Компонент ОПОП **40.03.01 Юриспруденция**

Правоохранительная и правоприменительная деятельность

наименование ОПОП

К.М.03.ДВ.02.02

шифр дисциплины

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплины (модуля) **Правовое регулирование информационной безопасности**

Разработчик(и):
Панкратова М.Е.
ФИО

доцент
Должность

канд. юрид. наук, доцент
ученая степень, звание

Утверждено на заседании кафедры
Теории и истории государства и права
наименование кафедры

протокол № 6 от 04.02.2026 г.
заведующая кафедрой Теории и истории государства и права


Лобченко Л.Н.

1. Критерии и средства оценивания компетенций и индикаторов их достижения, формируемых дисциплиной (модулем)

Код и наименование компетенции	Код и наименование индикатора(ов) достижения компетенции	Результаты обучения по дисциплине (модулю)			Оценочные средства текущего контроля	Оценочные средства промежуточной аттестации
		Знать	*Уметь*	*Владеть*		
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**1.1.** Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи **1.2.** Использует системный подход для решения поставленных задач, предлагает способы их решения	нормативные основы и особенности правотворческого процесса в РФ теоретические вопросы законотворчества, правоприменения и коллизионности нормативно-правовые акты отраслей материального и процессуального права, критерии уровней правосознания и правовой культуры нормативно-правовые акты отраслей материального и процессуального права, критерии уровней правосознания и правовой культуры	осуществлять профессиональную деятельность на основе развитого правосознания и правовой культуры выявлять взаимосвязь требований законодательства и правоприменительной практики определять соответствующие нормы права, позволяющие принять юридически правильное решение обеспечивать соблюдение законодательства субъектами права при разработке нормативно-правовых актов	навыками подготовки проектов нормативно-правовых актов и иных юридических документов навыками разрешения проблем и коллизий в процессе правоприменения навыками совершения юридических действий в точном соответствии с законодательством навыками сочетания профессионализма и должного уровня правосознания и правовой культуры	- комплект заданий для выполнения практических работ; - тестовые задания, доклад, реферат, презентация, дискуссии	Вопросы для зачета
ПК-2 Способен оценивать состояние законодательства, и вносить предложения по соблюдению и защите права и свободы человека и гражданина	**2.1** Определяет права и свободы человека как высшую ценность, основываясь на Конституции РФ и законодательстве	Конституционные права и гарантии человека и гражданина	определять права и свободы человека как высшую ценность	навыками оценки конституционного законодательства относительно прав и свобод	- комплект заданий для выполнения практических работ; - тестовые задания, доклад, реферат, презентация, дискуссии	Вопросы для зачета
	2.2. Осуществляет профессиональную деятельность на основе уважения чести и достоинства личности, соблюдения прав и свобод человека и гражданина	Конституционные права и гарантии человека и гражданина, сущность их высшей ценности	осуществлять профессиональную деятельность на основе уважения чести и достоинства личности	нормативными и иными навыками соблюдения прав и свобод человека и гражданина		
	2.3 Обеспечивает различными способами защиту прав и свобод человека и гражданина в процессе своей	Конституционные права и гарантии человека и гражданина, сущность их высшей ценности	обеспечивать различными способами защиту прав и свобод человека и гражданина	навыками защиты прав и свобод человека и гражданина в процессе своей профессиональной		

	профессиональной деятельности			деятельности		
	2.4. Вносит предложения по совершенствованию нормативных правовых актов, принимает участие во внесении изменений и дополнений в нормативные правовые акты	теоретические вопросы нормотворчества, его процедурных особенностей и юридическую технику	определять наиболее важные направления в нормотворчестве и вносить предложения по совершенствованию нормативных правовых актов	навыками внесении изменений и дополнений в нормативные правовые акты		
ПК-4 Способен юридически правильно квалифицировать факты и обстоятельства	**4.1.** Определяет основания возникновения, изменения и прекращения правоотношений в рамках конкретных обстоятельств	современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности;	пользоваться правовой информацией, анализировать ее с точки зрения поставленных задач;	навыками оказания юридической помощи, консультирование по частноправовым вопросам, в том числе по защите прав граждан и юридических лиц;	- комплект заданий для выполнения практических работ; - тестовые задания, доклад, реферат, презентация, дискуссии	Вопросы для зачета
	4.2. Выявляет и анализирует факты, имеющие юридическое значение	основные этапы законодательного процесса и оформления их результатов;	ориентироваться в системе законодательства и нормативно-правовых актов общефедерального и регионального уровня;	навыками защиты прав и законных интересов граждан, юридических лиц, государственных и муниципальных образований;		
	4.3. Дает правильную и обоснованную квалификацию юридическим фактам и обстоятельствам	*Знать:* порядок формирования, полномочия и основные формы работы общественных советов при федеральных и региональных органах государственной власти;	использовать нормативно-правовую документацию в сфере профессиональной деятельности;	профессиональными навыками по обеспечению конституционных прав человека;		
	4.4. Правильно определяет юридические последствия квалифицируемых обстоятельств	основные задачи по организации работы по обеспечению законности и правопорядка, безопасности личности, общества, государства;	изучать развитие законодательства, регламентирующего формы взаимодействия государства и гражданского общества;	навыками осуществления правовой экспертизы нормативных правовых актов в целях юридически правильной квалификации фактов и обстоятельств, прежде всего, с точки		

				зрения обеспечения соответствии действий и решений органов публичной власти Конституции и законодательству, а также - соблюдения основных прав и свобод человека и гражданина.		

2. Оценка уровня сформированности компетенций (индикаторов их достижения)

Показатели оценивания компетенций (индикаторов их достижения)	**Шкала и критерии оценки уровня сформированности компетенций (индикаторов их достижения)**			
	Ниже порогового *(«неудовлетворительно»)*	**Пороговый** *(«удовлетворительно»)*	**Продвинутый** *(«хорошо»)*	**Высокий** *(«отлично»)*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки.
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенции фактически не сформированы. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач.	Сформированность компетенций соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков достаточно для решения стандартных профессиональных	Сформированность компетенций полностью соответствует требованиям. Имеющихся знаний, умений, навыков в полной мере достаточно для решения сложных, в том числе нестандартных, профессиональных задач.

	ИЛИ Зачетное количество баллов не набрано согласно установленному диапазону	(профессиональных) задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	ИЛИ Набрано зачетное количество баллов согласно установленному диапазону

3. Критерии и шкала оценивания заданий текущего контроля

3.1 Критерии и шкала оценивания практических работ

Перечень практических работ, описание порядка выполнения и защиты работы, требования к результатам работы, структуре и содержанию отчета и т.п. представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

Оценка/баллы	Критерии оценивания
Отлично /91-100	Задание выполнено полностью и правильно. Отчет по практической работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
Хорошо /81-90	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений. Все требования, предъявляемые к работе, выполнены.
Удовлетворительно 61-80	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную/практическую работу. Большинство требований, предъявляемых к заданию, выполнены.
Неудовлетворительно /до 60	Задание выполнено со значительным количеством ошибок на низком уровне. Многие требования, предъявляемые к заданию, не выполнены. ИЛИ Задание не выполнено.

3.2 Критерии и шкала оценивания тестирования

Перечень тестовых вопросов и заданий, описание процедуры тестирования представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

В ФОС включен типовой вариант тестового задания:

Типовое тестовое задание:

Тест № 1

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись

- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Тест 2		
К негативным последствиям развития современных информационных и коммуникационных технологий можно отнести:		
	А)	формирование единого информационного пространства
	Б)	работа с информацией становится главным содержанием профессиональной деятельности
	В)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
	Г)	широкое использование информационных технологий во всех сферах человеческой деятельности
	Д)	доступность личной информации для общества и государства, вторжение информационных технологий в частную жизнь людей
2.	Термин «информатизация общества» обозначает:	
	А)	целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий
	Б)	увеличение избыточной информации, циркулирующей в обществе
	В)	увеличение роли средств массовой информации
	Г)	введение изучения информатики во все учебные заведения страны
	Д)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
3.	Развитый рынок информационных продуктов и услуг, изменение в структуре экономики, массовое использование информационных и коммуникационных технологий являются признаками:	
	А)	информационной культуры
	Б)	высшей степени развития цивилизации
	В)	информационного кризиса
	Г)	информационного общества
	Д)	информационной зависимости
4.	Методы обеспечения информационной безопасности делятся (указать неправильные ответ):	
	А)	правовые
	Б)	организационно-технические
	В)	политические
	Г)	экономические
	Д)	все перечисленные выше
5.	Обеспечение защиты информации проводится конструкторами и разработчиками программного обеспечения в следующих направлениях (указать неправильный ответ):	
	А)	защита от сбоев работы оборудования
	Б)	защита от случайной потери информации
	В)	защита от преднамеренного искажения
	Г)	разработка правовой базы для борьбы с преступлениями в сфере информационных технологий
	Д)	защита от несанкционированного доступа к информации
6.	Компьютерные вирусы – это:	
	А)	вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера
	Б)	программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК
	В)	программы, являющиеся следствием ошибок в операционной системе
	Г)	пункты А) и В)
	Д)	вирусы, сходные по природе с биологическими вирусами
7.	Отличительными особенностями компьютерного вируса являются:	
	А)	значительный объем программного кода

	Б)	способность к самостоятельному запуску и многократному копированию кода
	В)	способность к созданию помех корректной работе компьютера
	Г)	легкость распознавания
	Д)	Пункты Б) и В)
8.	Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?	
	А)	Уголовный кодекс РФ
	Б)	Гражданский кодекс РФ
	В)	Доктрина информационной безопасности РФ
	Г)	Постановления Правительства
	Д)	Указ Президента РФ
9.	Что не относится к объектам информационной безопасности Российской Федерации?	
	А)	природные и энергетические ресурсы
	Б)	информационные ресурсы всех видов
	В)	информационные системы различного класса и назначения, информационные технологии
	Г)	система формирования общественного сознания
	Д)	права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности
10.	Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?	
	А)	Неправомерный доступ к компьютерной информации
	Б)	Создание, использование и распространение вредоносных программ для ЭВМ
	В)	Умышленное нарушение правил эксплуатации ЭВМ и их сетей
	Г)	Все перечисленное выше
	Д)	Пункты Б) и В)
11.	Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?	
	А)	Доктрина информационной безопасности РФ
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Указ Президента РФ
	Д)	Закон «Об информации, информатизации и защите информации»
12.	Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?	
	А)	Закон «Об информации, информатизации и защите информации»
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Пункты А) и В)
	Д)	Указ Президента РФ
13.	Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:	
	А)	Указ Президента РФ
	Б)	Закон «Об информации, информатизации и защите информации»
	В)	Закон «О правовой охране программ для ЭВМ и баз данных»
	Г)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Д)	Доктрина национальной безопасности РФ
14.	Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?	
	А)	да, нарушено авторское право владельца сайта
	Б)	нет, так как нормативно-правовые акты не являются объектом авторского права

	В)	нет, если есть разрешение владельца сайта
	Г)	да, нарушено авторское право автора документа
	Д)	нет, если истек срок действия авторского права
15.	Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?	
	А)	можно, с указанием имени автора и источника заимствования
	Б)	можно, с разрешения и автора статьи, и издателя
	В)	можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения
	Г)	можно, поскольку опубликованные статьи не охраняются авторским правом
	Д)	можно, с разрешения издателя, издавшего данную статью, или автора статьи
16.	Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?	
	А)	имя автора, название статьи, адрес сайта, с которого заимствована статья
	Б)	адрес сайта и имя его владельца
	В)	имя автора и название статьи
	Г)	электронный адрес сайта, с которого заимствована статья
	Д)	название статьи и название сайта
17.	Можно ли использовать статьи из разных журналов и газет на политические, экономические, религиозные или социальные темы для подготовки с их использованием учебного материала?	
	А)	нет
	Б)	да, получив согласие правообладателей
	В)	да, указав источники заимствования
	Г)	да, не спрашивая согласия правообладателей, но с обязательным указанием источника заимствования и имен авторов
	Д)	да, указав ФИО авторов и название статей
18.	Считается ли статья, обнародованная в Интернет, объектом авторского права?	
	А)	нет, если статья впервые обнародована в сети Интернет
	Б)	да, при условии, что эта же статья в течение 1 года будет опубликована в печати
	В)	да, так как любая статья является объектом авторского права как произведение науки или литературы
	Г)	да, если указан год первого опубликования
	Д)	да, если автор использует знак охраны авторского права
19.	В каких случаях при обмене своими компьютерными играми с другими людьми, не будут нарушаться авторские права?	
	А)	если экземпляры этих компьютерных игр были выпущены в свет и введены в гражданский оборот с согласия автора
	Б)	если обладатели обмениваемых экземпляров компьютерных игр приобрели их по договору купли-продажи/мены
	В)	если одновременно соблюдены условия, указанные в пунктах А) и Б)
	Г)	если они распространяются путем сдачи в прокат
	Д)	если автору выплачивается авторское вознаграждение
20.	В каких случаях правомерно используются фотографии из коллекции одного из Интернет-сайтов для иллюстрирования своего материала, подготавливаемого в образовательных целях?	
	А)	если тематика фото-сюжетов соответствует теме всего материала
	Б)	в любом случае, т.к. факт размещения фотографии в Интернет означает согласие автора на ее дальнейшее свободное использование
	В)	если такое использование прямо разрешено правилами Интернет-сайта
	Г)	если фотографии размещены на сайте Интернет с согласия их авторов
	Д)	Если соблюдаются условия В) и Г)

Ответы к тестовым заданиям

Вариант ответа									
А)		Б)		В)		Г)		Д)	
2	12	6	13	4	18	3	10	1	15
9	16	11	14	8	19	5	17	7	20

Оценка	Критерии оценки
Отлично	90-100 % правильных ответов
Хорошо	70-89 % правильных ответов
Удовлетворительно	50-69 % правильных ответов
Неудовлетворительно	49% и меньше правильных ответов

3.3 Критерии и шкала оценивания доклада /информационного сообщения

Тематика докладов, информационных сообщений по дисциплине (модулю), требования к структуре, содержанию и оформлению изложены в методических материалах по освоению дисциплины (модуля), представлены в электронном курсе в ЭИОС МАУ.

В ФОС включены примерные темы докладов/информационных сообщений:

Примерные темы докладов

1. Правовой режим информации с ограниченным доступом: понятие, виды и законодательное регулирование
2. Электронная подпись как юридически значимый институт: нормативная база и правовые последствия использования
3. Правовые аспекты защиты информации при работе в сети Интернет: обязанности операторов, ответственность за нарушения
4. Инженерно-техническая защита информации в правовом поле: требования нормативных документов и ответственность за несоблюдение
5. Информационные войны и информационное оружие: международно-правовое регулирование и национальное законодательство
6. Кибертерроризм как объект уголовно-правового противодействия: составы преступлений и проблемы квалификации
7. Несанкционированный доступ к информации: уголовно-правовая и административная ответственность
8. Модель нарушителя информационной безопасности в правовой оценке: значение для доказывания и расследования
9. Правовые меры профилактики преступлений в сфере высоких технологий: система субъектов и инструментов
10. Понятие и виды защищаемой информации в российском законодательстве: конфиденциальная информация, персональные данные, служебная и коммерческая тайна
11. Правовая квалификация несанкционированного доступа к информации: проблемы разграничения составов
12. Утечка информации как правовая категория: основания ответственности и меры предупреждения
13. Угрозы информации в юридическом измерении: понятие, классификация и правовые механизмы минимизации
14. Документированная информация как объект правовой защиты: требования к обращению и юридическая сила
15. Информационные ресурсы как объекты права: правовой режим, собственность и оборотоспособность

16. Электронная почта в правовом поле: обязанности операторов связи, ответственность за спам и фишинг
17. Правовое регулирование методов и средств защиты компьютерной информации: требования к средствам защиты и их сертификация
18. Архивация файлов с правовой точки зрения: обеспечение доказательственного значения и целостности информации
19. Компьютерные вирусы как объект правового воздействия: составы преступлений (ст. 273 УК РФ) и судебная практика
20. Правовые основы защиты от компьютерных вирусов: обязанности организаций, стандарты и нормативные требования
21. Классификация антивирусных программных средств в системе правового регулирования: лицензирование, сертификация, требования ФСТЭК
22. Криптографические методы защиты информации в правовом аспекте: ограничения оборота, лицензирование и ответственность
23. Лицензирование и сертификация в области защиты информации: правовая природа, процедуры и юридические последствия
24. Правовая модель системы менеджмента информационной безопасности: соответствие законодательству и стандартам (ISO/IEC 27000, приказы ФСТЭК)
25. Деятельность Координационного центра в сфере информационной безопасности: правовые основы и региональная компетенция

Оценка/баллы	Критерии оценки
Отлично /91-100	Ориентированность в материале, полные и аргументированные ответы на дополнительные вопросы. Материал изложен логически последовательно, присутствуют самостоятельные выводы, используется материал из дополнительных источников, интернет ресурсов. Сообщение носит исследовательский характер. Используется наглядный материал (презентация).
Хорошо /81-90	Ориентированность в материале, но присутствуют некоторые затруднения в ответах на дополнительные вопросы. Отсутствует исследовательский компонент в сообщении. Отсутствует наглядный материал (презентация).
Удовлетворительно /61-80	Трудности в подборе материала, его структурировании. Использована, в основном, учебная литература, не использованы дополнительные источники информации. Трудности в ответе на дополнительные вопросы по теме сообщения, формулировке выводов. Материал изложен не последовательно, не установлены логические связи.
Неудовлетворительно /до 60	Доклад, информационное сообщение подготовлено по одному источнику информации либо не соответствует теме. ИЛИ Доклад, информационное сообщение не подготовлено.

3.4 Критерии и шкала оценивания кейс-задания

Рекомендации по выполнению кейс-заданий по дисциплине (модулю) изложены в методических материалах по освоению дисциплины (модуля), представлены в электронном курсе в ЭИОС МАУ.

В ФОС включено типовое кейс-задание:

1. Ситуационные задачи

Задача № 1. Нарушение режима защиты персональных данных в образовательной организации

В Мурманском арктическом университете (МАУ) на сайте деканата в открытом доступе был опубликован файл «Список_студентов_зачисление.xlsx», содержащий фамилии, имена, даты рождения, номера зачётных книжек, а также СНИЛС студентов заочной формы обучения. Файл был обнаружен случайно через поисковую систему и

скачан третьими лицами. По факту инцидента студенты обратились с жалобой в прокуратуру.

Вопросы:
1. Какие правовые нормы нарушены? Перечислите соответствующие статьи федеральных законов (укажите ФЗ «О персональных данных», возможные составы КоАП РФ и УК РФ).
2. Кто является оператором персональных данных и какие обязанности возложены на него законом?
3. Какие меры ответственности могут быть применены к должностным лицам МАУ?
4. Какие организационно-правовые и технические меры следует предпринять университету для предотвращения подобных ситуаций в будущем?

Задача № 2. Оспаривание электронной подписи в арбитражном суде

Между ООО «Арктика-Строй» (подрядчик) и ГБУ МО «Мурманскстройзаказчик» (заказчик) был заключён договор на выполнение работ по благоустройству общественной территории. Договор подписан усиленной квалифицированной электронной подписью (УКЭП) директора подрядчика. Впоследствии подрядчик отказался от выполнения работ, утверждая, что подпись была проставлена неуполномоченным лицом, поскольку электронная подпись директора хранилась в сейфе в свободном доступе. Заказчик обратился в суд с иском о взыскании неустойки.

Вопросы:
1. Какое правовое значение имеет УКЭП в соответствии с ФЗ «Об электронной подписи»?
2. Каков порядок использования электронной подписи юридическим лицом и распределение ответственности за её сохранность?
3. Оцените шансы сторон в судебном споре. Какие обстоятельства будут иметь решающее значение?
4. Разработайте рекомендации для организаций по защите ключей электронной подписи и разграничению полномочий.

Задача № 3. Несанкционированный доступ к корпоративной сети

Сотрудник коммерческой организации (ООО «Север-ИТ») — системный администратор, уволенный за нарушение трудовой дисциплины, используя ранее известные ему пароли, через два дня после увольнения подключился к корпоративной сети организации, скопировал базу данных клиентов и удалил часть рабочих файлов. Организация обратилась в правоохранительные органы.

Вопросы:
1. Квалифицируйте действия бывшего сотрудника по Уголовному кодексу РФ (укажите возможные статьи).
2. Какие доказательства необходимо собрать для возбуждения уголовного дела?
3. Какие меры организационного и технического характера должна была предпринять организация, чтобы минимизировать последствия увольнения?
4. Возможно ли привлечение организации к административной ответственности за нарушение законодательства о персональных данных (если база содержала персональные данные)?

Задача № 4. Распространение вредоносного ПО через фишинговую рассылку

В марте 2025 года в адрес сотрудников правительства Мурманской области поступила электронная рассылка от имени якобы Министерства цифрового развития РФ с темой «Срочная проверка учётных записей госслужащих». Во вложении содержался файл «Проверка_доступа.exe». После открытия файла на рабочих станциях произошло

шифрование документов. В результате часть документов была утрачена, а также скомпрометированы учётные записи нескольких сотрудников. По данному факту возбуждено уголовное дело.

Вопросы:

1. Какие составы преступлений усматриваются в действиях злоумышленников? (Укажите статьи УК РФ.)
2. Какие требования к обеспечению информационной безопасности установлены для государственных органов (укажите нормативные акты, включая приказы ФСТЭК, требования к защите информации в государственных информационных системах)?
3. Какие организационные меры необходимо принять в органах государственной власти для снижения рисков фишинговых атак?
4. Какие действия должны быть предприняты сразу после обнаружения инцидента (с точки зрения реагирования и юридического сопровождения)?

Оценка/баллы	Критерии оценки
Отлично /91-100	Выполнены соответствующие требования в полном объеме. Использованы системный и ситуативный подходы, представлено аргументированное рассуждение по проблеме, определены цели, задачи, причины возникновения ситуации, определены риски, трудности при разрешении проблемы, подготовлена программу действий.
Хорошо /81-90	Правильно определены цели, задачи, причины возникновения ситуации. Определены риски, трудности при разрешении проблемы. Подготовлена программа действий, но недостаточно четко и последовательно аргументировано решение ситуации.
Удовлетворительно 61-80	Представлены рассуждения по проблеме, определены цели, задачи, причины возникновения ситуации. Определены возможные связи проблемы с другими проблемами, частично представлена программа действий.
Неудовлетворительно /до 60	Представлены разрозненные аргументы по проблеме или аргументы отсутствуют. Отсутствуют цели, задач, результаты предстоящей деятельности. Программа действий содержит серьезные ошибки или отсутствует. ИЛИ Задание не выполнено.

3.5. Критерии и шкала оценивания мультимедийной презентации

Требования к структуре, содержанию и оформлению представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

В ФОС включена Примерная тематика презентаций

Примерная тематика презентаций

1. Система законодательства в сфере информационной безопасности и защиты информации
   2. Электронный документ: правовой режим, юридическая сила и требования к защите
2. Почтовая бомба как способ деструктивного воздействия: понятие, признаки и ответственность
3. Понятие и виды защищаемой информации по российскому законодательству

4. Несанкционированный доступ к информации: правовая квалификация и способы совершения
5. Утечка информации: каналы, причины и меры правового предупреждения
6. Угрозы информационной безопасности: понятие, классификация и правовые механизмы нейтрализации
7. Документированная информация как объект правовой защиты
8. Электронная подпись: правовое регулирование, виды и практика применения
9. Информационные ресурсы: правовой режим, оборотоспособность и защита
10. Электронная почта как объект угроз: спам, фишинг, вредоносные вложения и ответственность
11. Методы и средства защиты компьютерной информации: правовые требования и организационное обеспечение
12. Архивация файлов: правовое значение, принципы и правила обеспечения целостности информации
13. Компьютерные вирусы: классификация, правовая оценка и последствия воздействия
14. Основные методы защиты от компьютерных вирусов: организационно-правовые и технические меры
15. Классификация антивирусных программных средств: типы, функциональное назначение и требования к сертификации
16. Криптографическая защита файлов: правовые основы и общее назначение
17. Методы частотного криптоанализа: теоретические основы и практическое применение
18. Ключ шифрования: виды, способы ввода и правовой режим обращения
19. Компьютерные преступления: понятие, виды и уголовно-правовая характеристика
20. Криминалистическая характеристика преступлений в сфере компьютерной информации
21. Типичные орудия подготовки, совершения и сокрытия компьютерных преступлений
22. Способы совершения компьютерных преступлений: классификация и криминалистическое значение
23. Перехват информации: способы, правовая квалификация и меры противодействия
24. Несанкционированный доступ к средствам компьютерной техники: технические и правовые аспекты
25. Манипуляция данными и управляющими командами как способ совершения компьютерного преступления
26. Моделирование как способ совершения компьютерного преступления: понятие и методы выявления
27. Преодоление программных средств защиты: способы и правовые последствия
28. Тактика назначения и проведения судебных экспертиз при расследовании преступлений в сфере компьютерной информации
29. Особенности осмотра машинных носителей информации в ходе следственных действий
30. Особенности осмотра компьютерной техники: процессуальные и криминалистические аспекты
31. Тактика обыска и выемки компьютерной техники: правила поведения следователя и фиксация результатов

Оценка/баллы	**Критерии оценки**
Отлично /91-100	Презентация соответствует теме самостоятельной работы. Оформлен титульный слайд с заголовком. Сформулированная тема ясно изложена и структурирована, использованы графические изображения (фотографии,

	картинки и т.п.), соответствующие теме, выдержан стиль, цветовая гамма, использована анимация, звук. Логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению. Работа оформлена и предоставлена в установленный срок.
Хорошо /81-90	Презентация соответствует теме самостоятельной работы. Имеются неточности в изложении материала. Отсутствует логическая последовательность в суждениях. Не выдержан объем презентации, имеются упущения в оформлении. На дополнительные вопросы при защите даны неполные ответы. Работа оформлена и предоставлена в установленный срок.
Удовлетворительно 61-80	Презентация соответствует теме самостоятельной работы. Сформулированная тема изложена и структурирована не в полном объеме. Не использованы графические изображения (фотографии, картинки и т.п.), соответствующие теме. Присутствуют существенные отступления от требований к составлению презентации. Допущены фактические ошибки в содержании или при ответе на дополнительные вопросы.
Неудовлетворительно /до 60	Работа не выполнена или не соответствует теме самостоятельной работы.

3.6 Критерии и шкала оценивания посещаемости занятий

Посещение занятий обучающимися определяется в процентном соотношении

Баллы	Критерии оценки
10	посещаемость 75 - 100 %
5	посещаемость 50 - 74 %
0	посещаемость менее 50 %

3.7. Критерии и шкала оценивания результатов освоения дисциплины (модуля) с экзаменом

Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине (модулю), то он считается аттестованным.

В ФОС включен список вопросов и заданий к экзамену

Вопросы к зачёту

1. Комплексный подход к обеспечению информационной безопасности: сущность и составляющие.
2. Основные понятия защиты информации: объект защиты, уязвимость, угроза, способ защиты.
3. Угрозы информационной безопасности и каналы утечки информации: классификация и механизмы реализации.
4. Организационно-правовое обеспечение информационной безопасности: система нормативных правовых актов и структура органов власти.
5. Классификация автоматизированных систем и требования по защите информации: руководящий документ Гостехкомиссии России и характеристика девяти классов защищённости.
6. ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (Common Criteria): структура и назначение.

7. Профиль защиты, функциональные требования и требования доверия в системе оценки безопасности информационных технологий.
8. Каталог функций безопасности объекта: содержание и практическое применение.
9. Предположения безопасности и сокращение избыточных требований при разработке защищённых систем.
10. Политика информационной безопасности: понятие, ролевое управление и реализация в организациях.
11. Аппаратные и программные методы защиты данных: классификация и особенности применения.
12. Типы несанкционированного доступа к компьютерным системам и условия эффективного функционирования средств защиты.
13. Защита от локального несанкционированного доступа: механизмы и организационные меры.
14. Защита от удалённого несанкционированного доступа: средства и методы.
15. Защита от несанкционированного доступа к информации в коммутируемых каналах связи.
16. Методы восстановления информации после сбоев, разрушений и несанкционированных воздействий.
17. Разрушающие программные воздействия: обобщённая классификация и характеристика.
18. Модели взаимодействия прикладной программы и программной закладки: принципы функционирования.
19. Методы перехвата и навязывания информации: технические и организационные аспекты.
20. Классификация и методы внедрения программных закладок.
21. Компьютерные вирусы как особый класс разрушающих программных воздействий: классификация, жизненный цикл, последствия.
22. Защита от разрушающих программных воздействий: изолированная программная среда, виртуализация, контроль целостности.
23. Проблема защиты алгоритма при проектировании и реализации системы защиты информации.
24. Способы встраивания защитных механизмов в программное обеспечение.
25. Симметричные и асимметричные криптосистемы: принципы построения, сравнительная характеристика.
26. Способы создания симметричных криптосистем. Абсолютно стойкий шифр: понятие и условия реализации.
27. Криптографическая система DES и её модификации: структура, режимы работы, уязвимости.
28. Алгоритм криптографического преобразования по ГОСТ 28147-89: структура, основные элементы, область применения.
29. Принципы построения асимметричных криптографических систем: математическая основа, примеры реализации.
30. Электронная подпись: назначение, правовое регулирование, порядок использования.
31. Хеширование как механизм обеспечения целостности информации. ГОСТ Р 34.11-2012 (замена ГОСТ Р 34.11-94): характеристика алгоритма.
32. Современные алгоритмы электронной подписи. ГОСТ Р 34.10-2012 (замена ГОСТ Р 34.10-94): основные параметры и область применения.
33. Проблема подмены открытого ключа: угрозы и способы защиты (инфраструктура открытых ключей, сертификаты).
34. Комплексный метод защиты информации: сочетание организационных, правовых, технических и криптографических мер.
35. Методы защиты межсетевого обмена данными: межсетевые экраны, прокси-серверы,

VPN, DMZ.
36. Аппаратные шифраторы: структура, техническая реализация, области применения.
37. Программный продукт PGP (Pretty Good Privacy): архитектура, функции, применение для защиты электронной почты и файлов.
38. Взаимодействие межсетевых экранов (брандмауэров) и систем обнаружения вторжений (IDS/IPS): принципы совместной работы.
39. Государственная политика Российской Федерации в области информационной безопасности: нормативные
ы, стратегические документы.
40. Структура Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и её место в обеспечении информационной безопасности Российской Федерации.

Оценка	Баллы	Критерии оценивания
Зачтено	60 - 100	Набрано зачетное количество баллов согласно установленному диапазону
Не зачтено	менее 60	Зачетное количество согласно установленному диапазону баллов не набрано

4. Критерии и шкала оценивания результатов обучения по дисциплине (модулю) при проведении промежуточной аттестации

Критерии и шкала оценивания результатов освоения дисциплины (модуля) с зачетом

Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине (модулю), то он считается аттестованным с оценкой согласно шкале баллов для определения итоговой оценки:

Оценка	Баллы	Критерии оценивания
Отлично	91 - 100	Набрано зачетное количество баллов согласно установленному диапазону
Хорошо	81 - 90	Набрано зачетное количество баллов согласно установленному диапазону
Удовлетворительно	60 - 80	Набрано зачетное количество баллов согласно установленному диапазону
Неудовлетворительно	менее 60	Зачетное количество согласно установленному диапазону баллов не набрано

5. Задания диагностической работы для оценки результатов обучения по дисциплине (модулю) в рамках внутренней независимой оценки качества образования

ФОС содержит задания для оценивания знаний, умений и навыков, демонстрирующих уровень сформированности компетенций и индикаторов их достижения в процессе освоения дисциплины (модуля).

Комплект заданий разработан таким образом, чтобы осуществить процедуру оценки каждой компетенции, формируемых дисциплиной (модулем), у обучающегося в письменной форме.

Содержание комплекта заданий включает: *тестовые вопросы*, *ситуационные и практико-ориентированные задания*.

Комплект заданий диагностической работы

<table>
<tr><td colspan="3">УК-1
Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач</td></tr>
<tr><td>1</td><td colspan="2">Вставьте пропущенные слова: определение компетенции по формуле "вправе" - _____ возможности совершения государственными органами, органами местного самоуправления или организациями (их должностными лицами) действий в отношении граждан и организаций.
диспозитивное установление;
альтернативное установление;
безальтернативное установление.</td></tr>
<tr><td>2</td><td colspan="2">Укажите правильный ответ:
Антикоррупционная экспертиза законопроекта осуществляется:
его разработчиком;
органами местного самоуправления;
Верховным судом РФ;
нет правильного ответа</td></tr>
<tr><td>3</td><td colspan="2">Укажите факторы, характеризующие действие нормативно-правового акта во времени:
- момент обретения юридической силы;
- момент утраты юридической силы;
- круг лиц, на которых распространяет свое действие нормативно-правовой акт;
- территория государства.</td></tr>
<tr><td>4</td><td colspan="2">Соотнесите понятия и определения:</td></tr>
<tr><td></td><td>А.Отсутствие или неопределенность сроков, условий или оснований принятия решения, наличие дублирующих полномочий государственного органа, органа местного самоуправления или организации (их должностных лиц)
Б. возможность необоснованного установления исключений из общего порядка для граждан и организаций по усмотрению государственных органов, органов местного самоуправления или организаций (их должностных лиц)
В. отсутствие порядка совершения государственными органами, органами местного самоуправления или организациями (их должностными лицами) определенных действий либо одного из элементов такого порядка</td><td>1.широта дискреционных полномочий
2.выборочное изменение объема прав
3.отсутствие или неполнота административных процедур</td></tr>
<tr><td colspan="3">ПК-2
Способен оценивать состояние законодательства, и вносить предложения по соблюдению и защите права и свободы человека и гражданина</td></tr>
<tr><td>1</td><td colspan="2">Выберите правильный ответ:
Закон, устанавливающий или отягчающий ответственность за коррупционные</td></tr>
</table>

	правонарушения: 1. обратной силы не имеет; 2. может распространяться на правоотношения, возникшие ранее его вступления в силу, если это прямо указано в тексте закона; 3. применяется с обратной силой по усмотрению суда.
2	**Выберите правильный ответ:** Президент РФ: 1.обеспечивает принятие федеральных законов о противодействии коррупции; 2. определяет основные направления государственной политики в области противодействия коррупции 3. координируют деятельность органов внутренних дел Российской Федерации, органов федеральной службы безопасности, таможенных органов Российской Федерации и других правоохранительных органов по борьбе с коррупцией
3	**Запишите слово, пропущенное в схеме.**  **ответ…**
4	**Вставьте пропущенные термины.** Основными направлениями деятельности государственных органов по повышению эффективности …… коррупции являются проведение единой …….. политики в области противодействия …….., создание механизма взаимодействия …….. и государственных органов с ……. и парламентскими комиссиями по вопросам противодействия коррупции, а также с гражданами и институтами …….. общества, принятие ……., административных и иных мер, направленных на привлечение государственных и муниципальных служащих, а также граждан к более …….. в противодействии коррупции, на формирование в обществе негативного отношения к коррупционному поведению; Термины: А-законодательных, Б- государственной, В- коррупции, Г- активному участию, Д- гражданского, Е- противодействия, Ж- правоохранительных, З- общественными. ответ…
ПК-4 Способен юридически правильно квалифицировать факты и обстоятельства	
1	**Выберите правильный ответ:** Юридико-лингвистическая неопределенность - употребление неустоявшихся, двусмысленных терминов и категорий оценочного характера является: 1. Способом изложения нормативного материала 2. Коррупциогенным фактором **3.** Юридической коллизией.
2	**Выберите правильный ответ:** Антикоррупционная экспертиза нормативных правовых актов осуществляется: 1. при рассмотрении проекта и уже на стадии правоприменения; 2. только при рассмотрении проекта; 3. только на стадии правоприменения;

	4. не реже одного раза в три года после принятия акта.
4	**Вставьте пропущенные термины.** _____ это положения нормативных правовых актов (проектов нормативных правовых актов), устанавливающие для правоприменителя необоснованно широкие пределы усмотрения или возможность необоснованного применения исключений из общих правил, а также положения, содержащие неопределенные, трудновыполнимые и (или) обременительные требования к гражданам и организациям и тем самым создающие условия для проявления коррупции.
10	**Вставьте пропущенный термин:** _____ - наличие бланкетных и отсылочных норм, приводящее к принятию подзаконных актов, вторгающихся в компетенцию государственного органа, органа местного самоуправления или организации, принявшего первоначальный нормативный правовой акт.
ПК-5 Способен квалифицированно проводить научное исследование в области права	
1	**Дайте обоснованный ответ на вопрос:** В Министерство юстиции РФ поступил проект поправок Правительства РФ, которые планируется внести в Государственную Думу при рассмотрении во втором чтении проекта федерального закона. Нужно ли проводить антикоррупционную экспертизу таких поправок?
2	**Выберите правильный ответ:** К мерам по профилактике коррупции относятся (укажите все верные): 1. антикоррупционная экспертиза правовых актов и их проектов 2. формирование в обществе нетерпимости к коррупционному поведению; 3. развитие институтов общественного и парламентского контроля за соблюдением законодательства Российской Федерации о противодействии коррупции; 4. все вышеперечисленное.
3	**Укажите все правильные ответы:** К типичным противоречиям правовых актов Конституции Российской Федерации и федеральному законодательству можно отнести: 1.принятие органами государственной власти субъектов Российской Федерации правовых актов по вопросам, отнесенным к компетенции органов местного самоуправления; 2. неправильный выбор федерального закона, являющегося основанием для принятия правового акта; 3. наделение органов местного самоуправления отдельными государственными полномочиями.