создания отказоустойчивых информационных систем. 7. Оптимизация взаимодействия пользователей и обслуживающего персонала. Пути её достижения. 8. Методы и средства защиты от шпионажа и диверсий. 9. Методы и средства защиты от электромагнитных наводок и излучений. 10. Методы и средства защиты от несанкционированного доступа к защищаемой информации. 11. Модели защиты информации. Их основная суть. 12. Криптографические методы защиты информации.

3.5 Экзаменационные вопросы

– 1. Теория защиты информации. Основные направления. 2. Обеспечение информационной безопасности и направления защиты. 3. Комплексность (целевая, инструментальная, структурная, функциональная, временная). 4. Требования к системе защиты информации. 5. Угрозы информации. 6. Виды угроз. Основные нарушения. 7. Характер происхождения угроз. 8. Источники угроз. Предпосылки появления угроз. 9. Система защиты информации. 10. Классы каналов несанкционированного получения информации. 11. Причины нарушения целостности информации. 12. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных. 13. Методологические подходы к оценке уязвимости информации. Эмпирический подход к оценке уязвимости информации. 14. Модель защиты системы с полным перекрытием. 15. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации. 16. Методы определения требований к защите информации. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации. 17. Классификация требований к средствам защиты информации. 18. Требования к защите, определяемые структурой автоматизированной системы обработки данных. 19. Требования к защите, обуславливаемые видом защищаемой информации. 20. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации. 21. Анализ существующих методик определения требований к защите информации. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США». Основные положения. 22. Анализ существующих методик определения требований к защите информации. Руководящий документ Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 году. Часть 1. 23. Классы защищенности средств вычислительной техники от несанкционированного доступа. 24. Факторы, влияющие на требуемый уровень защиты информации. 25. Функции и задачи защиты

информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты. 26. Методы формирования функций защиты. 27. Класс задач функций защиты 1 – уменьшение степени распознавания объектов 28. Класс задач функций защиты 2 – защита содержания обрабатываемой, хранимой и передаваемой информации. 29. Класс задач функций защиты 3 – защита информации от информационного воздействия. 30. Функции защиты информации. 31. Стратегии защиты информации. 32. Способы и средства защиты информации. 33. Способы «абсолютной системы защиты». 34. Архитектура систем защиты информации. Требования. Общеметодологические принципы архитектуры системы защиты информации. 35. Построение средств защиты информации. 36. Ядро системы защиты. Ресурсы средства защиты информации 37. Организационное построение. Семирубежная модель защиты.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с. (наличие в библиотеке ТУСУР - 51 экз.)
2. Информационная безопасность и защита информации: Учебное пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; ред.: С.А. Клейменов. – М.: Academia, 2006. – 330 с. (наличие в библиотеке ТУСУР - 30 экз.)

4.2. Дополнительная литература

1. Методологические, организационные и правовые основы информационной безопасности: В 3 ч. / В.Н. Ильюшенко [и др.]; ред.: В.Н. Ильюшенко. – Томск: Изд-во Института оптики атмосферы СО РАН, 2005. – 474 с. (наличие в библиотеке ТУСУР - 37 экз.)
2. Технические средства защиты информации: Курс лекций / Волегов К. А., Бацула А. П., Литвинов Р. В. - 2006. 169 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/949, свободный.
3. Основы информационной безопасности: Учебное пособие / Голиков А. М. - 2007. 201 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1024, свободный.

4.3. Обязательные учебно-методические пособия

1. Технические средства защиты информации: Учебное пособие / Титов А. А. - 2010. 194 с. (данное издание рекомендовано к СРС) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/653, свободный.
2. Инженерно-техническая защита информации: Учебное пособие / Титов А. А. - 2010. 195 с. (данное издание рекомендовано к СРС) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/654, свободный.
3. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (данное издание рекомендовано для практических занятий) (наличие в библиотеке ТУСУР - 25 экз.)
4. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. (данное издание рекомендовано для практических занятий) [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. Научно-образовательный портал ТУСУР: https://edu.tusur.ru/.
2. Специального программного обеспечения не требуется.