МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **40.03.01 Юриспруденция**
Направленность (профиль): **Юриспруденция**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **ИП, Кафедра информационного права**
Курс: **2**
Семестр: **4**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	4	4	часов
2	Практические занятия	8	8	часов
3	Всего аудиторных занятий	12	12	часов
4	Из них в интерактивной форме	4	4	часов
5	Самостоятельная работа	56	56	часов
6	Всего (без экзамена)	68	68	часов
7	Подготовка и сдача зачета	4	4	часов
8	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Контрольные работы: 4 семестр - 1
Зачет: 4 семестр

Томск 2017

Согласована на портале № 19160

Рассмотрена и одобрена на заседании кафедры
протокол № 49 от « 3 » 3 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 40.03.01 Юриспруденция, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РЭТЭМ _____ Н. Н. Несмелова

Заведующий обеспечивающей каф.
РЭТЭМ _____ В. И. Туев

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

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф.
ИП _____ В. Г. Мельникова

Эксперт:

профессор каф. РЭТЭМ _____ Г. В. Смирнов

Согласована на портале № 19160

1. Цели и задачи дисциплины

1.1. Цели дисциплины

познакомить студентов с основными методами, способами и средствами получения, хранения, переработки информации, а также с принципами и методами защиты информации

закрепить навыки работы с компьютером как средством управления информацией

сформировать способность работать с информацией в глобальных компьютерных сетях

1.2. Задачи дисциплины

– познакомиться с основными принципами и методами защиты информации

– изучить основные понятия, принципы, методы и способы защиты информации на государственном и корпоративном уровнях

– освоить способы защиты личной информации и персональных данных при социальных взаимодействиях и работе с компьютерных сетях

– понять сущность правовых, организационных, психологических и технических аспектов информационной безопасности

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» (Б1.В.ОД.3) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Безопасность жизнедеятельности.

Последующими дисциплинами являются: Защита и обработка конфиденциальных документов, Защита информации в предпринимательском праве, Защита прав интеллектуальной собственности в телекоммуникационных системах.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-3 владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

– ОК-4 способностью работать с информацией в глобальных компьютерных сетях;

В результате изучения дисциплины студент должен:

– **знать** основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией; основы работы с информацией в глобальных компьютерных сетях; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности

– **уметь** применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; работать с информацией в глобальных компьютерных сетях; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности

– **владеть** основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью работать с информацией в глобальных компьютерных сетях; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятель-

Согласована на портале № 19160

ности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		4 семестр
Аудиторные занятия (всего)	12	12
Лекции	4	4
Практические занятия	8	8
Из них в интерактивной форме	4	4
Самостоятельная работа (всего)	56	56
Проработка лекционного материала	5	5
Самостоятельное изучение тем (вопросов) теоретической части курса	26	26
Подготовка к практическим занятиям, семинарам	17	17
Выполнение контрольных работ	8	8
Всего (без экзамена)	68	68
Подготовка и сдача зачета	4	4
Общая трудоемкость ч	72	72
Зачетные Единицы	2.0	2.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
4 семестр					
1 Информационная безопасность общества и личности	0	2	13	15	ОК-3, ОК-4
2 Принципы, методы и средства защиты информации	1	2	13	16	ОК-3, ОК-4
3 Правовые аспекты информационной безопасности	1	0	13	14	ОК-3, ОК-4
4 Организационные и психологические аспекты информационной безопасности	1	2	5	8	ОК-3, ОК-4

Согласована на портале № 19160

5 Технические аспекты защиты информации	1	2	12	15	ОК-3, ОК-4
Итого за семестр	4	8	56	68	
Итого	4	8	56	68	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
4 семестр			
2 Принципы, методы и средства защиты информации	Защищаемая информация и угрозы безопасности. Причины и каналы утечки информации. Цели, задачи и принципы защиты информации. Системный подход в обеспечении информационной безопасности. Методы и средства защиты информации. Режимы секретности и конфиденциальности. Защита государственной и коммерческой тайны. Защита персональных данных.	1	ОК-3, ОК-4
	Итого	1	
3 Правовые аспекты информационной безопасности	Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации. Основные законодательные акты, правовые нормы и положения. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовая ответственность за утечку информации и утрату носителей информации. Правовая защита интеллектуальной собственности.	1	ОК-3, ОК-4
	Итого	1	
4 Организационные и психологические аспекты информационной безопасности	Принципы, силы, средства и условия организационной защиты информации. Организация защиты служебной конфиденциальной информации. Организация защиты коммерческой тайны. Организация защиты сведений, составляющих государственную тайну. Психологические аспекты информационной безопасности. Комплексный контроль защиты информации.	1	ОК-3, ОК-4
	Итого	1	
5 Технические аспекты защиты информации	Технические каналы утечки информации. Методы инженерной защиты и	1	ОК-3, ОК-4

Согласована на портале № 19160

	технической охраны объектов. Методы и средства поиска электронных устройств перехвата информации. Организация и методическое обеспечение инженерно-технической защиты информации.		
	Итого	1	
Итого за семестр		4	

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
Предшествующие дисциплины					
1 Безопасность жизнедеятельности	+		+	+	
Последующие дисциплины					
1 Защита и обработка конфиденциальных документов	+	+	+	+	+
2 Защита информации в предпринимательском праве	+	+	+	+	+
3 Защита прав интеллектуальной собственности в телекоммуникационных системах	+	+	+	+	+

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

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

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

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ОК-3	+	+	+	Контрольная работа, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию

Согласована на портале № 19160

ОК-4	+	+	+	Контрольная работа, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

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

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

Методы	Интерактивные практические занятия	Всего
4 семестр		
Презентации с использованием мультимедиа с обсуждением		0
Решение ситуационных задач	4	4
Итого за семестр:	4	4
Итого	4	4

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Информационная безопасность общества и личности	Основные положения политики обеспечения информационной безопасности организации	2	ОК-3, ОК-4
	Итого	2	
2 Принципы, методы и средства защиты информации	Стандарты и спецификации в области информационной безопасности	2	ОК-3, ОК-4
	Итого	2	
4 Организационные и психологические аспекты информационной безопасности	Организационные меры по обеспечению безопасности. Служебные инструкции и ответственность	2	ОК-3, ОК-4
	Итого	2	
5 Технические аспекты защиты информации	Современные методы и средства сетевой защиты. Безопасность носителей данных	2	ОК-3, ОК-4
	Итого	2	
Итого за семестр		8	

Согласована на портале № 19160

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				
1 Информационная безопасность общества и личности	Подготовка к практическим занятиям, семинарам	2	ОК-3, ОК-4	Отчет по практическому занятию, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	10		
	Проработка лекционного материала	1		
	Итого	13		
2 Принципы, методы и средства защиты информации	Подготовка к практическим занятиям, семинарам	4	ОК-3, ОК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Отчет по практическому занятию, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	8		
	Проработка лекционного материала	1		
	Итого	13		
3 Правовые аспекты информационной безопасности	Выполнение контрольных работ	8	ОК-3, ОК-4	Контрольная работа, Отчет по практическому занятию, Тест
	Подготовка к практическим занятиям, семинарам	4		
	Проработка лекционного материала	1		
	Итого	13		
4 Организационные и психологические аспекты информационной безопасности	Подготовка к практическим занятиям, семинарам	4	ОК-3, ОК-4	Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Итого	5		
5 Технические аспекты защиты информации	Подготовка к практическим занятиям, семинарам	3	ОК-3, ОК-4	Выступление (доклад) на занятии, Конспект самоподготовки, Отчет по практическому занятию,
	Самостоятельное изуче-	8		

Согласована на портале № 19160

	ние тем (вопросов) теоретической части курса			Тест
	Проработка лекционного материала	1		
	Итого	12		
Итого за семестр		56		
	Подготовка и сдача зачета	4		Зачет
Итого		60		

9.1. Темы контрольных работ

1. Проведение патентных исследований. Подготовка заявки заявки на объект интеллектуальной собственности (изобретение, полезная модель, промышленный образец, товарный знак)

9.2. Темы для самостоятельного изучения теоретической части курса

1. Информация, ей сущность и виды. Особенности информационного общества. Основные методы, способы и средства получения, хранения, переработки информации, работа с компьютером как средством управления информацией. Работа с информацией в глобальных компьютерных сетях . Информационная безопасность общества и личности
2. Стандарты и спецификации в области информационной безопасности
3. Технические каналы утечки информации и средства защиты

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. Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5171

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

12.2. Дополнительная литература

1. Основы информационной безопасности: Учебное пособие / Голиков А. М. - 2007. 201 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1024, дата обращения: 29.04.2017.

2. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/book/5170 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5170

3. Белов, Е.Б. Основы информационной безопасности. [Электронный ресурс] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5121

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, дата обращения: 29.04.2017.

2. Защита и передача объектов интеллектуальной собственности: Методические указания

Согласована на портале № 19160

для проведения практических и самостоятельных работ / Изоткина Н. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1944, дата обращения: 29.04.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

1. https://www.yandex.ru/ - поисковая система Яндекс

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

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

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

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

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

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

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

Согласована на портале № 19160

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

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

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

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

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

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

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

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

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

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

Согласована на портале № 19160

- в форме электронного документа;
- в печатной форме.

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

Согласована на портале № 19160

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **40.03.01 Юриспруденция**
Направленность (профиль): **Юриспруденция**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **ИП, Кафедра информационного права**
Курс: **2**
Семестр: **4**

Учебный план набора 2013 года

Разработчик:
- доцент каф. РЭТЭМ Н. Н. Несмелова

Зачет: 4 семестр

Томск 2017

Согласована на портале № 19160

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
ОК-4	способностью работать с информацией в глобальных компьютерных сетях	Должен знать основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией; основы работы с информацией в глобальных компьютерных сетях; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности; Должен уметь применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; работать с информацией в глобальных компьютерных сетях; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности; Должен владеть основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;
ОК-3	владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	

Согласована на портале № 19160

		способностью работать с информацией в глобальных компьютерных сетях; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ОК-4

ОК-4: способностью работать с информацией в глобальных компьютерных сетях.

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	основы работы с информацией в глобальных компьютерных сетях; основные положения и методы информационной безопасности, применяе-	работать с информацией в глобальных компьютерных сетях; использовать основные положения и методы информационной безопасности	способностью работать с информацией в глобальных компьютерных сетях; способностью использовать основные положения и методы ин-

Согласована на портале № 19160

	мые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности	при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности	формационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности
Виды занятий	• Интерактивные практические занятия; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Выступление (доклад) на занятии; • Тест; • Отчет по практическому занятию; • Зачет;	• Контрольная работа; • Выступление (доклад) на занятии; • Тест; • Отчет по практическому занятию; • Зачет;	• Выступление (доклад) на занятии; • Отчет по практическому занятию; • Зачет;

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)	• основы работы с информацией в глобальных компьютерных сетях; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в	• работать с информацией в глобальных компьютерных сетях; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной	• способностью работать с информацией в глобальных компьютерных сетях; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной

Согласована на портале № 19160

	системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности;	безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности;	терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности ;
Хорошо (базовый уровень)	• основы работы с информацией в глобальных компьютерных сетях; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации;	• работать с информацией в глобальных компьютерных сетях; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации;	• способностью работать с информацией в глобальных компьютерных сетях; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; способностью применять в практической деятельности методы правовой и организационной защиты информации;
Удовлетворительно (пороговый уровень)	• основы работы с информацией в глобальных компьютерных сетях;	• работать с информацией в глобальных компьютерных сетях;	• способностью работать с информацией в глобальных компьютерных сетях;

2.2 Компетенция ОК-3

ОК-3: владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Согласована на портале № 19160

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности	применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности	основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности
Виды занятий	• Интерактивные практические занятия; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Выступление (доклад) на занятии; • Тест; • Отчет по практическому занятию; • Зачет;	• Контрольная работа; • Выступление (доклад) на занятии; • Тест; • Отчет по практическому занятию; • Зачет;	• Выступление (доклад) на занятии; • Отчет по практическому занятию; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Согласована на портале № 19160

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы и методы правовой и организационной защиты информации; психологические и технические аспекты информационной безопасности;	• применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе национальной безопасности Российской Федерации; анализировать и оценивать угрозы информационной безопасности для различных объектов; применять в практической деятельности методы правовой и организационной защиты информации; учитывать психологические и технические аспекты информационной безопасности;	• основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и средствами выявления угроз безопасности; навыками организации и обеспечения режима секретности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации; готовностью учитывать психологические и технические аспекты информационной безопасности ;
Хорошо (базовый уровень)	• основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией; основные положения и методы информационной безопасности, применяемые при решении социальных и профессиональных задач; место и роль информационной безопас-	• применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; определять место и роль информационной безопасности в системе	• основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью использовать основные положения и методы информационной безопасности при решении социальных и профессиональных задач; профессиональной терминологией, методами и сред-

Согласована на портале № 19160

	ности Российской Федерации; принципы и методы правовой и организационной защиты информации;	национальной безопасности Российской Федерации; применять в практической деятельности методы правовой и организационной защиты информации;	ствами выявления угроз безопасности; методами формирования требований по защите информации; способностью применять в практической деятельности методы правовой и организационной защиты информации;
Удовлетворительно (пороговый уровень)	• основные методы, способы и средства получения, хранения, переработки информации, способы работы с компьютером как средством управления информацией;	• применять основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией;	• основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

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 Вопросы на самоподготовку

- Стандарты и спецификации в области информационной безопасности
- Технические каналы утечки информации и средства защиты

3.2 Тестовые задания

- Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
- A. Сотрудники
- B. Хакеры
- C. Атакующие
- D. Контрагенты (лица, работающие по договору)
- Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
- A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- C. Улучшить контроль за безопасностью этой информации
-
-
- D. Снизить уровень классификации этой информации
- Что самое главное должно продумать руководство при классификации данных?
- A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- B. Необходимый уровень доступности, целостности и конфиденциальности
- C. Оценить уровень риска и отменить контрмеры
- D. Управление доступом, которое должно защищать данные
- Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Согласована на портале № 19160

– A. Владельцы данных
– B. Пользователи
– C. Администраторы
– D. Руководство
– Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
– A. Поддержка высшего руководства
– B. Эффективные защитные меры и методы их внедрения
– C. Актуальные и адекватные политики и процедуры безопасности
– D. Проведение тренингов по безопасности для всех сотрудников
– Основные угрозы доступности информации:
– A. непреднамеренные ошибки пользователей
– B. злонамеренное изменение данных
– C. хакерская атака
– D. перехват данных
– Суть компрометации информации
– A. внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
– B. несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
– C. внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать D. дополнительные усилия для выявления изменений и восстановления истинных сведений
– Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
– A. несанкционированного управления удаленным компьютером
– B. внедрения агрессивного программного кода в рамках активных объектов Web-страниц
– C. перехвата или подмены данных на путях транспортировки
– D. вмешательства в личную жизнь
– поставки неприемлемого содержания

3.3 Зачёт

– Информация, ей сущность и виды. Особенности информационного общества. Информационная безопасность общества. Защищаемая информация и угрозы безопасности. Причины и каналы утечки информации. Информационная безопасность личности. Цели, задачи и принципы защиты информации. Системный подход в обеспечении информационной безопасности. Методы и средства защиты информации. Режимы секретности и конфиденциальности. Защита государственной и коммерческой тайны. Защита персональных данных. Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации. Основные законодательные акты, правовые нормы и положения. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовая ответственность за утечку информации и утрату носителей информации. Правовая защита интеллектуальной собственности. Принципы, силы, средства и условия организационной защиты информации. Организация защиты служебной конфиденциальной информации. Организация защиты коммерческой тайны. Организация защиты сведений, составляющих государственную тайну. Психологические аспекты информационной безопасности. Комплексный контроль защиты информации. Технические каналы утечки информации. Методы инженерной защиты и технической охраны объектов. Методы и средства поиска электронных устройств перехвата информации. Организация и методическое обеспечение инженерно-технической защиты информации.

3.4 Темы докладов

– Стандарты и спецификации в области информационной безопасности
– Технические каналы утечки информации и средства защиты

Согласована на портале № 19160

3.5 Темы контрольных работ

– Проведение патентных исследований. Подготовка заявки заявки на объект интеллектуальной собственности (изобретение, полезная модель, промышленный образец, товарный знак)

3.6 Вопросы для подготовки к практическим занятиям, семинарам

– Основные положения политики обеспечения информационной безопасности организации

– Организационные меры по обеспечению безопасности. Служебные инструкции и ответственность

– Современные методы и средства сетевой защиты. Безопасность носителей данных

4 Методические материалы

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

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

4.1. Основная литература

1. Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5171

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

4.2. Дополнительная литература

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

2. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/book/5170 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5170

3. Белов, Е.Б. Основы информационной безопасности. [Электронный ресурс] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана. [Электронный ресурс]. - http://e.lanbook.com/book/5121

4.3. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, свободный.

2. Защита и передача объектов интеллектуальной собственности: Методические указания для проведения практических и самостоятельных работ / Изоткина Н. Ю. - 2012. 12 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1944, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. https://www.yandex.ru/ - поисковая система Яндекс

Согласована на портале № 19160