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: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЯ

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)**
Кафедра: **информационного, гражданского права и правового обеспечения инновационной деятельности (ИГПиПОИД)**
Курс: **2**
Семестр: **4**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	4 семестр	Всего	Единицы
Лекционные занятия	10	10	часов
Практические занятия	10	10	часов
Самостоятельная работа	112	112	часов
Самостоятельная работа под руководством преподавателя	10	10	часов
Контрольные работы	2	2	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
		4	з.е.

Формы промежуточной аттестации	Семестр	Количество
Зачет с оценкой	4	
Контрольные работы	4	1

Томск

1. Общие положения

1.1. Цели дисциплины

1. изучение теоретических и практических вопросов обеспечения информационной безопасности личности, общества, бизнеса и государства в новых технологических условиях, вопросов борьбы с киберпреступностью.

2. формирование у студентов навыков юридического сопровождения процессов, связанных с обеспечением информационной безопасности и противодействия киберпреступлениям.

1.2. Задачи дисциплины

1. углубленное усвоение студентами отраслевых теоретических знаний в рамках отрасли права «Уголовное право», включающей как общие положения уголовной ответственности в РФ, так и преступления главы 28 УК РФ "Преступления в сфере компьютерной информации", а так же смежные многообъектные преступления.

2. закрепление студентами отраслевых теоретических знаний в рамках отрасли права «Уголовное право», включающей как общие положения уголовной ответственности в РФ, так и преступления главы 28 УК РФ "Преступления в сфере компьютерной информации", а так же смежные многообъектные преступления.

3. уяснение студентами специфических положений отраслевых теоретических знаний в рамках отрасли права «Уголовное право», включающей как общие положения уголовной ответственности в РФ, так и преступления главы 28 УК РФ "Преступления в сфере компьютерной информации", а так же смежные многообъектные преступления.

4. приобретение студентами навыков по применению отраслевых теоретических знаний в рамках отрасли права «Уголовное право», включающей как общие положения уголовной ответственности в РФ, так и преступления главы 28 УК РФ "Преступления в сфере компьютерной информации", а так же смежные многообъектные преступления.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль профессиональной подготовки (major).

Индекс дисциплины: Б1.В.01.ДВ.04.01.

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
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		

ПК-1. Способен разрабатывать нормативные правовые акты	ПК-1.1. Знает формы и способы совершенствования отраслевых нормативных правовых актов имеет представление об актуальных проблемах правового регулирования в сфере цифровых прав	Знает формы и способы совершенствования нормативных правовых актов, регулирующих уголовную ответственность за киберпреступления; имеет представление об актуальных проблемах правового регулирования в сфере уголовной ответственности за киберпреступления
	ПК-1.2. Обосновывает необходимость совершенствования правового регулирования; оценивает законодательные инициативы в сфере цифровых прав	Обосновывает необходимость совершенствования правового регулирования в сфере уголовной ответственности за киберпреступления; оценивает законодательные инициативы в сфере цифровых прав
	ПК-1.3. Разрабатывает проекты нормативных правовых актов в сфере цифровых прав	Разрабатывает проекты нормативных правовых актов в сфере уголовной ответственности за киберпреступления
ПК-2. Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	ПК-2.1. Знает правовые основы и правоприменительну ю практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норма материального и процессуального права в сфере цифровых прав	Знает правовые основы и правоприменительную практику в сфере уголовной ответственности за киберпреступления; теоретические основы юридической оценки уголовно-правовых ситуаций; методику решения практических задач применения норма материального и процессуального права в сфере цифровых прав
	ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительно й деятельности; участвовать в процессе решения правовых споров; оценивать результативность и последовательность правовых решений в сфере цифровых прав	Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в сфере уголовной ответственности за киберпреступления; участвовать в процессе решения уголовно-правовых споров; оценивать результативность и последовательность правовых решений в сфере цифровых прав
	ПК-2.3. Владеет навыками составления правовых документов по требованиям юридической техники в сфере цифровых прав	Составляет правовые документы по требованиям юридической техники в сфере уголовной ответственности за киберпреступления

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 нормативноправовых (индивидуальных) актов в сфере уголовной ответственности за киберпреступления; понятие, виды и значение юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере уголовной ответственности за киберпреступления; содержание основных этапов проведения юридических экспертиз проектов нормативных правовых (индивидуальных) актов в сфере уголовной ответственности за киберпреступления
	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 уголовной ответственности за киберпреступления; составляет и оформляет основные виды письменных юридических заключений для участников общественных отношений в сфере уголовной ответственности за киберпреступления; 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
	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 уголовной ответственности за киберпреступления

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 4 зачетных единиц, 144 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
		4 семестр
Контактная работа обучающихся с преподавателем, всего	32	32
Лекционные занятия	10	10
Практические занятия	10	10
Самостоятельная работа под руководством преподавателя	10	10
Контрольные работы	2	2
Самостоятельная работа обучающихся, всего	112	112
Проработка лекционного материала	36	36
Самостоятельное изучение тем (вопросов) теоретической части дисциплины	40	40
Подготовка к контрольной работе	36	36
Общая трудоемкость (в часах)	144	144
Общая трудоемкость (в з.е.)	4	4

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
4 семестр							
1 Киберпреступность как новая криминальная угроза	1	1	2	1	18	23	ПК-1, ПК-2, ПК-3
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	2	2		2	18	24	ПК-1, ПК-2, ПК-3
3 Киберпреступления и уголовное законодательство Российской Федерации	1	1		2	19	23	ПК-1, ПК-2, ПК-3
4 Понятие преступлений в сфере цифровой информации и их система	2	2		1	19	24	ПК-1, ПК-2, ПК-3
5 Виды преступлений в сфере цифровой информации	2	2		2	19	25	ПК-1, ПК-2, ПК-3
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	2	2		2	19	25	ПК-1, ПК-2, ПК-3
Итого за семестр	10	10	2	10	112	144	
Итого	10	10	2	10	112	144	

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
4 семестр				
1 Киберпреступность как новая криминальная угроза	Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления. Международные масштабы киберпреступности. Конвенция о киберпреступности (Будапешт, 2001 г.) и дополнительный протокол к ней о типах уголовных правонарушений информационной безопасности. Правовые возможности борьбы с киберпреступностью: обзор международных, региональных и национальных моделей, их взаимосвязь.	1	1	ПК-1, ПК-2, ПК-3
	Итого	1	1	
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	Понятие и виды информации (компьютерная информация, документированная и недокументированная информация), Отношения в сфере обращения информации. Состояние развития информационных технологий в РФ и мире. Понятие, предмет и система информационной безопасности. Определение и основные термины информационной безопасности. Российские и международные стандарты управления информационной безопасностью. Правовые основы защиты информации. Объекты обеспечения информационной безопасности: сведения, сообщения, информационные потоки, информационная инфраструктура, статус субъектов информационной сферы. Уязвимость информации в системах ее хранения, передачи, обработки и отражения. Права граждан в информационной сфере. Цифровая безопасность и информационная безопасность. Виды защищаемой информации по законодательству РФ (государственная тайна, конфиденциальная информация, служебная тайна, профессиональная тайна, коммерческая тайна, банковская тайна и т.д.). Цифровая безопасность как объект уголовно-правовой охраны (основной, дополнительный и факультативный). Компьютерная (цифровая) информация как предмет преступлений. Международное сотрудничество в области защиты информации. Система международных органов, государственных органов России и зарубежных государств, осуществляющих борьбу с преступлениями в сфере высоких технологий	2	2	ПК-1, ПК-2, ПК-3
	Итого	2	2	

3 Киберпреступления и уголовное законодательство Российской Федерации	Киберпреступления в системе Особенной части УК РФ. Дуалистическая система: специальные и общие составы. Предметная основа составов. Основополагающие документы в области обеспечения информационной безопасности Российской Федерации (Конституционные гарантии права на информацию, Доктрина национальной безопасности, Доктрина информационной безопасности, Стратегия информационной безопасности, ФЗ "Об информации, информационных технологиях и о защите информации", ФЗ "О безопасности критической информационной инфраструктуры"), Закон РФ "Об информации, информационных технологиях и о защите информации", Закон РФ "О связи", Закон РФ "Об авторском праве и смежных правах", Закон РФ "О государственной тайне", Закон РФ "Об электронной цифровой подписи", Закон РФ "Об участии в международном информационном обмене"). Международные документы в сфере регулирования безопасности компьютерной информации. Конвенция об обеспечении международной информационной безопасности. Соглашения "О Сотрудничестве Государств-Участников СНГ в борьбе с преступлениями в сфере компьютерной информации". Европейская конвенция о киберпреступности.	1	2	ПК-1, ПК-2, ПК-3
	Итого	1	2	
4 Понятие преступлений в сфере цифровой информации и их система	Преступления в сфере цифровой безопасности и их классификация. Криминологическая характеристика преступности в сфере цифровой информации (статистика ГИАЦ МВД). Причины и условия, место преступлений в сфере цифровой информации. Установление уголовной ответственности против информационной безопасности. Способы совершения и меры предупреждения преступлений против информационной безопасности.	2	1	ПК-1, ПК-2, ПК-3
	Итого	2	1	

5 Виды преступлений в сфере цифровой информации	Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации, Создание, использование и распространение вредоносных компьютерных программ, Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Объективная и субъективная сторона преступлений в сфере компьютерной информации. Квалифицированные виды составов. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, получение данных, незаконный перехват информационных ресурсов, искажение информации). Преступления, связанные с контентом (детская порнография, расизм, агрессивные высказывания и др.). Преступления, связанные с нарушением интеллектуальных прав. Преступления, связанные с применением компьютеров и компьютерных технологий (компьютерное мошенничество, использование персональных данных, полученных незаконным путем, кибертерроризм, отмывание денег, др.).	2	2	ПК-1, ПК-2, ПК-3
	Итого	2	2	

6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	Иные (общие) преступления, совершаемые с использованием информационных технологий или в отношении телекоммуникационных сетей, в сфере экономики, охраны конституционных прав граждан, общественной безопасности и здоровья населения. Приемы выделения отдельных преступлений в тексте уголовного закона. Кража, Мошенничество с использованием электронных средств платежа, Мошенничество в сфере компьютерной информации, Незаконные организация и проведение азартных игр, Манипулирование рынком, Фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета, Внесение заведомо ложных сведений в межевой план, технический план, акт обследования, проект межевания земельного участка или земельных участков либо карту-план территории, Незаконное получение кредита, Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах, Манипулирование рынком, Неправомерное использование инсайдерской информации, Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем. Криптовалюта как предмет преступления. Виды и методы киберпреступлений.	2	2	ПК-1, ПК-2, ПК-3
	Итого	2	2	
	Итого за семестр	10	10	
	Итого	10	10	

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

5.4. Лабораторные занятия

Не предусмотрено учебным планом

5.5. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.5.

Таблица 5.5. – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			

1 Киберпреступность как новая криминальная угроза	Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления. Международные масштабы киберпреступности. Конвенция о киберпреступности (Будапешт, 2001 г.) и дополнительный протокол к ней о типах уголовных правонарушений информационной безопасности. Правовые возможности борьбы с киберпреступностью: обзор международных, региональных и национальных моделей, их взаимосвязь.	1	ПК-1, ПК-2, ПК-3
	Итого	1	
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	Понятие и виды информации (компьютерная информация, документированная и недокументированная информация), Отношения в сфере обращения информации. Состояние развития информационных технологий в РФ и мире. Понятие, предмет и система информационной безопасности. Определение и основные термины информационной безопасности. Российские и международные стандарты управления информационной безопасностью. Правовые основы защиты информации. Объекты обеспечения информационной безопасности: сведения, сообщения, информационные потоки, информационная инфраструктура, статус субъектов информационной сферы. Уязвимость информации в системах ее хранения, передачи, обработки и отражения. Права граждан в информационной сфере. Цифровая безопасность и информационная безопасность. Виды защищаемой информации по законодательству РФ (государственная тайна, конфиденциальная информация, служебная тайна, профессиональная тайна, коммерческая тайна, банковская тайна и т.д.). Цифровая безопасность как объект уголовно-правовой охраны (основной, дополнительный и факультативный). Компьютерная (цифровая) информация как предмет преступлений. Международное сотрудничество в области защиты информации. Система международных органов, государственных органов России и зарубежных государств, осуществляющих борьбу с преступлениями в сфере высоких технологий	2	ПК-1, ПК-2, ПК-3
	Итого	2	

3 Киберпреступления и уголовное законодательство Российской Федерации	Киберпреступления в системе Особенной части УК РФ. Дуалистическая система: специальные и общие составы. Предметная основа составов. Основополагающие документы в области обеспечения информационной безопасности Российской Федерации (Конституционные гарантии права на информацию, Доктрина национальной безопасности, Доктрина информационной безопасности, Стратегия информационной безопасности, ФЗ "Об информации, информационных технологиях и о защите информации", ФЗ "О безопасности критической информационной инфраструктуры"), Закон РФ "Об информации, информационных технологиях и о защите информации", Закон РФ "О связи", Закон РФ "Об авторском праве и смежных правах", Закон РФ "О государственной тайне", Закон РФ "Об электронной цифровой подписи", Закон РФ "Об участии в международном информационном обмене"). Международные документы в сфере регулирования безопасности компьютерной информации. Конвенция об обеспечении международной информационной безопасности. Соглашения "О Сотрудничестве Государств-Участников СНГ в борьбе с преступлениями в сфере компьютерной информации". Европейская конвенция о киберпреступности.	1	ПК-1, ПК-2, ПК-3
	Итого	1	
4 Понятие преступлений в сфере цифровой информации и их система	Преступления в сфере цифровой безопасности и их классификация. Криминологическая характеристика преступности в сфере цифровой информации (статистика ГИАЦ МВД). Причины и условия, место преступлений в сфере цифровой информации. Установление уголовной ответственности против информационной безопасности. Способы совершения и меры предупреждения преступлений против информационной безопасности.	2	ПК-1, ПК-2, ПК-3
	Итого	2	

5 Виды преступлений в сфере цифровой информации	Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации, Создание, использование и распространение вредоносных компьютерных программ, Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Объективная и субъективная сторона преступлений в сфере компьютерной информации. Квалифицированные виды составов. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, получение данных, незаконный перехват информационных ресурсов, искажение информации). Преступления, связанные с контентом (детская порнография, расизм, агрессивные высказывания и др.). Преступления, связанные с нарушением интеллектуальных прав. Преступления, связанные с применением компьютеров и компьютерных технологий (компьютерное мошенничество, использование персональных данных, полученных незаконным путем, кибертерроризм, отмывание денег, др.).	2	ПК-1, ПК-2, ПК-3
	Итого	2	

6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	Иные (общие) преступления, совершаемые с использованием информационных технологий или в отношении телекоммуникационных сетей, в сфере экономики, охраны конституционных прав граждан, общественной безопасности и здоровья населения. Приемы выделения отдельных преступлений в тексте уголовного закона. Кража, Мошенничество с использованием электронных средств платежа, Мошенничество в сфере компьютерной информации, Незаконные организация и проведение азартных игр, Манипулирование рынком, Фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета, Внесение заведомо ложных сведений в межевой план, технический план, акт обследования, проект межевания земельного участка или земельных участков либо карту-план территории, Незаконное получение кредита, Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах, Манипулирование рынком, Неправомерное использование инсайдерской информации, Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем. Криптовалюта как предмет преступления. Виды и методы киберпреступлений.	2	ПК-1, ПК-2, ПК-3
	Итого	2	
Итого за семестр		10	
Итого		10	

5.6. Контроль самостоятельной работы (курсовой проект / курсовая работа)

Не предусмотрено учебным планом

5.7. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.7.

Таблица 5.7. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
4 семестр				

1 Киберпреступность как новая криминальная угроза	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	18		
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	18		
3 Киберпреступления и уголовное законодательство Российской Федерации	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	7	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	19		
4 Понятие преступлений в сфере цифровой информации и их система	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	7	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	19		

5 Виды преступлений в сфере цифровой информации	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	7	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	19		
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	Проработка лекционного материала	6	ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	7	ПК-1, ПК-2, ПК-3	Зачёт с оценкой, Тестирование
	Подготовка к контрольной работе	6	ПК-1, ПК-2, ПК-3	Контрольная работа
	Итого	19		
Итого за семестр		112		
Итого		112		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.8.

Таблица 5.8 – Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Формируемые компетенции	Виды учебной деятельности					Формы контроля
	Лек. зан.	Прак. зан.	Конт.Раб.	СРП	Сам. раб.	
ПК-1	+	+	+	+	+	Зачёт с оценкой, Контрольная работа, Тестирование
ПК-2	+	+	+	+	+	Зачёт с оценкой, Контрольная работа, Тестирование
ПК-3	+	+	+	+	+	Зачёт с оценкой, 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. Уголовное право России. Общая часть : учебник для бакалавриата, специалитета и магистратуры / О. С. Капинус [и др.] ; под редакцией О. С. Капинус. — 2-е изд. — Москва : Издательство Юрайт, 2019. — 704 с. — (Бакалавр. Специалист. Магистр). — ISBN 978-5-534-09728-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/428526
.

2. Уголовное право России. Особенная часть в 2 т. Том 1 : учебник для вузов / О. С. Капинус [и др.] ; под редакцией О. С. Капинус. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 556 с. — (Высшее образование). — ISBN 978-5-534-09778-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490755.

3. Уголовное право России. Особенная часть в 2 т. Том 2 : учебник для вузов / О. С. Капинус [и др.] ; под редакцией О. С. Капинус. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 639 с. — (Высшее образование). — ISBN 978-5-534-09736-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490756.

7.2. Дополнительная литература

1. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-13898-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/496747.

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.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. 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.

2. 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 / Д. В. Хаминов, И. В. Чаднова, В. Г. Мельникова - 2022. 17 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9871.

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

Учебно-методические материалы для самостоятельной 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. Шеслер А.В., Ахмедшина Н.В. Уголовная ответственность за киберпреступления [Электронный ресурс]: электронный курс. Томск: ФДО, ТУСУР, 2023. (доступ из личного кабинета студента) (доступ из личного кабинета студента). (доступ из личного кабинета студента) .

7.5. Современные профессиональные базы данных и информационные справочные системы

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, Лаборатория

учебная аудитория для проведения занятий лабораторного типа
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 Киберпреступность как новая криминальная угроза	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
3 Киберпреступления и уголовное законодательство Российской Федерации	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий

4 Понятие преступлений в сфере цифровой информации и их система	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
5 Виды преступлений в сфере цифровой информации	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		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 **ориентирования**, 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 **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** 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 **системном** 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. По действующему российскому законодательству, такие деяния, подпадают под сферу действия различных нормативных актов:
   а) Уголовный кодекс РФ;
   б) Гражданский кодекс РФ;
   в) Концепция национальной безопасности;
   г) КОАП РФ
2. Какие деяния по действующему уголовному законодательству признаются преступными:
   а) Неправомерный доступ к компьютерной информации;
   б) Умышленное блокирование или уничтожение компьютерной информации;
   в) Создание, использование и распространение вредоносных программ для ЭВМ;
   г) Компьютерное мошенничество
3. Термин «Преступления в сфере экономики и высоких технологий» является относительно новым и дискуссионным для российской уголовно–правовой действительности, при этом дискуссии, идут в следующих направлениях:
   а) критерии отнесения общественно–опасных деяний к группе так называемых «компьютерных преступлений»;
   б) ставится под сомнение целесообразности использования термина «компьютерные преступления» с предложениями взамен – «информационные преступления», «Преступления в сфере экономики и высоких технологий» (как разновидность – преступления в сфере информации), «киберпреступления» и т.д.;
   в) как рассматривать современные высокие технологии, которые использовались при совершении преступления – как орудие совершения или как особый способ совершения преступления
   г) все варианты верны
4. Принято выделять два типа причинного комплекса преступлений в сфере экономики и высоких технологий:
   а) Причинный комплекс, не имеющий особенностей по сравнению с другими, «некомпьютерными» видами преступности. Отличие заключается только в том, что

преступники дополнительно используют компьютерные технологии.

б) Причинный комплекс который заключается в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений. связанных с появлением автоматизированных систем обработки информации.

в) Причинный комплекс связанный с повсеместным и всесторонним внедрением новых технологий, что привело к техническому оснащению отдельных преступников и организованных преступных групп.

г) Все варианты верны

5. Прогнозирование ситуации показывает, что в российских условиях рост преступлений в сфере экономики и высоких технологий, обусловлен следующими факторами:

а) рост числа ЭВМ, используемых в России и, как следствие этого, ростом числа их пользователей, увеличением объемов информации, хранимой в ЭВМ;

б) недостаточностью защиты программного обеспечения; непродуманной кадровой политикой в вопросах приема на работу и увольнения;

в) отсутствием законодательной базы.

г) все варианты верны

6. Какие из ниже перечисленных нормативных актов относятся к международному законодательству в области борьбы с правонарушениями и преступлениями в сфере высоких технологий:

а) Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г.

б) «Конвенция о киберпреступности» принятая Советом Европы 9 ноября 2001 г. в Страсбурге.

в) Кодификатор международной уголовной полиции генерального секретариата Интерпола.

г) Все варианты верны

7. Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, к факультативному перечню преступлений относит:

а) Неправомерное изменение компьютерных данных или компьютерных программ;

б) Компьютерный шпионаж;

в) Несанкционированный перехват;

г) Несанкционированное использование компьютера.

8. Принятие Конвенции по борьбе с киберпреступностью позволило приблизить достижение следующих поставленных в ней целей:

а) согласование государствами–участниками национальных уголовно–правовых норм, связанных с преступлениями в киберпространстве;

б) разработка процедур процессуального законодательства, необходимых для расследования таких преступлений и судебного преследования лиц, их совершивших, а также сбора доказательств, находящихся в электронной форме;

в) обеспечение быстрого и эффективного режима международного сотрудничества в данной области.

г) все варианты верны

9. В соответствии со ст. 272 УК РФ уголовно наказуемым признается … доступ к охраняемой законом компьютерной информации:

а) преступный;

б) неправомерный;

в) злоумышленный;

г) неосторожный.

10. Классификация преступлений в сфере экономики и высоких технологий по кодификатору международной уголовной полиции генерального секретариата Интерпола, в соответствии с названным кодификатором все компьютерные преступления классифицированы следующим образом:

а) Несанкционированный доступ и перехват;

б) компьютерный абордаж (несанкционированный доступ);

в) Изменение компьютерных данных;

г) передача информации, подлежащая судебному рассмотрению.

9.1.2. Перечень вопросов для зачета с оценкой

Приведены примеры типовых заданий, составленных по пройденным разделам дисциплины.

1. Цифровая безопасность как элемент обеспечения национальной безопасности. Правовые методы обеспечения цифровой безопасности
2. Информационная и цифровая безопасность как объект уголовно-правовой охраны. Понятие, предмет и система информационной безопасности
3. Нормативно-правовые основы информационной безопасности в Российской Федерации. Международное сотрудничество в области защиты информации
4. Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления
5. Понятие преступлений в сфере цифровой информации. Киберпреступления в системе Особенной части УК РФ. Преступления в сфере компьютерной информации: характеристика составов
6. Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств. Незаконные организация и проведение азартных игр
7. Мошенничество с использованием электронных средств платежа. Мошенничество в сфере компьютерной информации
8. Организация деятельности по привлечению денежных средств и (или) иного имущества. Неправомерный оборот средств платежей
9. Понятие и виды преступлений в сфере цифровой экономики. Криминологическая характеристика преступности в сфере цифровой экономики
10. Типичные способы совершения киберпреступлений. Методы сокрытия авторства преступления в сети Интернет

9.1.3. Примерный перечень вариантов (заданий) контрольных работ

1. Принципы уголовного права.
2. Понятие состава преступления.
3. Обстоятельства, исключающие преступность деяния.
4. Формы соучастия.
5. Виды соучастия.
6. Виды наказаний.
7. Основания освобождения от уголовной ответственности.
8. Условно-досрочное освобождение.
9. Уголовная ответственность: понятие, виды, формы реализации
10. Действие уголовного закона во времени
11. Обратная сила уголовного закона
12. Действие уголовного закона в пространстве
13. Уголовно-правовая характеристика общественной опасности как признака преступления
14. Институт рецидива преступлений
15. Уголовно-правовая характеристика бездействия как признака объективной стороны преступления
16. Неоконченное преступление: понятие, виды, уголовно-правовое значение
17. Квалификация неоконченного преступления
18. Добровольный отказ в Российском уголовном законодательстве
19. Ответственность соучастников в преступлении по уголовному законодательству России
20. Понятие, виды и уголовно-правовая оценка прикосновенности к преступлению.
21. Условия правомерности необходимой обороны: теоретический анализ и судебная практика
22. Понятие и виды обстоятельств исключающих преступность деяния
23. Условия освобождения лица от уголовной ответственности в связи с деятельным раскаянием и примирением с потерпевшим
24. Общая характеристика преступлений против здоровья.
25. Общая характеристика преступлений против половой свободы и половой неприкосновенности личности.
26. Общая характеристика преступлений против основных конституционных прав человека и гражданина.

27. Общая характеристика преступлений против семьи и несовершеннолетних.
28. Общая характеристика преступлений против собственности.
29. Общая характеристика преступлений в сфере экономической деятельности.
30. Общая характеристика коррупционных преступлений.

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.

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 ГПДиПД
протокол № 5 от «27» 1 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ИГПиПОИД	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14-b705-b5087cef9b02
Заведующий обеспечивающей каф. ГПДиПД	Д.В. Хаминов	Согласовано, a0493917-6204-454c-b7e1-57e73022ff30
Начальник учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

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. Звегинцева	Согласовано, 7de46f77-2f66-455c-96f1-56c003651096

РАЗРАБОТАНО:

Профессор кафедры уголовного права, каф. УП	А.В. Шеслер	Разработано, be0c399a-c604-4567-b129-6c042b0b8d90
Доцент кафедры уголовного права, каф. УП	Н.В. Ахмедшина	Разработано, 379c592b-8c3e-42a0-9e8e-f1e9c522694c
Доцент, каф. ГПДиПД	И.В. Чаднова	Разработано, 1b7465ef-94f1-4deb-a150-5983ee333540