Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Организационное и правовое обеспечение информационной безопасности

Специальность
10.05.03 Информационная безопасность автоматизированных систем

специализация №4 «Безопасность автоматизированных систем критически важных объектов»

Присваиваемая квалификация (степень)
специалист по защите информации

Форма обучения
очная

Год набора 2025

Челябинск 2025 г.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем специализация
специализация N 4 Безопасность автоматизированных систем критически важных объектов
Дисциплина: Организационное и правовое обеспечение информационной безопасности
Семестр (семестры) изучения: 8 семестр
Форма (формы) промежуточной аттестации: зачет

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «теория государства и права» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Перечень планируемых результатов обучения по дисциплине
1	2	3
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	**УК-2.1 Знать:** этапы жизненного цикла проекта и последовательность их реализации **УК-2.2 Уметь:** формулировать проблему, на решение которой направлен проект, грамотно определять цель проекта **УК-2.3 Владеть:** навыками проектирования решения конкретных задач проекта, выбирая оптимальный способ их решения
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**ОПК-5.1 Знать:** источники и классификацию угроз информационной безопасности, требования по защите информации при использовании СКЗИ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации **ОПК-5.2 Уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, разрабатывать требования к системе защиты информации **ОПК-5.2 Владеть:** **навыками работы с** нормативными правовыми актами в области информационной безопасности, применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и

		нейтрализации угроз безопасности компьютерных систем

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1	**УК – 2 / УК-2.1 Знать:** этапы жизненного цикла проекта и последовательность их реализации **УК-2.2 Уметь:** формулировать проблему, на решение которой направлен проект, грамотно определять цель проекта **УК-2.3 Владеть:** навыками проектирования решения конкретных задач проекта, выбирая оптимальный способ их решения	Тема 1. Тема 1. Информация как объект правового регулирования. Тема 2. Правые вопросы обеспечение информационной безопасности Тема 3. Правовое регулирование отношений по защите государственной тайны. Тема 4. Правовое регулирование отношений, связанных с режимом коммерческой тайны. Тема 5. Правовое регулирование отношений в области обработки персональных данных. Тема 6. Правовое регулирование электронного документооборота. Тема 7. Правовое регулирование отношений в области связи и массовых коммуникаций. Тема 8. Правовое регулирование отношений в области библиотечного и архивного дела. Тема 9. Правовое регулирование отношений в сфере организации и деятельности средств массовой	Вопросы для устного опроса по соответствующим темам. Тест.	Теоретические вопросы к зачету

		информации.		
2	ОПК-5 / **ОПК-5.1 Знать:** источники и классификацию угроз информационной безопасности, требования по защите информации при использовании СКЗИ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации **ОПК-5.2 Уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, разрабатывать требования к системе защиты информации **ОПК-5.2 Владеть:** навыками работы с нормативными правовыми актами в области информационной безопасности, применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем	Тема 1. Тема 1. Информация как объект правового регулирования. Тема 2. Правые вопросы обеспечение информационной безопасности Тема 3. Правовое регулирование отношений по защите государственной тайны. Тема 4. Правовое регулирование отношений, связанных с режимом коммерческой тайны. Тема 5. Правовое регулирование отношений в области обработки персональных данных. Тема 6. Правовое регулирование электронного документооборота. Тема 7. Правовое регулирование отношений в области связи и массовых коммуникаций. Тема 8. Правовое регулирование отношений в области библиотечного и архивного дела. Тема 9. Правовое регулирование отношений в сфере организации и деятельности средств массовой информации.	Вопросы для устного опроса по соответствующим темам. Тест.	Теоретические вопросы к зачету

3.2 Содержание оценочных средств

3.2.1. База вопросов для устного опроса по темам

Тема 1. Организационные источники и каналы утечки.

Место организационной защиты информации в системе комплексной защиты информации. Организационное обеспечение информационной безопасности как один из основных инструментов обеспечения безопасности организации.

Цели и задачи курса и его место в подготовке специалистов правоохранительной деятельности. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Совокупности методов защиты информации, используемых для перекрытия каналов утечки информации, как основные направления организационной защиты информации.

Коммуникационный процесс и его базовые элементы: источник информации, отправитель, сообщение, канал, получатель. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней. Классификация организационных каналов утечки конфиденциальной информации.

Тема 2. Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий

Отличительные особенности системы организационной защиты государственной и служебной тайн, обусловленные характером защищаемой информации и правом собственности на нее.

Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, различным степеням секретности. Присвоение грифа секретности работам, документам и изделиям. Изменение грифа секретности.

Порядок обращения с документами и другими материальными носителями, содержащими служебную информацию ограниченного распространения. Необходимость проставления пометки «Для служебного пользования».

Рассекречивание сведений и снятие ранее введенных ограничений. Основания для рассекречивания конфиденциальных сведений, документов и изделий.

Тема 3. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним.

Сотрудники правоохранительного органа как источник конфиденциальной информации и один из основных каналов ее разглашения. Особенности подбора сотрудников на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации «группы риска»: руководящий состав, средний управленческий состав, исполнители, сотрудники, осуществляющие технологические процессы передачи, обработки и хранения информации, и др.

Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации. Особенности документирования трудовых отношений с сотрудниками, обладающими конфиденциальной информацией.

Профессиональная ориентация и обучение персонала. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Основные формы обучения и методы контроля знаний.

Мотивация сотрудников к выполнению требований по защите информации. Основные формы воздействия на сотрудников как методы мотивации: использование различных форм вознаграждения.

Организация контроля за соблюдением персоналом требований режима защиты информации. Методы проверки персонала.

Основные меры по защите информации при увольнении сотрудника. Документирование процедуры увольнения сотрудника.

Тема 4. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников.

Понятие «допуск к государственной тайне». Формы допусков, их назначение и классификация. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск, и порядок ее составления, согласования и утверждения.

Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Снижение формы допуска и восстановление имевшегося допуска. Прекращение допуска. Порядок выдачи справок о форме допуска, учет, уничтожение.
Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.
Понятие «доступ к защищаемой информации». Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа.
Понятие «разрешительная система доступа», основные требования, предъявляемые к ней. Цели и задачи разрешительной системы. Порядок разработки, примерная структура и содержание Положения о разрешительной системе доступа. Организация работы по обеспечению контроля над ее выполнением. Формы разрешительных документов. Организация работ по созданию разрешительной системы. Положение о разрешительной системе доступа.
Особенности доступа к конфиденциальной информации различных категорий сотрудников. Обязанности лиц, допущенных к защищаемым сведениям.

Тема 5. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.
Понятие «служебное расследование» по фактам разглашения и утечки конфиденциальной информации. Цели и задачи служебного расследования.
Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования.
Документирование хода и результатов служебного расследования.

Тема 6. Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов
Понятие «охрана». Цели и задачи охраны. Объекты охраны: территория, здания, помещения, сотрудники, информационные ресурсы. Особенности их охраны. Виды и способы охраны.
Понятие «пропускной режим. Цели и задачи пропускного режима. Организация пропускного режима. Понятие пропуска. Виды пропусков и отличительных шифров. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты, их оборудование и организация работы.
Понятие «внутриобъектовый режим». Его основное назначение при ведении конфиденциальных работ и обращении с охраняемыми изделиями и документами. Порядок определения перечня предметов, запрещенных к проносу/провозу на режимную территорию.
Порядок допуска сотрудников в помещения, где ведутся конфиденциальные работы. Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организации и контроля доступа.

Тема 7. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.
Понятие режимных помещений и требования, предъявляемые к ним. Особенности оборудования помещения, где ведутся конфиденциальные работы.
Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ. Документальное оформление после обследования помещений на пригодность. Назначение ответственных лиц, имеющих право вскрывать и опечатывать режимные помещения.
Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных изделий и документов.
Порядок приема-сдачи под охрану режимных помещений.

Тема 8. Аналитическая работа как основа управления системой организационной защиты информации
Понятие, цели и задачи аналитической работы по защите информации. Методики аналитической работы, обеспечивающие управляемость системы организационной защиты информации.
Технология аналитической работы, ее основные этапы. Первый этап: определение проблемы, формулирование целей и предварительных гипотез (или версий); разработка программы (проекта) исследования. Второй этап: сбор информации; отбор и анализ источников информации; категории

источников; методы их оценки с точки зрения надежности; внутренние и внешние источники; план сбора информации; методы сбора (получения) информации. Третий этап: анализ собранной информации – производство аналитического продукта, его распространение (использование); процедура производства аналитического продукта: поиск смысловых логических связей между явлениями, фактами, событиями, людьми в соответствии с программой исследования и формулирования выводов, подтверждающих или опровергающих гипотезу.
Основные методы анализа: сравнение, сопоставление или противопоставление, классификация, в том числе многомерная, моделирование, графические методы, в том числе метод сети связей, и др.
Представление и оформление полученных результатов. Основные формы представления аналитического продукта.
Использование аналитических методов при определении объектов и субъектов защиты, их взаимоотношений, при проектировании построения, функционировании и оценке эффективности системы организационной защиты информации.

Тема 9. Планирование процессов организационной защиты информации
Сущность планирования как одной из основных функций управления системой организационной защиты информации. Цели планирования. Оценка и анализ состояния системы организационной защиты информации как основа планирования.
Стратегические и тактические планы. Соотношение планов организационной защиты информации с планами организации. Разновидности планов; их содержание и форма.
Методы планирования. Особенности программно-целевого планирования.

3.2.2 Тесты

1. В соответствии с Конституцией Российской Федерации информация и связь относятся:

а) к исключительному ведению Российской Федерации;

б) к совместному ведению Российской Федерации и субъектов Российской Федерации;

в) к ведению субъектов Российской Федерации.

2. Согласно легальному определению информация - это:

а) сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку;

б) сведения (сообщения, данные) независимо от формы их представления;

в) сообщение, переданное или полученное пользователем информационно-телекоммуникационной сети.

3. Лицо, самостоятельно создавшее информацию, либо получившее право разрешать или ограничивать доступ к информации, является:

а) создателем информации;

б) хранителем информации;

в) обладателем информации.

4. Не подлежат размещению в сети «Интернет»:

а) фамилии, имена и отчества председателя суда, заместителей председателя суда, судей, руководителя аппарата суда;

б) тексты судебных актов, вынесенные по делам, затрагивающим безопасность государства;

в) информация о внепроцессуальных обращениях, поступивших судьям по делам, находящимся в их производстве.

5.Объективная сторона информационной безопасности - это:

а) психологическое отношение граждан к вопросу правового регулирования отношений в сфере информационной безопасности;

б) система норм права об информационной безопасности;

в) система охранительных действий субъектов информационного права в отношении объекта охраны.

6. Под киберпреступлением понимается:

а) самостоятельный вид виновно совершенного общественно опасного деяния, запрещенного нормами Уголовного кодекса Российской Федерации;

б) любое преступление, совершенное в сфере информационной безопасности;

в) совершение действий в системе Интернет, при которых компьютер является орудием либо предметом посягательства в кибернетическом пространстве.

7. Понятие «информационная безопасность» закреплено:

а) в Законе Российской Федерации от 27 декабря 1991г. №1224-11 «О средствах массовой информации»;

б) в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

в) в Доктрине информационной безопасности.

8. К числу носителей сведений, составляющих государственную тайну, не относится:

а) руководитель органа государственной власти;

б) служебные документы;

в) техническое устройство.

9. Система защиты государственной тайны представляет собой:

а) совокупность органов защиты государственной тайны и используемых ими средств и методов защиты;

б) процедуры оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

в) порядок и способы отнесения сведений к государственной тайне и их засекречивание.

10. Под засекречиванием сведений понимается:

а) взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями;

б) передача сведений, составляющих государственную тайну, другим государствам или международным организациям;

в) ведение ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

11. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых:

а) административным актом органа государственной власти, в распоряжение которого переходит эта информация;

б) в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником;

в) в соответствии с заявлением собственника информации.

12. Коммерческая тайна представляет собой:

а) защищаемые юридическим лицом сведения любого характера (производственные, технические, экономические), имеющие коммерческую ценность в силу неизвестности их третьим лицам;

б) режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

в) сведения, для которых установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом.

13. Могут быть отнесены к информации, составляющей коммерческую тайну*:*

а) сведения о составе имущества государственного или муниципального предприятия, государственного учреждения;

б) сведения о численности и составе работников, о системе оплаты труда;

в) сведения, позволяющие юридическому лицу увеличить доходы и избежать неоправданных расходов.

14. Обладателем секрета производства является:

а) лицо, которое использует ноу-хау в целях извлечение прибыли;

б) лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании;

в) любое юридическое лицо или индивидуальный предприниматель.

15. По лицензионном договору:

а) одна сторона обязуется оформить в интересах другой стороны исключительное право на секрет производства;

б) одна сторона передает или обязуется передать принадлежащее ей исключительное право на секрет производства в полном объеме другой стороне;

в) одна сторона - обладатель исключительного права на секрет производства предоставляет или обязуется предоставить другой стороне право использования соответствующего секрета производства в установленных договором пределах.

16. Какая информация не относится к специальным категориям персональных данных?

а) информация о состоянии здоровья лица;

б) информации об имени и фамилии лица;

в) информация о религиозных взглядах лица.

17. Не относятся к числу специальных категорий персональных данных:

а) сведения, которые характеризуют физиологические особенности человека;

б) сведения, касающиеся расовой и национальной принадлежности;

в) сведения о состоянии здоровья и интимной жизни человека.

18. К числу прав субъекта персональных данных относится:

а) право на выбор вида обработки персональных данных автоматизированная, неавтоматизированная);

б) право на доступ к своим персональным данным;

в) право контролировать деятельность оператора персональных данных.

19. Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию – это:

а) ключ электронной подписи;

б) сертификат ключа проверки электронной подписи;

в) электронная подпись.

20. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети, называется:

а) электронным сообщением;

б) базой данных;

в) электронной цифровой подписью.

21. Удостоверяющий центр - это:

а) государственный орган, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации;

б) любое юридическое или физическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации;

в) юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации.

22. Тайна связи представляет собой:

а) деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений;

б) нечто скрываемое от других, известное не всем; секрет;

в) определенный режим доступа к информации, не подлежащей разглашению без согласия пользователя услуг, который реализуется путём принятия специальных мер организационного, правового, технического характера.

23. В соответствии с Федеральным законом « О почтовой связи» в Российской Федерации действуют:

а) почтовая связь общего пользования, осуществляемая государственными унитарными предприятиями, государственными учреждениями почтовой связи, а также иными операторами почтовой связи;

б) почтовая связь общего пользования; специальная связь федерального органа исполнительной власти; федеральная фельдъегерская связь; фельдъегерско-почтовая связь;

в) специальная связь федерального органа исполнительной власти, осуществляющего управление деятельностью в области связи;федеральная фельдъегерская связь;фельдъегерско-почтовая связь федерального органа исполнительной власти в области обороны.

24. Главный признак информационного общества:

а) наличие в продаже мобильных телефонов;

б) наличие у каждого свободного доступа к информационным ресурсам;

в) наличие у государства точных персональных данных каждого гражданина.

25. Какая информация относится к специальным категориям персональных данных?

а) информация о философских взглядах;

б) информация об образовании лица;

в) информация о семейном положении лица.

26. Сведения, составляющие тайну совещания судей, подпадают под режим:

а) государственной тайны;

б) тайны следствия;

в) тайны судопроизводства.

27. Кто вправе быть учредителем средства массовой информации?

а) государственный орган;

б) гражданин Российской Федерации, не достигший восемнадцатилетнего возраста;

в) гражданин иностранного государства.

28. Какие данные обязательно должны быть указаны в заявлении о регистрации средства массовой информации?

а) данные о главном редакторе;

б) телефоны редакции;

в) источники финансирования.

29. Что относится к условиям правомерности осуществления журналистом скрытой аудио- и видеозаписи?

а) отсутствие технических и иных условий для осуществления открытой записи;

б) получение санкции прокурора;

в) соответствие цели скрытой записи общественным интересам.

30. Распространение сообщений и материалов, подготовленных с использованием скрытой аудио- и видеозаписи, допускается:

а) если демонстрация записи производится по решению суда;

б) если это не нарушает интересов лица, аудио- или видеозапись которого сделана;

в) если это необходимо для защиты интересов лица, осуществившего скрытую аудио- или видеозапись.

31. К какой информации не может быть ограничен доступ граждан?

а) к информации о личной жизни высших должностных лиц;

б) к информации о массовых беспорядках в зоне, где введено военное положение;

в) к информации о состоянии окружающей среды.

32. Обеспечение информационной безопасности детей регулируется:

а) Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;

б) Федеральным законом от 07.02.2011 №3-ФЗ «О полиции»;

в) Федеральным законом от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

33. В Законе «О безопасности» сформулированы принципы обеспечения безопасности, к основным из которых отнесены:

а) соблюдение и защита прав и свобод человека и гражданина; законность; системность и комплексность применения органами государственной власти политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритет предупредительных мер в целях обеспечения безопасности; взаимодействие органов государственной власти с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности;

б) гуманизм; оперативность; законность; уважение и соблюдение прав и свобод человека и гражданина; взаимная ответственность личности, общества и государства по обеспечению безопасности; приоритет предупредительных мер в целях обеспечения безопасности; взаимодействие органов государственной власти с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности;

в) законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; системность и комплексность применения органами государственной власти политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритет предупредительных мер в целях обеспечения безопасности.

34. Информационная безопасность Российской Федерации – это:

а) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

б) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

3) состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

35. Правовое регулирование в информационной сфере – это воздействие государства на:

а) тех, кто мешает предоставлению и распространению информации;

б) общественные отношения в информационной сфере;

в) субъектов информационной сферы общества.

4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Критерии оценивания компетенций в ходе промежуточной аттестации

Код компетенции	Планируемые результаты обучения по дисциплине	Критерии оценивания			
		Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
УК-2	**УК-2.1: Знает** этапы жизненного цикла проекта и последовательность их реализации	Фрагментарный характер знаний, вопросы не раскрыты	Знания носят дискретный характер, имеются множественные пробелы	Знает материал по предмету, но его изложение содержит отдельные пробелы	Знает нормативные правовые акты в области защиты информации
	УК-2.2: Умеет формулировать проблему, на решение которой направлен проект, грамотно определять цель проекта	Материал по теме не раскрыт, фрагментарные представления по теме	Умеет успешно, но не систематично изложить вопросы темы, присутствуют ошибки	Умеет привести и успешно раскрыть отдельные юридические понятия и определения по предмету	Умеет использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации
	УК-2.3: Владеть навыками проектирования решения конкретных задач проекта, выбирая оптимальный способ их решения	Материал по теме не раскрыт, фрагментарное применение навыков	Владеет навыком изложения, однако имеются множественные ошибки в выводах и оценках	Владеет навыком по обоснованию поставленных вопросов при наличии ошибок в выводах и оценках	Владеет навыками обеспечения использования правовых актов в своей профессиональной деятельности

ОПК-5	**ОПК-5.1: Знает** источники и классификацию угроз информационной безопасности, требования по защите информации при использовании СКЗИ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	Фрагментарный характер знаний, вопросы не раскрыты	Знания носят дискретный характер, имеются множественные пробелы	Знает материал по предмету, но его изложение содержит отдельные пробелы	Знает основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности; организационно-правовые основы режима секретности
	ОПК-5.2: Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, разрабатывать требования к системе защиты информации	Материал по теме не раскрыт, фрагментарные представления по теме	Умеет успешно, но не систематично изложить вопросы темы, присутствуют ошибки	Умеет привести и успешно раскрыть отдельные юридические понятия и определения по предмету	Умеет использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации

	ОПК-5.2: Владеет навыками работы с нормативными правовыми актами в области информационной безопасности, применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем	Материал по теме не раскрыт, фрагментарное применение навыков	Владеет навыком изложения, однако имеются множественные ошибки в выводах и оценках	Владеет навыком по обоснованию поставленных вопросов при наличии ошибок в выводах и оценках	Владеет методами предупреждения и конструктивного разрешения конфликтных ситуаций в процессе правоохранительной деятельности, с учетом социальных, культурных, профессиональных и иных различий

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Формой контроля знаний является зачет. На зачете оцениваются теоретические знания обучающегося и приобретенные навыки их практического применения.

Зачет проводится в форме тестирования. Студент должен решить 25 тестовых заданий, показывающих уровень формирования компетенции. Из приведенных выше тестовых заданий должно быть сформулировано четыре варианта (четыре опросных листа с тестами), по 25 вопросов в каждом. Для решения тестовых заданий дается 30 минут.

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Результаты промежуточной аттестации и уровни сформированности компетенций.

Успеваемость обучающихся на зачете оценивается отметками «**зачтено», «не зачтено».**

По результатам оценивания результатов тестирования студенту могут быть заданы дополнительные уточняющие вопросы.

Оценка «зачтено» ставится, если более чем 20 вопросов тестовых заданий решены верно, при этом при решении задач студент продемонстрировал на среднем или высоком уровне умения квалифицированно применять нормативные правовые акты и давать квалифицированные заключения в сфере правовых основ информационной безопасности. Признается, что данные умения продемонстрированы на высоком уровне, если рассуждение последовательно, логично, основано на действующем законодательстве, правильно определены применимые нормы права, вывод точно изложен и последовательно аргументирован.

4.2.2 Критерии оценивания теста

Количество правильных ответов	Уровень сформированности компетенций ОК-4, ОПК-6	Оценка
Менее 10	недостаточный	Не зачтено
11-14	базовый	Не зачтено

15-19	средний	Зачтено
20-25	высокий	Зачтено

Ключи к Тестам

1	**А**	**18**	**Б**	**35**	**Б**
2	**Б**	**19**	**В**		
3	**В**	**20**	**А**		
4	**Б**	**21**	**В**		
5	**Б**	**22**	**В**		
6	**В**	**23**	**Б**		
7	**В**	**24**	**Б**		
8	**А**	**25**	**А**		
9	**А**	**26**	**А**		
10	**В**	**27**	**В**		
11	**Б**	**28**	**В**		
12	**Б**	**29**	**А**		
13	**В**	**30**	**В**		
14	**Б**	**31**	**А**		
15	**В**	**32**	**Б**		
16	**Б**	**33**	**Б**		
17	**А**	**34**	**Б**		

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета физического факультета согласовано М.А. Загребин

Заседанием кафедры прокурорского надзора и организации правоохранительной деятельности

Протокол заседания № 07 от 28.01.2025

Заведующий кафедрой согласовано А.В. Майоров

Автор (составитель) Т.П. Макашова

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13»апреля 2021 г. № 247-1