

**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**

**Информационная безопасность**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **09.03.04 Программная инженерия**

Направленность (профиль): **Программная инженерия**

Форма обучения: **заочная**

Факультет: **ЗиВФ, Заочный и вечерний факультет**

Кафедра: **АОИ, Кафедра автоматизации обработки информации**

Курс: **4, 5**

Семестр: **8, 9**

Учебный план набора 2012 года

**Распределение рабочего времени**

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	4	12	16	часов
2	Лабораторные работы		20	20	часов
3	Всего аудиторных занятий	4	32	36	часов
4	Самостоятельная работа	32	67	99	часов
5	Всего (без экзамена)	36	99	135	часов
6	Подготовка и сдача экзамена		9	9	часов
7	Общая трудоемкость	36	108	144	часов
		1.0	3.0	4.0	З.Е

Контрольные работы: 9 семестр - 1

Экзамен: 9 семестр

Томск 2017

## ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.04 Программная инженерия, утвержденного 12 марта 2015 года, рассмотрена и утверждена на заседании кафедры « \_\_\_ » \_\_\_\_\_ 20\_\_ года, протокол № \_\_\_\_\_.

Разработчик:

ассистент каф. КИБЭВС \_\_\_\_\_ А. К. Новохрестов

Заведующий обеспечивающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

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

Декан ЗиВФ

\_\_\_\_\_ И. В. Осипов

Заведующий выпускающей каф.  
АОИ

\_\_\_\_\_ Ю. П. Ехлаков

Эксперт:

Директор Центр системного проектирования

\_\_\_\_\_ А. А. Конев

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является изучение комплекса проблем информационной безопасности предприятий и организаций различных типов и направлений деятельности, построения, функционирования и совершенствования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сфере охраны интеллектуальной собственности и сохранности информационных ресурсов.

### 1.2. Задачи дисциплины

- Ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности.
- Обучение студентов работе с основными средствами защиты.
- 

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.В.ОД.14) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика и программирование, Моделирование систем, Правоведение.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-4 владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества;

В результате изучения дисциплины студент должен:

- **знать** базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем; задачи информационной безопасности; законодательство по обеспечению информационной безопасности; стандарты в области информационной безопасности; методы и средства защиты информационной безопасности; направления и методы ведения аналитической работы по выявлению угроз; технические процедуры по действиям в нештатной ситуации; методологии оценки рисков и угроз информационной безопасности.

- **уметь** выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов; оценивать и выбирать необходимые средства защиты; осуществлять мониторинг состояния информационной безопасности объекта; обеспечивать противодействие атакам на информационную систему; выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности;

- **владеть** навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.

## 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	
		8 семестр	9 семестр
Аудиторные занятия (всего)	36	4	32
Лекции	16	4	12
Лабораторные работы	20		20
Самостоятельная работа (всего)	99	32	67

Подготовка к контрольным работам	39	24	15
Оформление отчетов по лабораторным работам	20		20
Проработка лекционного материала	32	8	24
Выполнение контрольных работ	8		8
Всего (без экзамена)	135	36	99
Подготовка и сдача экзамена	9		9
Общая трудоемкость ч	144	36	108
Зачетные Единицы	4.0	1.0	3.0

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
<b>8 семестр</b>					
1 Базовые понятия в сфере обеспечения информационной безопасности.	1	0	2	3	ПК-4
2 Комплексный подход к обеспечению информационной безопасности.	1	0	2	3	ПК-4
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	1	0	2	3	ПК-4
4 Методы оценки рисков и угроз информационной безопасности.	1	0	26	27	ПК-4
Итого за семестр	4	0	32	36	
<b>9 семестр</b>					
5 Программно-аппаратные, технические и криптографические средства защиты информации.	4	20	28	52	ПК-4
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	2	0	4	6	ПК-4
7 Концепция и политика информационной безопасности.	2	0	4	6	ПК-4
8 Реализации стратегии обеспечения информационной безопасности.	4	0	31	35	ПК-4
Итого за семестр	12	20	67	99	

Итого	16	20	99	135	
-------	----	----	----	-----	--

## 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
<b>8 семестр</b>			
1 Базовые понятия в сфере обеспечения информационной безопасности.	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	1	ПК-4
	Итого	1	
2 Комплексный подход к обеспечению информационной безопасности.	Структура системы защиты информации.	1	ПК-4
	Итого	1	
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование.	1	ПК-4
	Итого	1	
4 Методы оценки рисков и угроз информационной безопасности.	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	1	ПК-4
	Итого	1	
Итого за семестр		4	
<b>9 семестр</b>			
5 Программно-аппаратные, технические и криптографические средства защиты информации.	Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа. Мандатное распределение доступа.	4	ПК-4
	Итого	4	
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	Определение организационных требований защиты ИТ.	2	ПК-4
	Итого	2	
7 Концепция и политика информационной безопасности.	Политика безопасности.	2	ПК-4
	Итого	2	
8 Реализации стратегии обеспечения информационной безопасности.	Определение организационных целей и стратегий защиты ИТ. Идентификация и анализ угроз активам ИТ в пределах организации. Определение соответствующих защитных мер.	4	ПК-4
	Итого	4	
Итого за семестр		12	

Итого	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	6	7	8
Предшествующие дисциплины								
1 Информатика и программирование	+							
2 Моделирование систем		+						
3 Правоведение			+					

### 5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Лабораторные работы	Самостоятельная работа	
ПК-4	+	+	+	Контрольная работа, Проверка контрольных работ, Отчет по лабораторной работе, Опрос на занятиях

## 6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

## 7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
5 Программно-аппаратные, технические и криптографические	Защита компьютерной информации на уровне доступа в систему	4	ПК-4

средства защиты информации.	Защита от атак по локальным и глобальным сетям	4	
	Защита от вредоносного ПО	4	
	Использование шифрования для защиты данных	4	
	Использование физических носителей и защитных систем на их основе	4	
	Итого	20	
Итого за семестр		20	
Итого		20	

### 8. Практические занятия (семинары)

Не предусмотрено РУП

### 9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
<b>8 семестр</b>				
1 Базовые понятия в сфере обеспечения информационной безопасности.	Проработка лекционного материала	2	ПК-4	Опрос на занятиях
	Итого	2		
2 Комплексный подход к обеспечению информационной безопасности.	Проработка лекционного материала	2	ПК-4	Опрос на занятиях
	Итого	2		
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	Проработка лекционного материала	2	ПК-4	Опрос на занятиях
	Итого	2		
4 Методы оценки рисков и угроз информационной безопасности.	Проработка лекционного материала	2	ПК-4	Контрольная работа, Опрос на занятиях
	Подготовка к контрольным работам	24		
	Итого	26		
Итого за семестр		32		
<b>9 семестр</b>				
5 Программно-аппаратные,	Проработка лекционного материала	8	ПК-4	Опрос на занятиях, Отчет по лабораторной ра-

технические и криптографические средства защиты информации.	Оформление отчетов по лабораторным работам	20		боте
	Итого	28		
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	Проработка лекционного материала	4	ПК-4	Опрос на занятиях
	Итого	4		
7 Концепция и политика информационной безопасности.	Проработка лекционного материала	4	ПК-4	Опрос на занятиях
	Итого	4		
8 Реализации стратегии обеспечения информационной безопасности.	Выполнение контрольных работ	8	ПК-4	Контрольная работа, Опрос на занятиях, Проверка контрольных работ
	Проработка лекционного материала	8		
	Подготовка к контрольным работам	15		
	Итого	31		
Итого за семестр		67		
	Подготовка и сдача экзамена	9		Экзамен
Итого		108		

### 9.1. Темы контрольных работ

1. Базовые понятия в сфере обеспечения информационной безопасности; комплексный подход к обеспечению информационной безопасности; организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации; методы оценки рисков и угроз информационной безопасности; программно-аппаратные, технические и криптографические средства защиты информации; основные принципы, направления и требования обеспечения информационной безопасности организации; концепция и политика информационной безопасности; реализации стратегии обеспечения информационной безопасности.

### 10. Курсовая работа (проект)

Не предусмотрено РУП

### 11. Рейтинговая система для оценки успеваемости студентов

Не предусмотрено

### 12. Учебно-методическое и информационное обеспечение дисциплины

#### 12.1. Основная литература

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

#### 12.2. Дополнительная литература

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



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

3. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.3. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-1ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf)

### **12.3 Учебно-методические пособия**

#### **12.3.1. Обязательные учебно-методические пособия**

1. «Методические указания к лабораторным и практическим работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_lab.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf)

2. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность» / Сопов М.А., 2012г. – 2 с. [Электронный ресурс] [Электронный ресурс]. - [http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_srs.pdf](http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf)

#### **12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья**

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

##### **Для лиц с нарушениями зрения:**

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

##### **Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

##### **Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

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

1. <http://www.edu.tusur.ru> – образовательный портал университета;
2. <http://www.lib.tusur.ru> – веб-сайт библиотеки университета;
3. <http://www.elibrary.ru> – научная электронная библиотека;
4. <http://www.edu.ru> – веб-сайт системы федеральных образовательных порталов.

## **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, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJ5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

#### **13.1.2. Материально-техническое обеспечение для лабораторных работ**

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель; – 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/

HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.;  
Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

### **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 Celeron D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

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

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

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

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

## **14. Фонд оценочных средств**

### **14.1. Основные требования к фонду оценочных средств и методические рекомендации**

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

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

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

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

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

общемедицинским показаниям	работы, вопросы к зачету, контрольные работы, устные ответы	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.

**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**

**Информационная безопасность**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки (специальность): **09.03.04 Программная инженерия**

Направленность (профиль): **Программная инженерия**

Форма обучения: **заочная**

Факультет: **ЗиВФ, Заочный и вечерний факультет**

Кафедра: **АОИ, Кафедра автоматизации обработки информации**

Курс: **4, 5**

Семестр: **8, 9**

Учебный план набора 2012 года

Разработчик:

– ассистент каф. КИБЭВС А. К. Новохрестов

Экзамен: 9 семестр

Томск 2017

## 1. Введение

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

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

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

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-4	владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	<p>Должен знать базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем; задачи информационной безопасности; законодательство по обеспечению информационной безопасности; стандарты в области информационной безопасности; методы и средства защиты информационной безопасности; направления и методы ведения аналитической работы по выявлению угроз; технические процедуры по действиям в нештатной ситуации; методологии оценки рисков и угроз информационной безопасности. ;</p> <p>Должен уметь выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов; оценивать и выбирать необходимые средства защиты; осуществлять мониторинг состояния информационной безопасности объекта; обеспечивать противодействие атакам на информационную систему; выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности; ;</p> <p>Должен владеть навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.;</p>

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	Обладает диапазоном практических умений,	Контролирует работу, проводит оценку, совершенствует

	ями в пределах изучаемой области с пониманием границ применимости	требуемых для развития творческих решений, абстрагирования проблем	шенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

## 2 Реализация компетенций

### 2.1 Компетенция ПК-4

ПК-4: владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.

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	концепции и атрибуты качества программного обеспечения	применять концепции и атрибуты качества программного обеспечения	навыками применения концепций и атрибутов качества программного обеспечения
Виды занятий	<ul style="list-style-type: none"> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> <li>• Лабораторные работы;</li> </ul>	<ul style="list-style-type: none"> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> <li>• Лабораторные работы;</li> </ul>	<ul style="list-style-type: none"> <li>• Самостоятельная работа;</li> <li>• Лабораторные работы;</li> </ul>
Используемые средства оценивания	<ul style="list-style-type: none"> <li>• Контрольная работа;</li> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Экзамен;</li> </ul>	<ul style="list-style-type: none"> <li>• Контрольная работа;</li> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Экзамен;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Экзамен;</li> </ul>

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)	<ul style="list-style-type: none"> <li>• на продвинутом уровне концепции и атрибуты качества программного обеспечения;</li> </ul>	<ul style="list-style-type: none"> <li>• на продвинутом уровне применять концепции и атрибуты качества программного обеспечения;</li> </ul>	<ul style="list-style-type: none"> <li>• на продвинутом уровне навыками применения концепций и атрибутов качества программного обеспечения;</li> </ul>
Хорошо (базовый уровень)	<ul style="list-style-type: none"> <li>• концепции и атрибуты качества программного обеспечения;</li> </ul>	<ul style="list-style-type: none"> <li>• применять концепции и атрибуты качества программного обеспе-</li> </ul>	<ul style="list-style-type: none"> <li>• навыками применения концепций и атрибутов качества про-</li> </ul>

		чения;	граммного обеспечения;
Удовлетворительный (пороговый уровень)	<ul style="list-style-type: none"> <li>на базовом уровне концепции и атрибуты качества программного обеспечения;</li> </ul>	<ul style="list-style-type: none"> <li>на базовом уровне применять концепции и атрибуты качества программного обеспечения;</li> </ul>	<ul style="list-style-type: none"> <li>на базовом уровне навыками применения концепций и атрибутов качества программного обеспечения;</li> </ul>

### 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 контрольных работ

– Базовые понятия в сфере обеспечения информационной безопасности; комплексный подход к обеспечению информационной безопасности; организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации; методы оценки рисков и угроз информационной безопасности; программно-аппаратные, технические и криптографические средства защиты информации; основные принципы, направления и требования обеспечения информационной безопасности организации; концепция и политика информационной безопасности; реализации стратегии обеспечения информационной безопасности.

#### 3.2 Темы опросов на занятиях

– Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.

– Структура системы защиты информации.

– Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование.

– Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.

– Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа.

– Мандатное распределение доступа.

– Определение организационных требований защиты ИТ.

– Политика безопасности.

– Определение организационных целей и стратегий защиты ИТ. Идентификация и анализ угроз активам ИТ в пределах организации. Определение соответствующих защитных мер.

#### 3.3 Темы контрольных работ

– 1. Основные понятия информационной безопасности. Организационно-правовое обеспечение информационной безопасности.

– 2. Оценка рисков. Программно-аппаратные средства защиты информации.

– 3. Политика безопасности. Менеджмент информационной безопасности.

#### 3.4 Экзаменационные вопросы

– 1. Основные регуляторы 2. Основные нормативно-правовые акты 3. Определения: информация, безопасность информации, защита информации, информационная безопасность, информационный процесс, документ, носитель 4. Свойства информации 5. Виды информации и их определения 6. Государственная тайна 7. Определения: угрозы, несанкционированный доступ. 8. Формы представления информации 9. Классификация угроз 10. Способы реализации угроз 11. Определения: защищаемая информация, доступ, допуск, уязвимость, сзи... 12. Виды защиты информации 13. Конституционные основы в информационной сфере 14. Доктрина ИБ РФ (составляющие национальных интересов РФ) 15. ФЗ «Об информации, информационных технологиях и о защите информации» 16. Преступления в информационной сфере (УК) 17. Задачи организационного обеспечения ЗИ 18. Управление ИБ 19. Модель угроз и модель нарушителя 20. Сложности в работе с пер-

соналом 21. Классификация инсайдерских угроз 22. Социальная инженерия 23. Определения (программно-аппаратная ЗИ): СВТ, доступ, допуск, идентификация, аутентификация 24. Дискреционное и мандатное управление доступом 25. Сертификация 26. Группы классов защищенности АС от НСД 27. Межсетевой экран, антивирус, СОВ 28. Криптографическое преобразование, шифрование, расшифрование. 29. Хэш-функция и ее свойства 30. Электронная подпись

### **3.5 Темы лабораторных работ**

- Защита компьютерной информации на уровне доступа в систему
- Защита от атак по локальным и глобальным сетям
- Защита от вредоносного ПО
- Использование шифрования для защиты данных
- Использование физических носителей и защитных систем на их основе

## **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 формирования компетенций, согласно п. 12 рабочей программы.

### **4.1. Основная литература**

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

### **4.2. Дополнительная литература**

1. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-1ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf)
2. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-1ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf)
3. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.3. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-1ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf)

### **4.3. Обязательные учебно-методические пособия**

1. «Методические указания к лабораторным и практическим работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс] [Электронный ресурс]. - [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_lab.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf)
2. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А., 2012г. – 2 с. [Электронный ресурс] [Электронный ресурс]. - [http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_srs.pdf](http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf)

### **4.4. Базы данных, информационно справочные и поисковые системы**

1. <http://www.edu.tusur.ru> – образовательный портал университета;
2. <http://www.lib.tusur.ru> – веб-сайт библиотеки университета;
3. <http://www.elibrary.ru> – научная электронная библиотека;
4. <http://www.edu.ru> – веб-сайт системы федеральных образовательных порталов.