

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего профессионального образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ  
ЭЛЕКТРОНИКИ» (ТУСУР)



Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820  
Владелец: Троян Павел Ефимович  
Действителен: с 19.01.2016 по 16.09.2019

«6» 09 2016 г.

## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной образовательной программы: бакалавриат  
Направление(я) подготовки (специальность): 38.03.02 Менеджмент  
Специализация: Информационный менеджмент  
Форма обучения: очная  
Факультет: Радиотехнический  
Кафедра: Телевидения и управления (ТУ)

Курс 3

Семестр 5

Учебный план набора 2013 г. и последующих лет.

Распределение рабочего времени:

№	Виды учебной работы	Семестр 1	Семестр 2	Семестр 3	Семестр 4	Семестр 5	Семестр 6	Семестр 7	Семестр 8	Всего	Единицы
1.	Лекции					18				18	часов
2.	Лабораторные работы					-				-	часов
3.	Практические занятия					36				36	часов
4.	Курсовой проект/работа (КРС) (аудиторная)					-				-	часов
5.	Всего аудиторных занятий (Сумма 1-4)					54				54	часов
6.	Из них в интерактивной форме					-				-	часов
7.	Самостоятельная работа студентов (СРС)					18				18	часов
8.	Всего (без экзамена) (Сумма 5,7)					72				72	часов
9.	Самост. работа на подготовку, сдачу экзамена					-				-	часов
10.	Общая трудоемкость (Сумма 8,9)					72				72	часов
	(в зачетных единицах)					2				2	ЗЕТ

Зачет 5 семестр

Томск 2016



### Лист согласований

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего профессионального образования (ФГОС ВПО) по направлению подготовки (специальности) 38.03.02 Менеджмент «Информационный менеджмент», рассмотрена и утверждена на заседании кафедры «17» июня 2016 г., протокол № 6.

Разработчики: программист каф. КИБЭВС \_\_\_\_\_ /А.К. Новохрестов/

Зав. кафедрой КИБЭВС, профессор \_\_\_\_\_ /А.А. Шелупанов/

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

Декан Радиотехнического факультета \_\_\_\_\_ /К.Ю. Попова/

Зав. профилирующей кафедрой КИБЭВС \_\_\_\_\_ /А.А. Шелупанов/

Зав. выпускающей кафедрой ТУ \_\_\_\_\_ /Т.Р. Газизов/

Эксперты:

Директор Центра системного проектирования \_\_\_\_\_ /А.А. Конев/

Доцент каф. КИБЭВС \_\_\_\_\_ /М.А. Сопов/

## **1. Цели и задачи дисциплины:**

Целью дисциплины «Защита информации и информационная безопасность» является заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, рассмотреть основные методологические принципы теории информационной безопасности, изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

Задачи дисциплины: ознакомление студентов с терминологией информационной безопасности, развитие мышления студентов, изучение методов и средств обеспечения информационной безопасности, обучение определению причин, видов, каналов утечки и искажения информации.

## **2. Место дисциплины в структуре ООП:**

Цикл дисциплины: Б1. Дисциплины (модули). Для эффективного освоения дисциплины студент должен знать основные положения дисциплин: Информатика; Моделирование систем. Последующие дисциплины: Сети ЭВМ.

## **3. Требования к результатам освоения дисциплины:**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-7).

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 2 (две) зачетные единицы.

Вид учебной работы	Всего часов	Семестры
		5
<b>Аудиторные занятия (всего)</b>	<b>54</b>	<b>54</b>
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	Не предусмотрено	
Практические занятия (ПЗ)	36	
Семинары (С)	Не предусмотрено	
Кolloквиумы (К)	Не предусмотрено	
Курсовой проект/(работа) (аудиторная нагрузка)	Не предусмотрено	
<i>Другие виды аудиторной работы</i>	Не предусмотрено	
<b>Самостоятельная работа (всего)</b>	<b>18</b>	<b>18</b>
В том числе:		
Курсовой проект (работа) (самостоятельная работа)	Не предусмотрено	
Подготовка к практическим занятиям	9	9
Индивидуальная работа	Не предусмотрено	
Контрольные работы	3	3
Лекционный материал	6	6
Вид промежуточной аттестации (зачет, экзамен)	Не предусмотрено	
Общая трудоемкость час	<b>72</b>	<b>72</b>
Зачетные Единицы Трудоемкости	<b>2</b>	<b>2</b>

#### 5. Содержание дисциплины

##### 5.1. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции	Лабораторн. работы	Практич. занятия.	Курсовой ПР (КРС)	Самост. работа студента	Всего час. (без экзам)	Формируемые компетенции (ОК, ПК, ПСК)
1.	Базовые понятия в сфере обеспечения информационной безопасности.	2	Не предусмотрено	-	Не предусмотрено	1	3	ОПК-7
2.	Комплексный подход к обеспечению информационной безопасности.	2		-		1	3	ОПК-7
3.	Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	2		8		3	13	ОПК-7
4.	Методы оценки рисков и угроз информационной безопасности.	2		4		2	8	ОПК-7
5.	Программно-аппаратные, технические и криптографические средства защиты информации.	2		20		6	28	ОПК-7
6.	Основные принципы, направления и требования обеспечения информационной безопасности организации.	2		-		1	3	ОПК-7
7.	Концепция и политика информационной безопасности.	2		-		1	3	ОПК-7
8.	Реализации стратегии обеспечения информационной безопасности.	2		4		2	8	ОПК-7
9.	Менеджмент информационной безопасности.	2		-		1	3	ОПК-7
<b>10.</b>	<b>Итого</b>	<b>18</b>		<b>36</b>		<b>18</b>	<b>72</b>	

## 5.2. Содержание разделов дисциплины (по лекциям)

№ п/п	Наименование разделов	Содержание разделов	Трудоемкость (час.)	Формируемые компетенции (ОК, ПК, ПСК)
1.	Базовые понятия в сфере обеспечения информационной безопасности.	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	2	ОПК-7
2.	Комплексный подход к обеспечению информационной безопасности.	Структура системы защиты информации.	2	ОПК-7
3.	Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации.	Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование.	2	ОПК-7
4.	Методы оценки рисков и угроз информационной безопасности.	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	2	ОПК-7
5.	Программно-аппаратные, технические и криптографические средства защиты информации.	Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа. Мандатное распределение доступа.	2	ОПК-7
6.	Основные принципы, направления и требования обеспечения информационной безопасности организации.	Определение организационных требований защиты ИТ.	2	ОПК-7
7.	Концепция и политика информационной безопасности.	Политика безопасности.	2	ОПК-7
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	ОПК-7
9.	Менеджмент информационной безопасности.	Контроль выполнения и функционирования защитных мер. Разработка и реализация программы осведомленности о защите. Обнаружение инцидентов и реагирование на них.	2	ОПК-7

**5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами**

№ п/п	Наименование обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины из табл.5.1, для которых необходимо изучение обеспечивающих (предыдущих) и обеспечиваемых (последующих) дисциплин								
		1	2	3	4	5	6	7	8	9
<b>Предшествующие дисциплины</b>										
1.	Информатика	+	+	+		+		+	+	+
2.	Моделирование систем	+		+	+	+	+		+	+
<b>Последующие дисциплины</b>										
1.	Сети ЭВМ	+	+	+	+	+	+	+	+	+

**5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий (пример)**

Перечень компетенций	Виды занятий					Формы контроля по всем видам занятий (примеры)
	Л	Лаб	Пр.	КР/КП	СРС	
ОПК-7	+		+		+	Опрос на лекции Отчет по практической работе

Л – лекция, Пр – практические и семинарские занятия, Лаб – лабораторные работы, КР/КП – курсовая работа/проект, СРС – самостоятельная работа студента

**6. Методы и формы организации обучения**

**Технологии интерактивного обучения при разных формах занятий в часах**

Не предусмотрено

## 7. Лабораторный практикум

Не предусмотрены

## 8. Практические занятия (семинары)

№ п/п	№ раздела дисциплины из табл. 5.1	Наименование лабораторных работ	Трудо-емкость (час.)	Компетенции ОК, ПК, ПСК
1	3	Защита персональных данных и коммерческой тайны	4	ОПК-7
2	3	Политика безопасности и инструкции для сотрудников предприятия	4	ОПК-7
3	4	Оценка рисков информационной безопасности	4	ОПК-7
4	5	Защита компьютерной информации на уровне доступа в систему	4	ОПК-7
5	5	Защита от атак по локальным и глобальным сетям	4	ОПК-7
6	5	Защита от вредоносного ПО	4	ОПК-7
7	5	Использование шифрования для защиты данных	4	ОПК-7
8	5	Использование физических носителей и защитных систем на их основе	4	ОПК-7
9	8	Разработка системы защиты предприятия	4	ОПК-7

## 9. Самостоятельная работа

№ п/п	№ раздела дисциплины из табл. 5.1	Виды самостоятельной работы (детализация)	Трудо-емкость (час.)	Компетенции ОК, ПК, ПСК	Контроль выполнения работы (Опрос, тест, дом. задание, и т.д)
1.	1,2,3,4,5,6,7,8,9	Проработка лекционного материала	6	ОПК-7	Опрос на лекции
2.	3,4,5,8	Подготовка к практическим занятиям	9	ОПК-7	Отчет по практической работе
3.	1,2,3,4,5,6,7,8,9	Контрольные работы	3	ОПК-7	Контрольная работа

## 10. Примерная тематика курсовых проектов (работ)

Не предусмотрено

## 11. Рейтинговая система для оценки успеваемости студентов

**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
Посещение занятий	4	5	4	<b>13</b>
Практические работы	9	9	9	<b>27</b>
Контрольные работы	10	10	10	<b>30</b>
<b>Итого максимум за период:</b>	<b>23</b>	<b>24</b>	<b>23</b>	<b>70</b>
<b>Зачет</b>	-	-	-	<b>30</b>
<b>Нарастающим итогом</b>	<b>23</b>	<b>47</b>	<b>70</b>	<b>100</b>

**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

**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)	<b>90 – 100</b>	A (отлично)
4 (хорошо) (зачтено)	<b>85 – 89</b>	B (очень хорошо)
	<b>75 – 84</b>	C (хорошо)
	<b>70 – 74</b>	D (удовлетворительно)
<b>65 – 69</b>		
3 (удовлетворительно) (зачтено)	<b>60 – 64</b>	E (посредственно)
	<b>Ниже 60 баллов</b>	F (неудовлетворительно)



## 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]  
URL: [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)

### 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]  
URL: [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]  
URL: [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]  
URL: [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 и программное обеспечение

Для обеспечения дисциплины используются следующие УМП:

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]  
URL: [http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_lab.pdf](http://keva.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]  
URL: [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)

### 12.4 Базы данных, информационно-справочные и поисковые системы

<http://www.edu.tusur.ru> – образовательный портал университета;

<http://www.lib.tusur.ru> – веб-сайт библиотеки университета;

<http://www.elibrary.ru> – научная электронная библиотека;

<http://www.edu.ru> – веб-сайт системы федеральных образовательных порталов.

## 13. Материально-техническое обеспечение дисциплины

1. Мультимедийная лекционная аудитория.
2. Компьютерный класс с выходом в Интернет.

## 14. Методические рекомендации по организации изучения дисциплины

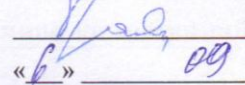
Не предусмотрено.

Приложение к рабочей программе

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

УТВЕРЖДАЮ

Проректор по учебной работе

 П. Е. Троян  
« 6 » 2016 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**  
**ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Уровень основной образовательной программы:	бакалавриат
Направление(я) подготовки (специальность):	38.03.02 Менеджмент
Специализация:	Информационный менеджмент
Форма обучения:	очная
Факультет	Радиотехнический
Кафедра	Телевидения и управления (ТУ)
Курс 3	Семестр 5

Учебный план набора 2013 г. и последующих лет.

Зачет 5 семестр

Томск 2016

## Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины «Защита информации и информационная безопасность» 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 Защита информации и информационная безопасность используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной компетенций приведен в таблице 1.

**Таблица 1 - Перечень закрепленных за дисциплиной компетенций**

Код	Формулировка компетенции	Этапы формирования компетенции
ОПК-7	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом <b>основных требований информационной безопасности</b>	<p>Знать:</p> <ul style="list-style-type: none"><li>– базовые концепции и модели информационной безопасности;</li><li>– основы функционирования безопасности информационных систем;</li><li>– задачи информационной безопасности;</li><li>– законодательство по обеспечению информационной безопасности;</li><li>– стандарты в области информационной безопасности;</li><li>– методы и средства защиты информационной безопасности;</li><li>– направления и методы ведения аналитической работы по выявлению угроз;</li><li>– технические процедуры по действиям в нештатной ситуации;</li><li>– методологии оценки рисков и угроз информационной безопасности.</li></ul> <p>Уметь:</p> <ul style="list-style-type: none"><li>– выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем;</li><li>– проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов;</li><li>– оценивать и выбирать необходимые средства защиты;</li><li>– осуществлять мониторинг состояния информационной безопасности объекта;</li><li>– обеспечивать противодействие атакам на информационную систему;</li><li>– выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности;</li></ul> <p>Владеть:</p> <p>навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах</p>

## 1 Реализация компетенций

### 1.1 Компетенция ОПК-7

**ОПК-7: Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.**

Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 2.

**Таблица 2 - Этапы формирования компетенции и используемые средства оценивания**

<b>Состав</b>	<b>Знать</b>	<b>Уметь</b>	<b>Владеть</b>
<b>Содержание этапов</b>	<ul style="list-style-type: none"> <li>– базовые концепции и модели информационной безопасности;</li> <li>– основы функционирования информационных систем;</li> <li>– задачи информационной безопасности;</li> <li>– законодательство по обеспечению информационной безопасности;</li> <li>– стандарты в области информационной безопасности;</li> <li>– методы и средства защиты информационной безопасности;</li> <li>– направления и методы ведения аналитической работы по выявлению угроз;</li> <li>– технические процедуры по действиям в нештатной ситуации;</li> <li>– методологии оценки рисков и угроз информационной безопасности</li> </ul>	<ul style="list-style-type: none"> <li>– выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем;</li> <li>– проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов;</li> <li>– оценивать и выбирать необходимые средства защиты;</li> <li>– осуществлять мониторинг состояния информационной безопасности объекта;</li> <li>– обеспечивать противодействие атакам на информационную систему;</li> <li>– выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности</li> </ul>	<ul style="list-style-type: none"> <li>навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах</li> </ul>
<b>Виды занятий</b>	Лекции	Практические работы Самостоятельная работа студентов	Практические работы
<b>Используемые средства оценивания</b>	Контрольная работа Зачет	Оформление отчетов и защита практических работ Оценивание самостоятельной работы студента	Оформление отчетов и защита практических работ  Зачет

Общие характеристики показателей и критериев оценивания компетенции на всех этапах приведены в таблице 3.



**Таблица 3 - Общие характеристики показателей и критериев оценивания компетенции по этапам**

Показатели и критерии	Знать	Уметь	Владеть
<b>Отлично (высокий уровень)</b>	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
<b>Хорошо (базовый уровень)</b>	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
<b>Удовлетворительно (пороговый уровень)</b>	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

**Таблица 4 – Показатели и критерии оценивания компетенции на этапах**

Показатели и критерии	Знать	Уметь	Владеть
<b>Отлично (высокий уровень)</b>	<p>Знает:</p> <ul style="list-style-type: none"> <li>– базовые концепции и модели информационной безопасности;</li> <li>– основы функционирования безопасности информационных систем;</li> <li>– задачи информационной безопасности;</li> <li>– законодательство по обеспечению информационной безопасности;</li> <li>– стандарты в области информационной безопасности;</li> <li>– методы и средства защиты информационной безопасности;</li> <li>– направления и методы ведения аналитической работы по выявлению угроз;</li> <li>– технические процедуры по действиям в нештатной ситуации;</li> <li>– методологии оценки рисков и угроз информационной безопасности</li> </ul>	<p>Умеет:</p> <ul style="list-style-type: none"> <li>– выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем;</li> <li>– проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов;</li> <li>– оценивать и выбирать необходимые средства защиты;</li> <li>– осуществлять мониторинг состояния информационной безопасности объекта;</li> <li>– обеспечивать противодействие атакам на информационную систему;</li> <li>– выполнять (контролировать выполнение) требований</li> </ul>	<p>Навыками работы с программными и аппаратными средствами, обеспечивающими защиту информации в компьютерных системах</p>



		инструкции по обеспечению информационной безопасности	
<b>Хорошо (базовый уровень)</b>	Знает: – базовые концепции и модели информационной безопасности; – основы функционирования безопасности информационных систем; – задачи информационной безопасности; – стандарты в области информационной безопасности; – методы и средства защиты информационной безопасности;	Умеет: – 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	Владеет навыками формирования и применения комплекса мер для обеспечения безопасности информации в организации.
<b>Удовлетворительно (пороговый уровень)</b>	Знает базовые концепции и модели информационной безопасности, а также методы и средства защиты информационной безопасности	Умеет: – обеспечивать противодействие атакам на информационную систему; – выполнять требования инструкции по обеспечению информационной безопасности	Владеет базовыми навыками необходимыми для обеспечения безопасности информации на организации.

## 2 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в составе:

- контрольная работа;
- практические работы;
- самостоятельная работа;
- зачет.

### 2.1. 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.

## **2.2 Темы практических работ**

1. Защита персональных данных и коммерческой тайны
2. Политика безопасности и инструкции для сотрудников предприятия
3. Оценка рисков информационной безопасности
4. Защита компьютерной информации на уровне доступа в систему
5. Защита от атак по локальным и глобальным сетям
6. Защита от вредоносного ПО
7. Использование шифрования для защиты данных
8. Использование физических носителей и защитных систем на их основе
9. Разработка системы защиты предприятия

## **2.3 Вопросы к зачету**

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

## **3 Методические материалы**

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

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]  
URL: [http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov\\_ozh.pdf](http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozh.pdf)

2. 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]  
URL: [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.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс]  
URL: [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. 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]  
URL: [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)

5. «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]  
URL: [http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf\\_isr/ib/metod\\_lab.pdf](http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf)

6. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А., 2012г. – 2 с. [Электронный ресурс]  
URL: [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)