

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
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: a1119608-cdff-4455-b54e-5235117c185c

Владелец: Семенко Павел Васильевич

Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Уровень образования: **высшее образование - магистратура**

Направление подготовки / специальность: **40.04.01 Юриспруденция**

Направленность (профиль) / специализация: **Цифровое право**

Форма обучения: **очно-заочная (в том числе с применением дистанционных образовательных технологий)**

Факультет: **Факультет дистанционного обучения (ФДО)**

Кафедра: **Кафедра информационного, гражданского права и правового обеспечения инновационной деятельности (ИГПиПОИД)**

Курс: **2**

Семестр: **3**

Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	8	8	часов
Практические занятия	8	8	часов
Самостоятельная работа	80	80	часов
Самостоятельная работа под руководством преподавателя	8	8	часов
Контрольные работы	4	4	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
		3	з.е.

Формы промежуточной аттестация	Семестр	Количество
Зачет	3	
Контрольные работы	3	2

## 1. Общие положения

### 1.1. Цели дисциплины

1. Сформировать компетенции, позволяющие осуществлять на высоком профессиональном уровне юридическую деятельность в сфере правового обеспечения информационной безопасности.

### 1.2. Задачи дисциплины

1. Изучить законодательство и практику его применения в сфере обеспечения информационной безопасности.

2. сформировать навыки толкования и применения права в сфере обеспечения информационной безопасности.

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль направления подготовки (hard skills - HS).

Индекс дисциплины: Б1.О.02.06.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

## 3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
<b>Универсальные компетенции</b>		
-	-	-
<b>Общепрофессиональные компетенции</b>		

ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Знает современные информационные технологии, применимые в юридической деятельности и требования информационной безопасности	Знает технологии защиты информации, применяемые в современной юридической деятельности для обеспечения соответствия требованиям информационной безопасности
	ОПК-7.2. Умеет выбирать подходящие для решения задач профессиональной деятельности информационные технологии и соблюдать требования информационной безопасности	Умеет выбирать подходящие для решения задач профессиональной деятельности технологии защиты информации и соблюдать требования информационной безопасности
	ОПК-7.3. Владеет навыками применения информационных технологий и профессиональных баз данных (справочно-правовых систем, государственных информационных систем ) для решения задач профессиональной деятельности с учетом требований информационной безопасности	Владеет навыками применения информационных технологий и профессиональных баз данных ( Консультант+, Гарант, ГАС, ГИС ) для решения задач профессиональной деятельности и обеспечения соблюдения требований информационной безопасности
<b>Профессиональные компетенции</b>		

ПК-3. Готов к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства	ПК-3.1. Знает законодательство о порядке проведения экспертиз нормативно-правовых (индивидуальных) актов в сфере цифровых прав; понятие, виды и значение юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере цифровых прав; содержание основных этапов проведения юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере цифровых прав	Знает законодательство о порядке проведения экспертиз нормативно-правовых (индивидуальных) актов в сфере обеспечения информационной безопасности; понятие, виды и значение юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере обеспечения информационной безопасности; содержание основных этапов проведения юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере обеспечения информационной безопасности
	ПК-3.2. Умеет осуществлять поиск, мониторинг, оценку и обработку правовых источников информации в сфере цифровых прав; составляет и оформляет основные виды письменных юридических заключений для участников общественных отношений в сфере цифровых прав; выявляет в ходе проведения юридических экспертиз дефекты нормативных правовых (индивидуальных) актов и их проектов, а также формулирует предложения по их устранению в сфере цифровых прав;	Осуществляет поиск, мониторинг, оценку и обработку правовых источников информации в сфере обеспечения информационной безопасности; составляет и оформляет основные виды письменных юридических заключений для участников общественных отношений в сфере обеспечения информационной безопасности; выявляет в ходе проведения юридических экспертиз дефекты нормативных правовых (индивидуальных) актов и их проектов, а также формулирует предложения по их устранению в сфере обеспечения информационной безопасности
	ПК-3.3. Готовит и представляет юридические заключения, осуществляет правовую экспертизу нормативных актов и их проектов в сфере цифровых прав	Готовит и представляет юридические заключения, осуществляет правовую экспертизу нормативных актов и их проектов в сфере обеспечения информационной безопасности

ПК-4. Способен принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности	ПК-4.1. Знает законодательство об осуществлении просветительской, информационной и консультационной работы в сфере цифровых прав для физических и юридических лиц, органов публичной власти и общественных объединений; виды и формы юридических консультаций, применяемых в сфере цифровых прав	Знает законодательство об осуществлении просветительской, информационной и консультационной работы в сфере цифровых прав для физических и юридических лиц, органов публичной власти и общественных объединений; виды и формы юридических консультаций, применяемых в сфере обеспечения информационной безопасности
	ПК-4.2. Составляет юридические заключения, используемые для осуществления просветительской, информационной и консультационной работы в сфере цифровых прав для физических и юридических лиц, органов публичной власти и общественных объединений	Составляет юридические заключения, используемые для осуществления просветительской, информационной и консультационной работы в сфере обеспечения информационной безопасности для физических и юридических лиц, органов публичной власти и общественных объединений
	ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления просветительской, информационной и консультационной работы в сфере цифровых прав для физических и юридических лиц, органов публичной власти и общественных объединений	Владеет навыками представления юридических заключений, используемых для осуществления просветительской, информационной и консультационной работы в сфере обеспечения информационной безопасности для физических и юридических лиц, органов публичной власти и общественных объединений

**4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		3 семестр
<b>Контактная аудиторная работа обучающихся с преподавателем, всего</b>	28	28
Лекционные занятия	8	8
Практические занятия	8	8

Самостоятельная работа под руководством преподавателя	8	8
Контрольные работы	4	4
<b>Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего</b>	80	80
Проработка лекционного материала	22	22
Самостоятельное изучение тем (вопросов) теоретической части дисциплины	28	28
Подготовка к контрольной работе	30	30
<b>Общая трудоемкость (в часах)</b>	108	108
<b>Общая трудоемкость (в з.е.)</b>	3	3

## 5. Структура и содержание дисциплины

### 5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Контр. раб.	СРП, ч.	Сам. раб., ч	Всего часов (без промежуточной аттестации)	Формируемые компетенции
<b>3 семестр</b>							
1 Информационная безопасность: основные понятия	2	2	4	2	11	21	ОПК-7, ПК-3, ПК-4
2 Организационное обеспечение информационной безопасности	1	1		1	13	16	ОПК-7, ПК-3, ПК-4
3 Нормативно-правовое обеспечение информационной безопасности	1	1		1	14	17	ОПК-7, ПК-3, ПК-4
4 Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации	2	1		1	18	22	ОПК-7, ПК-3, ПК-4
5 Правовые режимы обеспечения безопасности информации ограниченного доступа	1	1		1	12	15	ОПК-7, ПК-3, ПК-4
6 Юридическая ответственность за правонарушения в информационной сфере	1	2		2	12	17	ОПК-7, ПК-3, ПК-4
Итого за семестр	8	8	4	8	80	108	
Итого	8	8	4	8	80	108	

### 5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины	Трудоемкость (лекционные занятия), ч	СРП, ч	Формируемые компетенции
<b>3 семестр</b>				
1 Информационная безопасность: основные понятия	Понятие информационной безопасности, основные задачи и методы ее обеспечения. Национальные интересы РФ в информационной сфере и их обеспечение. Угрозы информационной безопасности. Государственная политика в сфере информационной безопасности. Понятие информационной безопасности личности. Информационно-психологическая безопасность личности. Информационно-идеологическая безопасность личности. Понятие информационной безопасности общества. Угрозы информационной безопасности общества. Понятие информационной безопасности государства. Угрозы информационной безопасности государства.	2	2	ОПК-7, ПК-3, ПК-4
	Итого	2	2	
2 Организационное обеспечение информационной безопасности	Понятие и предмет обеспечения информационной безопасности (ОИБ). Организационные меры по обеспечению информационной безопасности на уровне международного сотрудничества, на уровне РФ, на уровне организации.	1	1	ОПК-7, ПК-3, ПК-4
	Итого	1	1	
3 Нормативно-правовое обеспечение информационной безопасности	Объекты правового регулирования ОИБ. Уровни правового регулирования ОИБ. Источники права в сфере обеспечения информационной безопасности	1	1	ОПК-7, ПК-3, ПК-4
	Итого	1	1	

4 Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации	Понятие и характеристика информационной инфраструктуры. Ее элементы. Понятие критической информационной инфраструктуры. Объекты КИИ. Категорирование объектов КИИ. Требования к обеспечению безопасности КИИ.	2	1	ОПК-7, ПК-3, ПК-4
	Итого	2	1	
5 Правовые режимы обеспечения безопасности информации ограниченного доступа	Правовые режимы информации Правовые средства обеспечения режимов информации Роль локальных нормативных актов в обеспечении правового режима информации Виды информации ограниченного доступа. Конфиденциальная информация Режим коммерческой тайны Режим служебной тайны Государственная тайна: понятие, режим, порядок засекречивания/рассекречивания	1	1	ОПК-7, ПК-3, ПК-4
	Итого	1	1	
6 Юридическая ответственность за правонарушения в информационной сфере	Общая характеристика и виды ответственности за правонарушения в информационной сфере. Дисциплинарная ответственность в информационной сфере. Административная ответственность в информационной сфере. Уголовная ответственность в информационной сфере. Материальная ответственность в информационной сфере. Особенности ответственности в области массовой информации. Особенности ответственности в сети «Интернет».	1	2	ОПК-7, ПК-3, ПК-4
	Итого	1	2	
Итого за семестр		8	8	
Итого		8	8	

### 5.3. Контрольные работы

Виды контрольных работ и часы на контрольные работы приведены в таблице 5.3.

Таблица 5.3 – Контрольные работы

№ п.п.	Виды контрольных работ	Трудоемкость, ч	Формируемые компетенции
--------	------------------------	-----------------	-------------------------



3 семестр			
1	Контрольная работа	2	ОПК-7, ПК-3, ПК-4
2	Контрольная работа	2	ОПК-7, ПК-3, ПК-4
Итого за семестр		4	
Итого		4	

#### 5.4. Лабораторные занятия

Не предусмотрено учебным планом

#### 5.5. Контроль самостоятельной работы (курсовой проект / курсовая работа)

Не предусмотрено учебным планом

#### 5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
<b>3 семестр</b>				
1 Информационная безопасность: основные понятия	Проработка лекционного материала	3	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	4	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	11		
2 Организационное обеспечение информационной безопасности	Проработка лекционного материала	3	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	5	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	5	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	13		

3 Нормативное-правовое обеспечение информационной безопасности	Проработка лекционного материала	4	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	5	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	5	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	14		
4 Правовые средства обеспечения информационной инфраструктуры Российской Федерации	Проработка лекционного материала	4	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	8	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	18		
5 Правовые режимы обеспечения безопасности информации ограниченного доступа	Проработка лекционного материала	4	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	4	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	12		
6 Юридическая ответственность за правонарушения в информационной сфере	Проработка лекционного материала	4	ОПК-7, ПК-3, ПК-4	Зачёт
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	4	ОПК-7, ПК-3, ПК-4	Зачёт, Тестирование
	Подготовка к контрольной работе	4	ОПК-7, ПК-3, ПК-4	Контрольная работа
	Итого	12		
Итого за семестр		80		
Итого		80		

### 5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной

деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности					Формы контроля
	Лек. зан.	Прак. зан.	Конт.Раб.	СРП	Сам. раб.	
ОПК-7	+	+	+	+	+	Зачёт, Контрольная работа, Тестирование
ПК-3	+	+	+	+	+	Зачёт, Контрольная работа, Тестирование
ПК-4	+	+	+	+	+	Зачёт, Контрольная работа, Тестирование

## 6. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется

## 7. Учебно-методическое и информационное обеспечение дисциплины

### 7.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/498844>.

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/496492>.

### 7.2. Дополнительная литература

1. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/488767>.

### 7.3. Учебно-методические пособия

#### 7.3.1. Обязательные учебно-методические пособия

1. Методические указания по организации и выполнению самостоятельной работы студентами очной формы обучения по направлению подготовки 40.04.01. (магистратура) «Юриспруденция», направленность (профиль) подготовки «Цифровое право»: В.Г. Мельникова, Д.В. Хаминов, И.В. Чаднова. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники / Хаминов Д. В., Чаднова И. В., Мельникова В. Г. — 2022. 17 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/9871>.

2. Семинарские (практические) занятия: Методические указания по выполнению семинарских (практических) занятий для студентов очной формы обучения по направлению 40.04.01 «Юриспруденция» профиль «Цифровое право» / В. Г. Мельникова, Д. В. Хаминов, И. В. Чаднова - 2022. 12 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/9872>.

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

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся

из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

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

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

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

- в форме электронного документа;
- в печатной форме.

#### **7.4. Иное учебно-методическое обеспечение**

1. Мельникова В.Г. Правовое обеспечение информационной безопасности/ В.Г. Мельникова - Томск [Электронный ресурс]: ТУСУР, ФДО, 2022 (доступ из личного кабинета студента) .

#### **7.5. Современные профессиональные базы данных и информационные справочные системы**

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: <https://lib.tusur.ru/ru/resursy/bazy-dannyh>.

### **8. Материально-техническое и программное обеспечение дисциплины**

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

Учебные аудитории для проведения занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, для самостоятельной работы студентов

634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- Веб-камера - 6 шт.;
- Наушники с микрофоном - 6 шт.;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Google Chrome;
- Kaspersky Endpoint Security для Windows;
- LibreOffice;
- Microsoft Windows;

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

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

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;

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

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

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

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

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

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

## 9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

### 9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Информационная безопасность: основные понятия	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
2 Организационное обеспечение информационной безопасности	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий

3 Нормативно-правовое обеспечение информационной безопасности	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
4 Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
5 Правовые режимы обеспечения безопасности информации ограниченного доступа	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий
6 Юридическая ответственность за правонарушения в информационной сфере	ОПК-7, ПК-3, ПК-4	Зачёт	Перечень вопросов для зачета
		Контрольная работа	Примерный перечень тем и тестовых заданий на контрольные работы
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков

4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне <b>ориентирования</b> , представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на <b>репродуктивном</b> уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на <b>аналитическом</b> уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на <b>системном</b> уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

### 9.1.1. Примерный перечень тестовых заданий

1. Объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы – это:
  - а) угроза информационной безопасности
  - б) угроза национальной безопасности
  - в) национальные интересы в военной сфере
  - г) национальные интересы в информационной сфере
2. информационная безопасность Российской Федерации – это:
  - а) осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;
  - б) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав

- и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
- в) состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий;
- г) состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны;
3. Сведения о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства должны иметь режим:
- а) общедоступной информации
  - б) открытых данных
  - в) коммерческой тайны
  - г) государственной тайны
4. Что из перечисленного не является видом мер по обеспечению информационной безопасности:
- а) организационные
  - б) технические
  - в) информационные
  - г) правовые
5. Что из перечисленного не является объектом информационной инфраструктуры:
- а) автоматизированная система управления
  - б) сеть электросвязи
  - в) многофункциональный центр
  - г) информационно-телекоммуникационная сеть
6. целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации – это
- а) компьютерный инцидент
  - б) компьютерная атака
  - в) телекоммуникационная атака
  - г) сетевая авария
7. факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки – это:
- а) компьютерный инцидент
  - б) компьютерная атака
  - в) телекоммуникационная атака
  - г) сетевая авария
8. По какому из данных объектов требуется проводить категорирование?
- а) бетономешалка
  - б) АСУ банка
  - в) база данных клиентов магазина (ок. 200 клиентов)
  - г) локальная компьютерная сеть из 10 компьютеров
9. К средствам обеспечения информационной безопасности относятся:
- а) технические средства, используемые силами обеспечения информационной безопасности;
  - б) правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;



- в) организационные средства, используемые силами информационной безопасности
  - г) правовые средства, используемые средствами обеспечения информационной безопасности
10. Какой из документов необходимо оформить субъекту критической информационной инфраструктуры для исполнения обязанностей по информационной безопасности:
- а) Устав
  - б) Приказ о назначении начальника службы безопасности
  - в) Положение о защите персональных данных
  - г) Сведения о категорировании объектов КИИ
11. Виды информационной безопасности:
- а) Персональная, корпоративная, государственная
  - б) Клиентская, серверная, сетевая
  - в) Локальная, глобальная, смешанная
  - г) Коммерческая, служебная, государственная
12. К правовым методам, обеспечивающим информационную безопасность, относятся:
- а) Разработка аппаратных средств обеспечения правовых данных
  - б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
  - в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
  - г) Разработка пропускного режима
13. К принципам политики информационной безопасности относится принцип:
- а) Невозможности миновать защитные средства сети (системы)
  - б) Усиления основного звена сети, системы
  - в) Полного блокирования доступа при риск-ситуациях
  - г) Недопуска на территорию внешних субъектов
14. Принципом политики информационной безопасности является принцип:
- а) Усиления защищенности самого незащищенного звена сети (системы)
  - б) Перехода в безопасное состояние работы сети, системы
  - в) Полного доступа пользователей ко всем ресурсам сети, системы
  - г) Полного блокирования доступа при риск-ситуациях
15. Принципом политики информационной безопасности является принцип:
- а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
  - б) Одноуровневой защиты сети, системы
  - в) Совместимых, однотипных программно-технических средств сети, системы
  - г) Недопуска на территорию внешних субъектов
16. Ответственность за защищенность данных в компьютерной сети несет:
- а) Владелец сети
  - б) Администратор сети
  - в) Пользователь сети
  - г) Менеджер сети
17. Утечкой информации в системе называется ситуация, характеризующаяся:
- а) Потерей данных в системе
  - б) Изменением формы информации
  - в) Изменением содержания информации
  - г) Внедрением фэйковой информации
18. Совокупность содержащейся в базах данных информации, и информационных технологий и технических средств, обеспечивающих ее обработку, называется:
- а) система защиты информации
  - б) автоматизированная система
  - в) информационная система
  - г) система обработки персональных данных
19. Как называется лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам?
- а) субъект персональных данных
  - б) оператор информационной системы

- в) обладатель информации
  - г) пользователь информации
20. Как называется гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных?
- а) обладатель информации
  - б) субъект информации
  - в) обладатель информационной системы
  - г) оператор информационной системы

### 9.1.2. Перечень вопросов для зачета

Приведены примеры типовых заданий из банка контрольных тестов, составленных по пройденным разделам дисциплины

1. Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства?
  - а) Федеральный закон “Об информации, информационных технологиях и о защите информации”
  - б) Федеральный закон “О государственной тайне”
  - в) Доктрина информационной безопасности Российской Федерации
  - г) Федеральный закон “О безопасности”
2. Кто признается инсайдером?
  - а) сотрудник, который стал источником утечки информации
  - б) любой источник информации
  - в) программа-вирус, обеспечивающая утечку информации
  - г) владелец сети
3. Сведения о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства должны иметь режим:
  - а) общедоступной информации
  - б) открытых данных
  - в) коммерческой тайны
  - г) государственной тайны
4. Что из перечисленного не является видом мер по обеспечению информационной безопасности:
  - а) организационные
  - б) технические
  - в) информационные
  - г) правовые
5. Что из перечисленного не является объектом информационной инфраструктуры:
  - а) автоматизированная система управления
  - б) сеть электросвязи
  - в) многофункциональный центр
  - г) информационно-телекоммуникационная сеть
6. Комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов называется
  - а) лицензирование
  - б) сертификация
  - в) торговая марка
  - г) товарный знак
7. К коммерческой тайне не относятся:
  - а) сведения о заработной плате
  - б) сведения о размере сделок
  - в) сведения о технологии
  - г) сведения о контрагентах
8. К органам, осуществляющим контроль в сфере обеспечения информационной

- безопасности относится:
- а) Полиция
  - б) Таможня
  - в) суд
  - г) ФСТЭК
9. Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры - это
- а) объекты КИИ
  - б) субъекты КИИ
  - в) информационная инфраструктура
  - г) значимый объект
10. К принципам обеспечения безопасности критической информационной инфраструктуры относится:
- а) приоритет предотвращения компьютерных атак
  - б) конфиденциальность
  - в) доступность
  - г) актуальность

### **9.1.3. Примерный перечень тем и тестовых заданий на контрольные работы**

Правовое обеспечение информационной безопасности

1. Информационная безопасность: основные понятия
2. Организационное обеспечение информационной безопасности
3. Нормативно-правовое обеспечение информационной безопасности
4. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации
5. Правовые режимы обеспечения безопасности информации ограниченного доступа

### **9.2. Методические рекомендации**

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе по дисциплине.

При изучении дисциплины необходимо обращать особое внимание на требования по

обеспечению информационной безопасности их отражение в нормативно-правовых актах различного уровня. Следует изучать теоретические положения по рекомендованным источникам и лекциям, затем соотнести теоретические положения с нормами действующих нормативно-правовых актов. Студентам следует уделять внимание правовым и организационным мерам обеспечения информационной безопасности, а также учитывать постоянный технический прогресс в сфере угроз информационной безопасности и мерам, позволяющим им противостоять.

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

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

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

### **9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

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

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

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

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

**Для лиц с нарушениями зрения:**

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

**Для лиц с нарушениями слуха:**

- в форме электронного документа;

– в печатной форме.

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

– в форме электронного документа;

– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

## ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры ИГПиПОИД  
протокол № 6 от «18» 1 2023 г.

### СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ИГПиПОИД	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14- b705-b5087cef9b02
Заведующий обеспечивающей каф. ИГПиПОИД	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14- b705-b5087cef9b02
Декан ФДО	И.П. Черкашина	Согласовано, 4580bdea-d7a1-4d22- bda1-21376d739cfc

### ЭКСПЕРТЫ:

Заведующий кафедрой, каф. ИГПиПОИД	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14- b705-b5087cef9b02
Специалист по учебно-методической работе I категории, каф. ЮФ	С.Ю. Звезгинцева	Согласовано, 7de46f77-2f66-455c- 96f1-56c003651096

### РАЗРАБОТАНО:

Заведующий кафедрой, каф. ИП	В.Г. Мельникова	Разработано, 72b97820-0b02-4f14- b705-b5087cef9b02
------------------------------	-----------------	--