

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**Федеральное государственное бюджетное образовательное учреждение высшего образования**  
**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ**  
**УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»**  
**(ТУСУР)**



УТВЕРЖДАЮ  
Директор департамента образования

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Информационная безопасность**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **09.03.04 Программная инженерия**

Направленность (профиль) / специализация: **Проектирование и разработка программных продуктов**

Форма обучения: **заочная**

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

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

Курс: **4, 5**

Семестр: **8, 9**

Учебный план набора 2014 года

**Распределение рабочего времени**

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	4	12	16	часов
2	Лабораторные работы	0	20	20	часов
3	Всего аудиторных занятий	4	32	36	часов
4	Самостоятельная работа	32	103	135	часов
5	Всего (без экзамена)	36	135	171	часов
6	Подготовка и сдача экзамена	0	9	9	часов
7	Общая трудоемкость	36	144	180	часов
				5.0	З.Е.

Контрольные работы: 9 семестр - 1

Экзамен: 9 семестр

Томск 2018

## ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.04 Программная инженерия, утвержденного 12.03.2015 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «\_\_» \_\_\_\_\_ 20\_\_ года, протокол №\_\_\_\_\_.

Разработчик:

доцент каф. КИБЭВС

\_\_\_\_\_ Е. Ю. Костюченко

Заведующий обеспечивающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ

\_\_\_\_\_ И. В. Осипов

Заведующий выпускающей каф.  
АОИ

\_\_\_\_\_ Ю. П. Ехлаков

Эксперты:

Доцент лаборатории безопасных  
биомедицинских технологий ЦТБ  
КИБЭВС

\_\_\_\_\_ А. А. Конев

Доцент кафедры автоматизации об-  
работки информации (АОИ)

\_\_\_\_\_ Н. Ю. Салмина

## 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.8) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информационная безопасность, Теория систем и системный анализ, Информационная безопасность.

Последующими дисциплинами являются: Информационная безопасность, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Информационная безопасность.

## 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 обучающийся 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 обеспечивающими защиту информации в компьютерных системах

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 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	0	20
Самостоятельная работа (всего)	135	32	103
Оформление отчетов по лабораторным работам	20	0	20
Подготовка к лабораторным работам	20	0	20
Проработка лекционного материала	32	8	24
Самостоятельное изучение тем (вопросов) теоретической части курса	28	24	4
Выполнение контрольных работ	35	0	35
Всего (без экзамена)	171	36	135
Подготовка и сдача экзамена	9	0	9
Общая трудоемкость, ч	180	36	144
Зачетные Единицы	5.0		

## 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	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Базовые понятия в сфере обеспечения информационной безопасности	2	0	4	6	ПК-4
2 Комплексный подход к обеспечению информационной безопасности	2	0	4	6	ПК-4
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	0	0	24	24	ПК-4
Итого за семестр	4	0	32	36	
9 семестр					
4 Методы оценки рисков и угроз информационной безопасности.	4	0	8	12	ПК-4
5 Программно-аппаратные, технические и криптографические средства защиты информации.	0	16	36	52	ПК-4
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	2	4	12	18	ПК-4
7 Концепция и политика информационной безопасности.	2	0	4	6	ПК-4
8 Реализации стратегии обеспечения информационной безопасности.	2	0	4	6	ПК-4

9 Менеджмент информационной безопасности.	2	0	39	41	ПК-4
Итого за семестр	12	20	103	135	
Итого	16	20	135	171	

### 5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Базовые понятия в сфере обеспечения информационной безопасности	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	2	ПК-4
	Итого	2	
2 Комплексный подход к обеспечению информационной безопасности	Структура системы защиты информации.	2	ПК-4
	Итого	2	
Итого за семестр		4	
9 семестр			
4 Методы оценки рисков и угроз информационной безопасности.	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	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.	2	ПК-4
	Итого	2	
9 Менеджмент информационной безопасности.	Контроль выполнения и функционирования защитных мер. Разработка и реализация программы осведомленности о защите. Обнаружение инцидентов и реагирование на них.	2	ПК-4

	Итого	2	
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	9
Предшествующие дисциплины									
1 Информационная безопасность	+	+	+	+	+	+	+	+	+
2 Теория систем и системный анализ	+	+	+	+	+	+	+	+	+
3 Информационная безопасность	+	+	+	+	+	+	+	+	+
Последующие дисциплины									
1 Информационная безопасность	+	+	+	+	+	+	+	+	+
2 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+	+	+	+
3 Информационная безопасность	+	+	+	+	+	+	+	+	+

### 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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	
ПК-4	+	+	+	Контрольная работа, Экзамен, Отчет по лабораторной работе, Тест

### 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 средства защиты информации.	Защита компьютерной информации на уровне доступа в систему	2	ПК-4
	Защита от компьютерных вирусов	2	
	Защита от атак по локальным и глобальным сетям	4	
	Шифрованная файловая система Windows	2	
	Шифрование диска BitLocker	4	
	Использование клиентов электронной почты	2	
	Итого	16	
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	Защита персональных данных	4	ПК-4
	Итого	4	
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
8 семестр				
1 Базовые понятия в сфере обеспечения информационной безопасности	Проработка лекционного материала	4	ПК-4	Тест, Экзамен
	Итого	4		
2 Комплексный подход к обеспечению информационной безопасности	Проработка лекционного материала	4	ПК-4	Тест, Экзамен
	Итого	4		
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Самостоятельное изучение тем (вопросов) теоретической части курса	24	ПК-4	Тест, Экзамен
	Итого	24		

Итого за семестр		32		
9 семестр				
4 Методы оценки рисков и угроз информационной безопасности.	Проработка лекционного материала	8	ПК-4	Тест, Экзамен
	Итого	8		
5 Программно-аппаратные, технические и криптографические средства защиты информации.	Самостоятельное изучение тем (вопросов) теоретической части курса	4	ПК-4	Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	16		
	Оформление отчетов по лабораторным работам	16		
	Итого	36		
6 Основные принципы, направления и требования обеспечения информационной безопасности организации.	Проработка лекционного материала	4	ПК-4	Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	12		
7 Концепция и политика информационной безопасности.	Проработка лекционного материала	4	ПК-4	Тест, Экзамен
	Итого	4		
8 Реализации стратегии обеспечения информационной безопасности.	Проработка лекционного материала	4	ПК-4	Тест, Экзамен
	Итого	4		
9 Менеджмент информационной безопасности.	Выполнение контрольных работ	35	ПК-4	Контрольная работа, Тест, Экзамен
	Проработка лекционного материала	4		
	Итого	39		
Итого за семестр		103		
	Подготовка и сдача экзамена	9		Экзамен
Итого		144		



## 10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

## 11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

## 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 [Электронный ресурс]: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov\\_oz\\_i.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_oz_i.pdf) (дата обращения: 20.09.2018).

### 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 [Электронный ресурс]: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 — Режим доступа: [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) (дата обращения: 20.09.2018).

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 [Электронный ресурс]: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-2ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf) (дата обращения: 20.09.2018).

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 [Электронный ресурс]: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov\\_poib/npa-ib-3ch.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf) (дата обращения: 20.09.2018).

### 12.3. Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Методические указания по лабораторным, контрольным работам и по ведению самостоятельной работы 09.03.04 Программная инженерия / Евсютин О.О., Конев А. А., Костюченко Е.Ю., Сопов М.А. 2018. – 96 с [Электронный ресурс]: — Режим доступа: [http://kibevs.tusur.ru/sites/default/files/files/upload/metod\\_labaoi.pdf](http://kibevs.tusur.ru/sites/default/files/files/upload/metod_labaoi.pdf) (дата обращения: 20.09.2018).

#### 12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и 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. Профессиональные базы данных и информационные справочные системы

1. <https://lib.tusur.ru/>
2. <https://edu.tusur.ru/>
3. Рекомендуется использовать информационные, справочные и нормативные базы дан-

### **13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение**

#### **13.1. Общие требования к материально-техническому и программному обеспечению дисциплины**

##### **13.1.1. Материально-техническое и программное 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. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

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

###### **Учебная лаборатория**

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634034, Томская область, г. Томск, Вершинина улица, д. 74, 426 ауд.

Описание имеющегося оборудования:

- ПЭВМ (Intel Pentium, 2 Gb RAM) (12 шт.);
- Магнитомаркерная доска;
- Видеопроектор;
- Экран;
- ПЭВМ (10 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- InkScape

##### **13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы**

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **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 комфортного просмотра.

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

### **14. Оценочные материалы и методические рекомендации по организации изучения дисциплины**

#### **14.1. Содержание оценочных материалов и методические рекомендации**

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

##### **14.1.1. Тестовые задания**

1. Что из нижеперечисленной информации, обрабатываемой в рамках различного специализированного программного обеспечения, не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?

а) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

б) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

в) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

г) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Что модель угроз безопасности информации (в частности, программного обеспечения) не включает в себя?

а) Описание информационной системы и ее структурно-функциональных характеристик;

б) Описание угроз безопасности информации;

в) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;

г) Стадии (этапы работ) создания системы защиты информационной системы.

3. В каких целях проводится анализ уязвимостей информационной системы (в частности, программных ее составляющих)?

а) Оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации;

- b) Оценки эффективности использования политик разграничения доступа;
- c) Оптимизации производительности программно-аппаратных средств защиты информации;
- d) Сегментации информационной системы.

4. Как называется системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании (на основе, в частности, анализа используемого в ней программного обеспечения) в соответствии с определёнными критериями и показателями безопасности?

- a) Аттестация;
- b) Аудит;
- c) Сертификация;
- d) Пентест.

5. Как называется абстрактное (формализованное или неформализованное) описание нарушителя правил (например, при использовании программного обеспечения) разграничения доступа?

- a) Характеристика нарушителя;
- b) Модель нарушителя;
- c) Сценарий нарушителя;
- d) Модель источников угроз.

6. Как называется стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта?

- a) Тестирование черного ящика;
- b) Тестирование белого ящика;
- c) Тестирование красного ящика;
- d) Тестирование неизвестного ящика.

7. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности (в частности, применительно к программному обеспечению)?

- a) Построение модели нарушителя;
- b) Идентификация ресурсов;
- c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам;
- d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.

8. Какая угроза безопасности информации является преднамеренной?

- a) Ошибки персонала;
- b) Сбой программного обеспечения;
- c) Фальсификация, подделка документов;
- d) Открытие электронного письма, содержащего вирус.

9. К какому классу угроз относится перехват данных, например, при использовании сетевого программного обеспечения?

- a) Доступности;
- b) Конфиденциальности;
- c) Целостности;
- d) Достоверности.

10. Как называется совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности

информации (в частности, используемой в рамках программного обеспечения)?

- a) Угрозой безопасности;
- b) Компьютерной безопасностью;
- c) Анализом угроз;
- d) Атакой на информационную систему.

11. Что из перечисленного происходит при использовании RAID-массивов?

- a) Производится полное шифрование данных
- b) Обеспечивается более высокий уровень защиты от вирусов
- c) Повышается надёжность хранения данных
- d) Увеличивается максимальная пропускная способность сети

12. Что из перечисленного не используется в программном обеспечении биометрической аутентификации?

- a) Рисунок папиллярного узора;
- b) Клавиатурный почерк;
- c) Пластиковая карта с магнитной полосой;
- d) Радужная оболочка глаза.

13. К какой подсистеме (реализуемых, в частности, в виде модулей программного обеспечения) не предъявляются требования в Руководящем документе «Классификация автоматизированных систем и требований по защите информации»?

- a) управления доступом;
- b) регистрации и учета;
- c) технической защиты информации;
- d) обеспечения целостности.

14. За счет мер, направленных на повышение чего достигается свойство доступности информации, обрабатываемой в программном обеспечении?

- a) Аутентичности;
- b) Непротиворечивости;
- c) Отказоустойчивости;
- d) Неотказуемости.

15. Каким термином называются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?

- a) Конфиденциальная информация;
- b) Секретная информация;
- c) Военная тайна;
- d) Государственная тайна.

16. Как называется получение доступа к информации субъектом в нарушение действующей политики разграничения доступа и в обход реализующего это разграничение программного обеспечения?

- a) Несанкционированный доступ;
- b) Злоумышленный доступ
- c) Неразрешенный доступ;
- d) Запретный доступ.

17. Какой вид информации не относится к категории конфиденциальной информации?

- a) Коммерческая тайна;
- b) Тайна судопроизводства;

- c) Персональные данные;
- d) Государственная тайна.

18. В рамках программного обеспечения зачастую используется различная информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Каким термином (согласно законодательству РФ) такая информация называется?

- a) Конфиденциальная информация;
- b) Персональные данные;
- c) Информация про личность;
- d) Информация с ограниченным доступом.

19. Как называется набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, в частности, с использованием программного обеспечения?

- a) Моделью безопасности;
- b) Методом шифрования;
- c) Компьютерной безопасностью;
- d) Политикой безопасности.

20. Какое из утверждений является неверным? «В программном обеспечении, предназначенном для выявления атак используется сигнатурный метод, который характеризуется ...»

- a) Сравнением исследуемого объекта с ранее известными образцами-эталоном;
- b) Способностью обнаруживать ранее неизвестные атаки;
- c) Простотой в настройке и эксплуатации для конечного пользователя системы;
- d) Популярностью использования в системах антивирусной защиты.

21. На какие типы делятся задачи по резервированию системы защиты (и, в частности, программных ее элементов)?

- a) Теплое и холодное резервирование;
- b) Холодное и горячее резервирование;
- c) Белое и серое резервирование;
- d) Толстое и тонкое резервирование.

22. Что подразумевает инструментальная комплексность в сфере информационной безопасности?

- a) Непрерывность осуществления мероприятий по защите информации;
- b) Защиту информации от внешних и внутренних угроз;
- c) Интеграцию всех видов и направлений ИБ для достижения поставленных целей;
- d) Обеспечение требуемого уровня защиты во всех элементах системы обработки информации.\*

#### 14.1.2. 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 персоналом
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

#### **14.1.3. Темы контрольных работ**

В рамках самостоятельного выполнения контрольной работы проводится выполнение индивидуального задания по выявлению угроз в области в соответствии с темой индивидуального задания.

Контрольная работа проводится по материалам разделов дисциплины №№ 1-9  
Темы индивидуальных заданий:

- Система защиты информации на жестком диске ПЭВМ
- Средства аутентификации по биометрическим показателям - отпечаток пальца
- Система аутентификации человека на объекте
- Система видеонаблюдения
- Система аутентификации человека за компьютером
- Датчик случайных чисел
- Система анализа трафика
- Комплекс для отработки навыков защиты сервера
- Специальные обследования объектов информатизации
- Система идентификации по УЭК
- Веб-сервер специализированного комплекса для отработки навыков защиты сервера
- Система гарантированного уничтожения информации
- Средства резервного копирования
- Аттестационный и эксплуатационный контроль защищаемого помещения
- Защита телефонных линий от прослушивания
- Подсистема ЭЦП (ЦР УЦ)
- Средства анализа проводных линий связи
- Межсетевой экран
- Аналитическая система промышленного шпионажа
- Средства защиты от передачи информации по мобильному телефону
- Защищенный ноутбук
- Защита вычислений в параллельных системах
- Оценка психофизиологического состояния человека за компьютером
- Система идентификации по биометрическим показателям - голос
- Комплексная защита веб-сервера
- Защищенная база данных
- Идентификация диктора по голосу
- Идентификация человека по лицу

Банкомат  
Подсистема защиты электронного дневника "Оценка-5. Электронный дневник".  
Система защиты жесткого диска ПЭВМ  
Система защиты информации на ноутбуке от НСД - двухфакторная аутентификация  
Система передачи данных показаний акселерометра мобильного устройства  
Система идентификации по биометрическим показателям  
Средства слежения за пользователем на компьютере  
Антивирус  
VPN, шифрование трафика - индивидуальное место  
Защита базы данных  
Защита сервера электронной почты  
Резервное копирование данных  
Система защиты информации на ноутбуке от НСД - от электронных средств  
Защита WiFi точки  
Система видеонаблюдения  
Сканер уязвимости в сети  
Криптографический клиент электронной почты  
Защита мобильного телефона  
Защита автомобиля от угона  
Средства аутентификации в компьютерной сети  
Защита программ от излучения  
Ревер-инжиниринг программных средств  
Система защиты от НСД к компьютеру  
Специализированный сервер для взлома (система проверки и статистики).

В рамках выполнения задания необходимо:

1. Составить описание объекта из задания в соответствии с нотацией IDEF1.
2. Выявить объекты защиты в рамках полученной структуры.
3. Выявить угрозы объектам в соответствии с типами (конфиденциальность, целостность, доступность).
4. Предложить потенциальные организационные и технические меры, направленные на противодействие выделенным угрозам.

#### **14.1.4. Темы лабораторных работ**

Защита компьютерной информации на уровне доступа в систему  
Защита от компьютерных вирусов  
Защита от атак по локальным и глобальным сетям  
Шифрованная файловая система Windows  
Шифрование диска BitLocker  
Защита персональных данных  
Использование клиентов электронной почты

#### **14.1.5. Методические рекомендации**

На самостоятельное изучение выносятся:

раздел "Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации" (Главы 1, 2 основного учебника 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] - Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov\\_oz\\_i.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_oz_i.pdf) (дата обращения: 21.06.2018)).

Темы для самостоятельного изучения:

1. Информационное право в теории государства и права
2. Информация как объект правового регулирования
3. Правовые основы использования организационных и технических средств защиты информации



4. Лицензирование деятельности в области защиты информации
5. Сертификация, стандартизация, аккредитация в информационной сфере
6. Юридическая ответственность за нарушение норм защиты информации
7. Функции организационной составляющей системы защиты информации
8. Регламентация работы с информацией и её носителями
9. Регламентация действий при осуществлении информационных процессов
10. Регламентация работы с элементами системы защиты информации

раздел "Программно-аппаратные, технические и криптографические средства защиты информации." (Глава 6 основного учебника 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] - Режим доступа: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov\\_oz\\_i.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_oz_i.pdf) (дата обращения: 21.06.2018)).

Темы для самостоятельного изучения:

1. Терминология в области криптографической защиты
2. Угрозы со стороны участников информационного обмена
3. Требования к криптосистемам
4. Основные алгоритмы шифрования
5. Симметричные криптосистемы
6. Криптографические хэш-функции
7. Ассиметричные криптосистемы (криптосистемы с открытым ключом)
8. Управление ключами
9. Криптоанализ и атаки на криптосистемы
10. Характеристики безопасности обеспечиваемые средствами криптографической защиты информации:

11. Удостоверяющий центр

#### **14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	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 материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов 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.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся 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 лиц с ограниченными возможностями здоровья и 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 лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.