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 УР

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: **очная**
Факультет: **Юридический факультет (ЮФ)**
Кафедра: **Кафедра информационного права (ИП)**
Курс: **2**
Семестр: **3**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	36	36	часов
Самостоятельная работа	126	126	часов
Общая трудоемкость (включая промежуточную аттестацию)	180	180	часов
	5	5	з.е.

Формы промежуточной аттестация	Семестр
Зачет с оценкой	3

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		

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 современные информационные технологии, используемые в уголовно-правовой сфере правоприменения и требования 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 в сфере уголовной ответственности за киберпреступления информационные технологии 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 (справочно-правовых систем, государственных информационных систем) для решения задач в сфере уголовной ответственности за киберпреступления с учетом требований информационной безопасности
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. Составляет правовые документы 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 нормативноправовых (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. Осуществляет 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 5 зачетных единиц, 180 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
Контактная аудиторная работа обучающихся с преподавателем, всего	54	54
Лекционные занятия	18	18
Практические занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	126	126
Подготовка к зачету с оценкой	30	30
Выполнение практического задания	36	36
Подготовка к тестированию	30	30
Подготовка к устному опросу / собеседованию	30	30
Общая трудоемкость (в часах)	180	180
Общая трудоемкость (в з.е.)	5	5

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	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
3 семестр					
1 Киберпреступность как новая криминальная угроза	3	6	21	30	ОПК-7, 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	3	6	21	30	ОПК-7, ПК-1, ПК-2, ПК-3
3 Киберпреступления и уголовное законодательство Российской Федерации	3	6	21	30	ОПК-7, ПК-1, ПК-2, ПК-3
4 Понятие преступлений в сфере цифровой информации и их система	3	6	21	30	ОПК-7, ПК-1, ПК-2, ПК-3
5 Виды преступлений в сфере цифровой информации	3	6	21	30	ОПК-7, ПК-1, ПК-2, ПК-3
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	3	6	21	30	ОПК-7, ПК-1, ПК-2, ПК-3
Итого за семестр	18	36	126	180	
Итого	18	36	126	180	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции

3 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.	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	
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	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	

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.	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	
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.	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	

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.).	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	

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.	3	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	3	
	Итого за семестр	18	
	Итого	18	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
3 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.	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	
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	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	

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.	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	
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.	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	

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.).	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	

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.	6	ОПК-7, ПК-1, ПК-2, ПК-3
	Итого	6	
	Итого за семестр	36	
	Итого	36	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

5.5. 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
3 семестр				
1 Киберпреступность как новая криминальная угроза	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		
3 Киберпреступления и уголовное законодательство Российской Федерации	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		
4 Понятие преступлений в сфере цифровой информации и их система	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		

5 Виды преступлений в сфере цифровой информации	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	Подготовка к зачету с оценкой	5	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой
	Выполнение практического задания	6	ОПК-7, ПК-1, ПК-2, ПК-3	Практическое задание
	Подготовка к тестированию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	5	ОПК-7, ПК-1, ПК-2, ПК-3	Устный опрос / собеседование
	Итого	21		
Итого за семестр		126		
Итого		126		

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.	Сам. раб.	
ОПК-7	+	+	+	Зачёт с оценкой, Устный опрос / собеседование, Практическое задание, Тестирование
ПК-1	+	+	+	Зачёт с оценкой, Устный опрос / собеседование, Практическое задание, Тестирование
ПК-2	+	+	+	Зачёт с оценкой, Устный опрос / собеседование, Практическое задание, Тестирование
ПК-3	+	+	+	Зачёт с оценкой, Устный опрос / собеседование, Практическое задание, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
3 семестр				
Зачёт с оценкой	5	10	15	30
Устный опрос / собеседование	5	10	10	25
Практическое задание	10	10	10	30
Тестирование	5	5	5	15
Итого максимум за период	25	35	40	100
Нарастающим итогом	25	60	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

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

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]. [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]. [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]. [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]. [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]. [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. [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. [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 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. 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. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций,

текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Учебная аудитория: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий семинарского типа, помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 303 ауд.

Описание имеющегося оборудования:

- Интерактивная панель;
- Камера;
- Микрофон;
- Тумба для докладчика;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. 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.

8.4. 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	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
2 Цифровая безопасность и цифровая информация как объекты правового и уголовно-правового регулирования. Понятие, предмет и система цифровой безопасности	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
3 Киберпреступления и уголовное законодательство Российской Федерации	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
4 Понятие преступлений в сфере цифровой информации и их система	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий

5 Виды преступлений в сфере цифровой информации	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
6 Преступления в сферах цифровой информации. Обзор основных видов и методов осуществления киберпреступлений	ОПК-7, ПК-1, ПК-2, ПК-3	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Практическое задание	Темы практических заданий
		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: Уголовный кодекс РФ; Гражданский кодекс РФ; Концепция национальной безопасности; КОАП РФ
2. Какие деяния по действующему уголовному законодательству признаются преступными: Неправомерный доступ к компьютерной информации; Умышленное блокирование или уничтожение компьютерной информации; Создание, использование и распространение вредоносных программ для ЭВМ; 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: критерии отнесения общественно–опасных деяний к группе так называемых «компьютерных преступлений»; 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.; как рассматривать современные высокие технологии, которые использовались при совершении преступления – как орудие совершения или как особый способ совершения преступления
4. Принято выделять два типа причинного комплекса преступлений в сфере экономики и высоких технологий: Причинный комплекс, не имеющий особенностей по сравнению с другими, «некомпьютерными» видами преступности. Отличие заключается только в том, что преступники дополнительно используют компьютерные технологии. В результате несколько изменяются условия преступной деятельности, ее формы, масштабы и последствия. Причинный комплекс который заключается в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений. связанных с появлением автоматизированных систем обработки информации. Причинный комплекс связанный с повсеместное и всестороннее внедрение новых технологий привело к техническому оснащению отдельных преступников и организованных преступных групп.
5. Прогнозирование ситуации показывает, что в российских условиях рост преступлений в сфере экономики и высоких технологий, обусловлен следующими факторами: рост числа ЭВМ, используемых в России и, как следствие этого, ростом числа их пользователей,

увеличением объемов информации, хранимой в ЭВМ; недостаточностью защиты программного обеспечения; непродуманной кадровой политикой в вопросах приема на работу и увольнения; отсутствием законодательной базы.

6. Какие из ниже перечисленных нормативных актов относятся к международному законодательству в области борьбы с правонарушениями и преступлениями в сфере высоких технологий: Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г. «Конвенция о киберпреступности» принятая Советом Европы 9 ноября 2001 г. в Страсбурге. Кодификатор международной уголовной полиции генерального секретариата Интерпола.
7. Рекомендация № R 89 (9) Комитета Министров стран–членов Совета Европы о преступлениях, связанных с компьютерами, к факультативному перечню преступлений относит. Неправомерное изменение компьютерных данных или компьютерных программ; Компьютерный шпионаж; Несанкционированный перехват; Несанкционированное использование компьютера.
8. Принятие Конвенции по борьбе с киберпреступностью позволило приблизить достижение следующих поставленных в ней целей: согласование государствами–участниками национальных уголовно–правовых норм, связанных с преступлениями в киберпространстве; разработка процедур процессуального законодательства, необходимых для расследования таких преступлений и судебного преследования лиц, их совершивших, а также сбора доказательств, находящихся в электронной форме; обеспечение быстрого и эффективного режима международного сотрудничества в данной области.
9. В соответствии со ст. 272 УК РФ уголовно наказуемым признается … доступ к охраняемой законом компьютерной информации: преступный; неправомерный; злоумышленный; 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: Несанкционированный доступ и перехват; компьютерный абордаж (несанкционированный доступ); Изменение компьютерных данных; передача информации, подлежащая судебному рассмотрению.

9.1.2. Перечень вопросов для зачета с оценкой

1. Понятие и виды информации
2. Основные нормативно-правовые источники обеспечения цифровой безопасности
3. Цифровая безопасность как элемент обеспечения национальной безопасности
4. Правовые методы обеспечения цифровой безопасности
5. Международно-правовое регулирование цифровой безопасности
6. Информационная и цифровая безопасность как объект уголовно-правовой охраны
7. Понятие, предмет и система информационной безопасности
8. Нормативно-правовые основы информационной безопасности в Российской Федерации
9. Международное сотрудничество в области защиты информации
10. Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления
11. Понятие преступлений в сфере цифровой информации
12. Киберпреступления в системе Особенной части УК РФ
13. Преступления в сфере компьютерной информации: характеристика составов
14. Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств
15. Мошенничество с использованием электронных средств платежа
16. Мошенничество в сфере компьютерной информации
17. Незаконные организация и проведение азартных игр
18. Организация деятельности по привлечению денежных средств и (или) иного имущества
19. Неправомерный оборот средств платежей
20. Понятие и виды преступлений в сфере цифровой экономики
21. Понятие и виды преступлений в сфере цифровой информации

22. Криминологическая характеристика преступности в сфере цифровой экономики
23. Типичные способы совершения киберпреступлений
24. Методы сокрытия авторства преступления в сети Интернет
25. Понятие доказательств в цифровом виде. Источники сбора доказательств в цифровом виде
26. Методы компьютерно-технических экспертиз, их правовые основы

9.1.3. Примерный перечень вопросов для устного опроса / собеседования

1. Перечислите основные аспекты обеспечения информационной безопасности и дайте их определения.
2. Какие вам известны подходы к классификации угроз безопасности информации?
3. Приведите примеры угроз, которые являются нарушением целостности и доступности.
4. Какой подход к оценке и управлению рисками информационной безопасности используется в современных организациях?
5. Перечислите основные нормативные акты в области защиты государственной и коммерческой тайн РФ.
6. Является ли целесообразным международное сотрудничество в области информационной безопасности и почему?
7. В какой степени разработка кибероружия в государственных масштабах является приемлемым действием?

9.1.4. Темы практических заданий

1. Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы. Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?
2. Аспирант университета Хохлов занимался исследовательской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые черви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации. Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?
3. Студент технического вуза Иванченко во время занятий по информатике подключился к сети "Интернет" и регулярно получал в течение семестра материалы разного содержания, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в "Интернет" и пришел чек на оплату 105 часов пребывания в сети "Интернет". Руководство института поставило вопрос о привлечении Иванченко к уголовной и гражданской ответственности. Дайте правовую оценку действиям студента Иванченко.
4. Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов Ситибанка. Рассылка представляла собой электронное письмо с сообщением опереводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-баккинга CitibankOnline для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран CitibankOnline. Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в

Ситибанке, в сумме 15 и 20 тысяч долларов соответственно. Квалифицируйте содеянное Савченко.

5. ГУВД Московской области было возбуждено уголовное дело по факту совершение неправомерного доступа в охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г. Павловский Посад Лебедева. Следствие квалифицировало действие Лебедева по ч. 2 ст. 272 УК РФ, т.е. изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации. Дайте юридическую оценку содеянного. Что следует понимать под компьютерной информацией?

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 / электронном журнале 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 9.2.

Таблица 9.2 – 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 УП
протокол № 6 от «22» 1 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ИП	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14-b705-b5087cef9b02
Заведующий обеспечивающей каф. УП	И.В. Чаднова	Согласовано, 1b7465ef-94f1-4deb-a150-5983ee333540
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Заведующий кафедрой, каф. ИП	В.Г. Мельникова	Согласовано, 72b97820-0b02-4f14-b705-b5087cef9b02
Заведующий кафедрой, каф. ТП	Д.В. Хаминов	Согласовано, a0493917-6204-454c-b7e1-57e73022ff30

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