МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **40.03.01 Юриспруденция**
Направленность (профиль): **Юриспруденция**
Форма обучения: **очная**
Факультет: **ЮФ, Юридический факультет**
Кафедра: **ИП, Кафедра информационного права**
Курс: **2**
Семестр: **3**
Учебный план набора 2017 года

Распределение рабочего времени

№	Виды учебной деятельности	3 семестр	Всего	Единицы
1	Лекции	10	10	часов
2	Практические занятия	24	24	часов
3	Всего аудиторных занятий	34	34	часов
4	Из них в интерактивной форме	6	6	часов
5	Самостоятельная работа	38	38	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Зачет: 3 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 9 » 6 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:

мнс каф. КИБЭВС _____ А. Ю. Якимук

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

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

Декан ЮФ _____ С. Л. Красинский

Заведующий выпускающей каф.
ИП _____ В. Г. Мельникова

Эксперт:

доцент каф. КИБЭВС _____ А. А. Конев

1. Цели и задачи дисциплины

1.1. Цели дисциплины

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.

1.2. 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 ОПОП

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

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информационные технологии в юридической деятельности.

Последующими дисциплинами являются: Правовое обеспечение предпринимательской деятельности (ГПО 1), Правовое сопровождение инновационной деятельности (ГПО 3).

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** сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

– **уметь** классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации

– **владеть** профессиональной терминологией в области 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
		3 семестр
Аудиторные занятия (всего)	34	34
Лекции	10	10
Практические занятия	24	24
Из них в интерактивной форме	6	6
Самостоятельная работа (всего)	38	38

Проработка лекционного материала	16	16
Написание рефератов	12	12
Подготовка к практическим занятиям, семинарам	10	10
Всего (без экзамена)	72	72
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
3 семестр					
1 Понятие информационной безопасности, ее роль в национальной безопасности	1	0	2	3	ОК-3, ОК-4
2 Терминологические основы информационной безопасности	1	6	6	13	ОК-3, ОК-4
3 Угрозы	1	0	2	3	ОК-3, ОК-4
4 Классификация и анализ угроз информационной безопасности	1	6	4	11	ОК-3, ОК-4
5 Модель угроз, модель нарушителя	1	6	4	11	ОК-3, ОК-4
6 Модели оценки угроз конфиденциальности, целостности, доступности	2	0	2	4	ОК-3, ОК-4
7 Функции и задачи защиты информации	2	6	16	24	ОК-3, ОК-4
8 Проблемы региональной информационной безопасности	1	0	2	3	ОК-3, ОК-4
Итого за семестр	10	24	38	72	
Итого	10	24	38	72	

5.2. Содержание разделов дисциплины (по лекциям)

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

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
3 семестр			

1 Понятие информационной безопасности, ее роль в национальной безопасности	Понятие информационной безопасности. Информационное право в теории государства и права. Информация как объект правового регулирования. Национальные интересы Российской Федерации в информационной сфере. Правовое обеспечение защиты информации.	1	ОК-3, ОК-4
	Итого	1	
2 Терминологические основы информационной безопасности	Основные термины и определения. Общедоступная информация и информация ограниченного доступа.	1	ОК-3, ОК-4
	Итого	1	
3 Угрозы	Угрозы. Уязвимости. Факторы. Характер происхождения угроз.	1	ОК-3, ОК-4
	Итого	1	
4 Классификация и анализ угроз информационной безопасности	Виды угроз. Источники угроз. Предпосылки появления угроз.	1	ОК-3, ОК-4
	Итого	1	
5 Модель угроз, модель нарушителя	Классы каналов несанкционированного получения информации. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Архитектура систем защиты информации. Семирубежная модель защиты информации.	1	ОК-3, ОК-4
	Итого	1	
6 Модели оценки угроз конфиденциальности, целостности, доступности	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования к вычислительным системам, которые используются для обработки конфиденциальной информации.	2	ОК-3, ОК-4
	Итого	2	
7 Функции и задачи защиты информации	Методы формирования функций защиты. Управление системой защиты информации. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии.	2	ОК-3, ОК-4

	Итого	2	
8 Проблемы региональной информационной безопасности	Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.	1	ОК-3, ОК-4
	Итого	1	
Итого за семестр		10	

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

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин							
	1	2	3	4	5	6	7	8
Предшествующие дисциплины								
1 Информационные технологии в юридической деятельности	+	+		+				
Последующие дисциплины								
1 Правовое обеспечение предпринимательской деятельности (ГПО 1)	+	+						
2 Правовое сопровождение инновационной деятельности (ГПО 3)	+		+					

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	+	+	+	Опрос на занятиях, Зачет, Реферат, Отчет по практическому занятию
ОК-4	+	+	+	Опрос на занятиях, Зачет, Реферат, 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	Интерактивные лекции	Всего
3 семестр			
Презентации с использованием интерактивной доски с обсуждением		2	2
Работа в команде	4		4
Итого за семестр:	4	2	6
Итого	4	2	6

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
3 семестр			
2 Терминологические основы информационной безопасности	Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы	6	ОК-3, ОК-4
	Итого	6	
4 Классификация и анализ угроз информационной безопасности	Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации	6	ОК-3, ОК-4
	Итого	6	
5 Модель угроз, модель нарушителя	Построение модели угроз для выбранного объекта информатизации	6	ОК-3, ОК-4
	Итого	6	
7 Функции и задачи защиты информации	Оценка безопасности информации на объектах ее обработки	6	ОК-3, ОК-4
	Итого	6	
Итого за семестр		24	

9. Самостоятельная работа

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

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
3 семестр				
1 Понятие информационной безопасности, ее роль в национальной безопасности	Проработка лекционного материала	2	ОК-3	Зачет, Опрос на занятиях
	Итого	2		
2 Терминологические основы информационной безопасности	Подготовка к практическим занятиям, семинарам	4	ОК-3, ОК-4	Зачет, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	6		
3 Угрозы	Проработка лекционного материала	2	ОК-4	Зачет, Опрос на занятиях
	Итого	2		
4 Классификация и анализ угроз информационной безопасности	Подготовка к практическим занятиям, семинарам	2	ОК-3, ОК-4	Зачет, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		
5 Модель угроз, модель нарушителя	Подготовка к практическим занятиям, семинарам	2	ОК-3, ОК-4	Зачет, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	4		
6 Модели оценки угроз конфиденциальности, целостности, доступности	Проработка лекционного материала	2	ОК-4	Зачет
	Итого	2		
7 Функции и задачи защиты информации	Подготовка к практическим занятиям, семинарам	2	ОК-3, ОК-4	Зачет, Опрос на занятиях, Отчет по практическому занятию, Реферат
	Написание рефератов	12		
	Проработка лекционного материала	2		
	Итого	16		
8 Проблемы региональной	Проработка лекционного материала	2	ОК-3	Зачет, Опрос на занятиях

информационной безопасности	Итого	2		
Итого за семестр		38		
Итого		38		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
3 семестр				
Зачет			30	30
Опрос на занятиях	5	5	10	20
Отчет по практическому занятию	10	10	10	30
Реферат			20	20
Итого максимум за период	15	15	70	100
Нарастающим итогом	15	30	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)

2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Шелупанов А.А., Сопов М.А. и др. Основы защиты информации. Учебное пособие. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf
2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. 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]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf
3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

12.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Основы информационной безопасности: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

1. Не предусмотрены.

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 используется мультимедийная лекционная аудитория, с количеством посадочных мест не менее 55-60, 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 (семинарских) занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 4 этаж, ауд. 407. Состав оборудования: Учебная мебель; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже плата Gigabyte GA-H55M-S2mATX/ Intel Original Soc-1156 Core i3 3.06 GHz/ DDR III Kingston CL9 - 2 штуки по 2048 Mb/ SATA-II 250Gb Hitachi / 1024 Mb GeForse GT240 PCI-E. с широкополосным доступом в Internet, – 6 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP3; Visual Studio 2010; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

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.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

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

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

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

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)

С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

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

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

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

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **40.03.01 Юриспруденция**
Направленность (профиль): **Юриспруденция**
Форма обучения: **очная**
Факультет: **ЮФ, Юридический факультет**
Кафедра: **ИП, Кафедра информационного права**
Курс: **2**
Семестр: **3**

Учебный план набора 2017 года

Разработчик:
- мнс каф. КИБЭВС А. Ю. Якимук

Зачет: 3 семестр

Томск 2017

1. Введение

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

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

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

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ОК-3	владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией	Должен знать сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; Должен уметь классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; Должен владеть профессиональной терминологией в области информационной безопасности;
ОК-4	способностью работать с информацией в глобальных компьютерных сетях	

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	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми	Работает при прямом наблюдении

уровень)		для выполнения простых задач	

2 Реализация компетенций

2.1 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 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Должен знать сущность и понятие информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	Должен уметь классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	Должен владеть профессиональной терминологией в области информационной безопасности
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Опрос на занятиях; • Реферат; • Отчет по практическому занятию; • Зачет;	• Опрос на занятиях; • Реферат; • Отчет по практическому занятию; • Зачет;	• Реферат; • 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)	• 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;

2.2 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 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	структуру сети Интернет основные Интернет-порталы правовой информации РФ и зарубежья	работать с информацией в глобальных компьютерных сетях работать с правовой информацией в глобальных компьютерных сетях	основными методами, способами и средствами поиска и получения информации в сети Интернет основными методами, способами и средствами поиска и получения правовой информации в сети Интернет
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Опрос на занятиях; • Реферат; • Отчет по практическому занятию; • Зачет;	• Опрос на занятиях; • Реферат; • Отчет по практическому занятию; • Зачет;	• Реферат; • Отчет по практическому занятию; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в та-

блице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• основные тенденции развития технологий передачи информаций в информационных системах;	• применяет сервисы глобальных компьютерных сетей в своей профессиональной деятельности;	• владеет навыками обработки и работы с конфиденциальной информацией;
Хорошо (базовый уровень)	• основные характеристики современных компьютерных информационных сетей;	• обладает диапазоном практических умений, требуемых для правоприменительной деятельности и умеет применять современные информационные технологии для поиска и обработки правовой информации в глобальной сети Интернет;	• навыками сбора и обработки информации в глобальной сети Интернет;
Удовлетворительно (пороговый уровень)	• обладает знаниями законодательства, необходимыми для правильного решения задач правоприменительной деятельности в изучаемой отрасли права (или области знаний);	• обладает основными умениями, требуемыми для выполнения задач правоприменительной деятельности;	• работает под контролем;

3 Типовые контрольные задания

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

3.1 Темы рефератов

– Структура органов государственной власти, регламентирующая деятельность по защите информации в РФ
– Современные способы идентификации и аутентификации в информационных системах
– Анализ руководящих документов по оценке защищенности автоматизированных систем

3.2 Зачёт

– Теория защиты информации. Основные направления
– Источники угроз. Предпосылки появления угроз
– Классификация требований к средствам защиты информации
– Способы и средства защиты информации

3.3 Темы опросов на занятиях

– Понятие информационной безопасности. Информационное право в теории государства и права. Информация как
– объект правового регулирования. Национальные интересы Российской Федерации в информационной сфере. Правовое обеспечение защиты информации.
– Основные термины и определения. Общедоступная информация и информация ограниченного доступа.
– Угрозы. Уязвимости. Факторы. Характер происхождения угроз.

– Виды угроз. Источники угроз. Предпосылки появления угроз.

– Классы каналов несанкционированного получения информации. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных. Архитектура систем защиты информации. Семирубежная модель защиты информации.

– Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования к вычислительным системам, которые используются для обработки конфиденциальной информации.

– Методы формирования функций защиты. Управление системой защиты информации. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека. Применение криптографии.

– Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта.

3.4 Вопросы для подготовки к практическим занятиям, семинарам

– Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы

– Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации

– Построение модели угроз для выбранного объекта информатизации

– Оценка безопасности информации на объектах ее обработки

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

2. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. 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]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

3. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 224с. ISBN 978-5-91191-228-7 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf

4.2. Дополнительная литература

1. Сост.: Шелупанов А.А., Сопов М.А,. и др. Нормативно-правовые акты информационной безопасности. Учебное пособие. В трех частях. Ч.3. Издание седьмое, перераб. и допол. Гриф СибРОУМО – Томск: В-Спектр, 2011. - 220с. ISBN 978-5-91191-229-5 [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf

4.3. Обязательные учебно-методические пособия

1. Мещеряков Р.В. Основы информационной безопасности: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/files/work_progs/metodich_oib_praktiki_i_sr.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрены.