Фонд оценочных средств для промежуточной аттестации

по дисциплине

Организационное и правовое обеспечение информационной безопасности

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Организационное и правовое обеспечение информационной безопасности**.
Семестр (семестры) изучения: 10 семестр.
Форма (формы) промежуточной аттестации: зачёт 10 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Организационное и правовое обеспечение информационной безопасности» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
УК-10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1. Имеет представление о содержании понятий «экстремизм», «терроризм», основных формах их проявления и последствиях. УК-10.2. Имеет представление о содержании понятия «коррупционное поведение», разграничивает коррупционные и схожие некоррупционные явления в различных сферах жизни общества. УК-10.3. Организует профессиональную среду, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.	Знать: – этические и правовые нормы поведения; – содержание понятий «экстремизм», «терроризм», «коррупционное поведение»; основные формы их проявления и последствия; – основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве; – практику применения действующего антикоррупционного законодательства. Уметь: – правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве; – разграничивать коррупционные и

			схожие некоррупционные явления в различных сферах жизни общества. Владеть: – навыками применения на практике антикоррупционного законодательства; – навыками пресечения коррупционного поведения; – навыками организации профессиональной среды, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности. ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и	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. 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. Владеть: – навыками работы с нормативными правовыми актами в области информационной безопасности; – навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

		организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.	
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.2 Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в	Знать: – нормативные правовые акты в области защиты информации. Уметь: – использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации. Владеть: – навыками обеспечения использования правовых актов в своей профессиональной деятельности.

		организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	

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-10 ОПК-5, ОПК-6	Организационное и правовое обеспечение информационной безопасности	Устный опрос по темам. Тесты.	Перечень вопросов к зачету.

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

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. К основным организационным мероприятиям по защите информации можно отнести:
а) организацию режима и охраны; организацию работы с сотрудниками; организацию работы с документами; организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией.
б) организацию охраны подвижных объектов; организацию работы с партнерами; организацию работы с документами; организацию контрразведывательных мероприятий; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией
в) организацию пропускного режима; организацию работы с клиентами; организацию использования технических средств сбора и хранения конфиденциальной информации; организацию аналитической работы.

2. Силы и средства защиты коммерческого предприятия в зависимости от решаемых задач, условий, специфических особенностей подразделяются на следующие основные направления защиты:
а) правовой защиты, технической защиты, специальной защиты, информационно-коммерческой защиты.
б) правовой защиты, инженерно-технической защиты, организационной защиты.
в) физической защиты, технической защиты, специальной защиты, морально-

психологической защиты.

3. Под политикой информационной безопасности понимается:
а) разработка пакета документов, направленных на защиту информации и ассоциированных с ней ресурсов.
б) отдача указаний и контроль за их выполнением, направленных на защиту информации и ассоциированных с ней ресурсов.
в) совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

4. Основными задачами сил и средств физического защиты фирмы являются:
а) - организация личной охраны руководителей фирмы и ведущих специалистов.
- организация охраны персонала и аттестованных по режиму конфиденциальных помещений.
- организация и поддержание пропускного и внутри объектового режима.
- организация и установление мер физической и технической защиты зданий и помещений.
- организация и осуществление мер по обеспечению безопасности деятельности и защиты сведений, составляющих государственную и коммерческую тайну.
- разработка и совершенствование системы предотвращения несанкционированного доступа и допуска к сведениям, составляющим коммерческую тайну.
- организация, разработка и контроль системы безопасности в повседневных и особых условиях.
б) - организация личной охраны всего персонала предприятия.
- организация внутри объектового режима.
- организация и установление мер физической и технической защиты при перевозке ценных грузов.
- организация и осуществление мер защите сведений, составляющих коммерческую тайну.
- разработка системы предотвращения несанкционированного доступа к сведениям, составляющим коммерческую тайну.
в) - организация личной охраны администрации фирмы и членов их семей.
- организация охраны стационарных объектов предприятия.
- осуществление мер по защите сведений, составляющих государственную тайну.
- разработка системы предотвращения несанкционированного доступа к сведениям, составляющим коммерческую тайну.
- организация, разработка и контроль системы безопасности в особых условиях.

5. К основным техническим средствам безопасности коммерческого предприятия относятся:
а) средства физической защиты, аппаратные средства защиты, программные средства защиты, правовые методы защиты.
б) средства физической защиты, аппаратные средства защиты, программные средства защиты, математические (криптографические) методы защиты
в) средства физической защиты, производственные средства защиты,

информационно-коммерческие методы защиты

6. Основными принципами создания и поддержания организационного обеспечения комплексной безопасности являются:
а) законности, комплексности, обоснованности, соблюдение баланса защиты жизненно важных интересов предприятия и субъекта защиты, ответственности за порученный участок работы, децентрализации управления.
б) законности, плановости, обособленности, соблюдение баланса защиты жизненно важных интересов предприятия и государства, непрерывности, централизации управления, взаимодействия и координации
в) законности, комплексности, обоснованности, соблюдение баланса защиты жизненно важных интересов предприятия и субъекта защиты, взаимной ответственности, централизации управления, взаимодействия и координации.

7. Система безопасности предприятия действует на основе следующих организационно-правовых документов:
а) Конституции РФ. Устава области. Федерального закона «О безопасности».
б) Устава. Положения о системе собственной безопасности. Руководства по защите конфиденциальной информации. Инструкции о порядке работы с иностранными специалистами. Руководства по инженерно-технической защите помещений и технических средств.
в) Конвенции по правам человека. Положения о системе коллективной безопасности. Приказов и инструкций по безопасности.

8. Внешний контроль над деятельностью службы безопасности осуществляют:
а) органы внутренних дел; следственные органы; прокуратура; суд; общественные организации.
б) органы внутренних дел; следственные органы; прокуратура; суд; политические партии и движения
в) органы внутренних дел; следственные органы; прокуратура; суд; другие административные органы по вопросам, отнесенным к их компетенции в сфере частной детективной и охранной деятельности.

9. В целях сыска служба безопасности имеет право:
а) проводить допрос граждан и должностных лиц. Наводить справки. Изучать предметы и документы. Вести розыск утраченного (похищенного) иму¬щества. Вести негласное наблюдение и прослушивание граждан. Приобретать, хранить и применять в установленном порядке огнестрельное оружие. Оказывать содействие правоохранительным органам в обеспечении правопорядка, в том числе и на договорной основе.
б) проводить устный опрос граждан и должностных лиц. Изучать предметы и документы. Вести розыск похищенного имущества. Вести наблюдение. Применять в установленном порядке специальные средства.
в) проводить устный опрос граждан и должностных лиц (с их согласия). Наводить справки. Изучать предметы и документы (с письменного согласия их владельцев).

Вести розыск утраченного (похищенного) имущества. Вести наблюдение. Использовать видео-, аудиозаписи, кино- и фотосъемки (в порядке, установленном законом), технические и иные средства, не причиняющие вреда жизни и здоровью граждан и окружающей среде, а также средства оперативной радио- и телефонной связи. Приобретать, хранить и применять в установленном порядке специальные средства. Оказывать содействие правоохранительным органам в обеспечении правопорядка, в том числе и на договорной основе.

10. По отношению к информации и информационным ресурсам проявляются следующие угрозы:
а) целостности; подделке; полноты; доступности.
б) целостности; конфиденциальности; фальсификации; доступности.
в) целостности; конфиденциальности; полноты; доступности.

11. Существует следующие формы допуска к секретным работам и документам:
а) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности», «совершенно секретно», «секретно»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно», «секретно»).
- третья форма допуска (имеют право на ознакомление со сведениями «секретно»).
б) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности», «совершенно секретно», «секретно»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно», «секретно»).
- третья форма допуска (имеют право на ознакомление со сведениями «секретно» и «для служебного пользования»).
в) - наивысшая форма допуска (имеют право на ознакомление со сведениями «особой важности»).
- вторая форма допуска (имеют право на ознакомление со сведениями «совершенно секретно»). Третья форма допуска (имеют право на ознакомление со сведениями «секретно»).

12. Условия прекращения допуска должностного лица или гражданина к государственной тайне:
а) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий; длительным отсутствием на рабочем месте (например по болезни); возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.
б) расторжения с ним трудового договора (контракта) в связи с про-ведением организационных и (или) штатных мероприятий; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защи¬той государственной тайны; возникновения обстоятельств, являющихся согласно статье 22 Закона «О государственной тайне» основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

в) в связи с переходом на новую должность; однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны; в связи с увольнением из предприятия.

13. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне могут касаться:
а) права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на хранение сведений, составляющих государственную тайну; права на проведении проверочных мероприятий в период нахождения в отпуску.
б) права выезда за город, на дачу без охраны на срок; права на продажу сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.
в) права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.
14. Допуск специалиста к коммерческим секретам обязывает:
а) строго соблюдать требования инструкций по работе с коммерческими секретами; ответственность за нарушение режима информационной безопасности.
б) строго соблюдать требования руководства предприятия по вопросам трудового договора; обязательства по предоставлению гарантий и компенсаций за работу с конфиденциальной информацией.
в) быстрый карьерный рост по работе; применять свои права в области соблюдения режима информационной безопасности.

15. Под режимом КТ следует понимать:
а) выполнение обладателем информации, состав¬ляющей КТ, неукоснительное исполнение распоряжений руководства по охране ее конфиденциальности коммерческих секретов.
б) проведение руководством предприятия комплекса мер по расследованию нарушений обращения с конфиденциальной информацией
в) правовые, организационные, технические и иные принимаемые обладателем информации, составляющей КТ, меры по охране ее конфиденциальности.

16. Обладатель информации, составляющей государственную тайну, имеет право:
а) использовать информацию, составляющую государственную тайну, для собственных нужд.
б) по своему усмотрению передавать секретную информацию сторонним организациям.
в) вносить предложения по вопросам совершенствования режима охраны

государственной тайны.

17. Комиссия, проводящая служебное расследование по факту нарушения информационной безопасности, обязана:
а) - установить условия, обстоятельства и причины разглашения сведений или утраты документов и выработать рекомендации по их устранению;
- использовать все имеющиеся возможности по розыску утраченного документа;
- выявить лиц, виновных в разглашении сведений или утрате документа.
б) - установить условия, обстоятельства и причины разглашения сведений или утраты документов и выработать рекомендации по их устранению;
- использовать все имеющиеся возможности для передачи дела в суд;
- выявить лиц, виновных в разглашении сведений или утрате документа.
в) - оповестить руководство предприятия о нарушении информационной безопасности;
- использовать все имеющиеся возможности по розыску утраченного документа;
- выявить лиц, виновных в разглашении сведений или утрате документа.

18. Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:
а) - процентные надбавки к заработной плате в зависимости от сте¬пени секретности сведений, к которым они имеют доступ;
- быстрый карьерный рост.
б) - процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.
в) - процентные надбавки к заработной плате в зависимости от сте¬пени секретности сведений, к которым они имеют доступ;
- моральное стимулирование.

19. Основаниям для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:
а) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
б) постоянное проживание его близких родственников в другом регионе страны;
в) временное проживание его самого на съемных квартирах или в гостиницах.

20. Эффективная защита обеспечивается при выполнении следующих условий:
а) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между заинтересованными подразделениями фирмы;
- разработка режимных мер на основе оценки информации и объектов, подлежащих

защите (классификации);
- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;
- централизацией специального делопроизводства;
- наличием списка лиц, допущенным к такого рода информации;
- наличие вооруженной охраны, а также введением усиленных пропускных режимов.
б) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между заинтересованными подразделениями фирмы;
- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);
- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;
- организация специального делопроизводства, введение соответствующей маркировки документов;
- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;
- наличие охраны, а также пропускного и внутриобъектового режимов.
в) - единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между заинтересованными подразделениями фирмы;
- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);
- персональная ответственность на всех исполнительских уровнях за обеспечение сохранности конфиденциальной информации;
- организация специального делопроизводства, введение соответствующей маркировки документов;
- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;
- наличием вневедомственной охраны.

21. Объектами охраны предприятия выступают:
а) Стационарные объекты. Руководство предприятия и их семьи. Денежные средства. Ценные бумаги и другие ценности.
б) Стационарные объекты. Подвижные объекты. Персонал. Денежные средства. Ценные бумаги и другие ценности.
в) Стационарные объекты. Отдельные сотрудники предприятия. Денежные средства. Служба безопасности предприятия.

22. Существует несколько видов охраны, в том числе:
а) охрана с помощью привлечения собак (кинологическая служба); охрана путем выставления постов; комбинированная охрана.

б) охрана с помощью технических средств с подключением на пульт централизованного наблюдения и остановкой автоматической сигнализации; охрана путем выставления постов; комбинированная охрана.
в) автономная охрана с помощью технических средств наблюдения и автоматической сигнализации; охрана путем выставления подвижных; комбинированная охрана.

23. Система обеспечения безопасности объекта охранной деятельности должна строиться на следующих принципах:
а) Комплексность. Эшелонирование. Равнопрочность. Разумная достаточность. Непрерывность.
б) Комплексность. Эшелонирование. Оснащенность. Разумная достаточность. Непрерывность.
в) Комплексность. Эшелонирование. Своевременность. Разумная достаточность. Непрерывность.

24. К основным требованиям внутриобъектового режима относится:
а) Соблюдение распорядка рабочего времени. Строгое соблюдение сотрудниками правил производственной безопасности. Установление порядка приема и работы с посетителями сторонних организаций. Порядок сдачи и приема конфиденциальных документов. Порядок ведения факсовых и телекоммуникационных обменов информацией.
б) Установление четкого распорядка рабочего времени. Строгое соблюдение сотрудниками правил взаимоотношений в коллективе. Установление порядка работы с партнерами. Оснащение фирмы техническими средствами обеспечения производственной деятельности. Порядок посещения помещений сотрудниками и посетителями. Порядок ведения телефонных, разговоров.
в) Установление четкого распорядка рабочего времени. Строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности. Установление порядка приема и работы с посетителями сторонних организаций. Оборудование фирмы техническими средствами обеспечения производственной деятельности. Порядок сдачи и приема помещений под охрану. Порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

25. По уровню охраны и объему предпринимаемых мер безопасности коммерческие предприятия (организации) подразделяют следующие основные категории:
а) объекты со свободным допуском персонала и клиентов; объекты с простыми ограничениями и ограждениями типа неохраняемых заграждений; объекты с охраняемыми заграждениями, контролируемыми охранниками, с постовыми нарядами, патрульными службами и сотрудниками пропускной системы; объекты с особым режимом охраны, допуск на которые обеспечивается специально подготовленными и расставленными по территории и периферии охранниками и сложными техническими системами с телемониторами и звуковой сигнализацией.

б) объекты со свободным допуском персонала и клиентов; объекты с простыми ограничениями; объекты с особым режимом охраны, допуск на которые обеспечивается охранниками и сложными техническими системами с телемониторами и звуковой сигнализацией.
в) объекты со свободным допуском персонала и клиентов; объекты контролируемыми не вооруженными охранниками службы безопасности предприятия; объекты с усиленным режимом охраны.

3.2.3. База теоретических вопросов к зачету

№ п/п	Формулировка вопроса	Контролируемые темы
1.	Организационные источники и каналы утечки.	1
2.	Силы, средства и условия организационной защиты информации	1
3.	Особенности системы организационной защиты информации, составляющей государственную тайну.	3
4.	Особенности системы организационной защиты информации, составляющей служебную тайну.	5
5.	Порядок засекречивания конфиденциальных сведений, документов и изделий.	2
6.	Порядок рассекречивания конфиденциальных сведений, документов и изделий.	2
7.	Особенности подбора сотрудников на должности, связанные с работой с конфиденциальной информацией.	3
8.	Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации и особенности документирования трудовых отношений.	3
9.	Понятие и виды ответственности за преступления и правонарушения в сфере защиты информации.	3
10.	Процедура оформления, изменения формы допуска и переоформления допусков и ее документирование.	4
11.	Организация доступа к конфиденциальной информации.	4
12.	Понятие, цели, задачи и основные требования разрешительной системы доступа, предъявляемые к ней.	4
13.	Особенности доступа к конфиденциальной информации различных категорий сотрудников. Обязанности лиц, допущенных к защищаемым сведениям.	5
14.	Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации.	5
15.	Организация контроля за соблюдением сотрудников требований режима защиты информации. Методы проверки сотрудников.	5
16.	Основные меры по защите информации при увольнении сотрудника. Документирование процедуры увольнения сотрудника.	6
17.	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации	6
18.	Организация охраны территории, зданий, помещений и персонала	7
19.	Виды и способы охраны. Факторы выбора приемов и средств охраны..	7
20.	Организация пропускного режимов	8
21.	Организация внутриобъектового режимов	8
22.	Понятие режимных помещений и требования, предъявляемые к ним.	9
23.	Порядок аттестации помещений на пригодность их для ведения конфиденциальных работ и его документальное оформление.	9

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации устанавливается действующими нормативными документами ФГБОУ ВО «ЧелГУ» (Положением о текущем контроле и промежуточной аттестации обучающихся в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет» по программам высшего образования»).

Зачет проводится в устной форме. Обучающийся получает билет, который включает 2 теоретических вопроса. Для зачета задания билета представлены в виде теоретических вопросов из базы вопросов, ответ на которые позволяет оценить уровень сформированности знаний и умений в структуре компетенций дисциплины. Продолжительность подготовки ответа – 40 минут. После подготовки экзаменатор заслушивает ответ обучающегося на два вопроса (задания) билета. Ответы на вопросы билета оцениваются в соответствии с критериями оценки теоретического вопроса. Экзаменатор имеет право задавать обучающемуся дополнительные вопросы по теоретической и практической части курса. По результатам оценивания ответа студента на вопросы билета и дополнительные вопросы (если они были заданы), экзаменатор определяет уровень сформированности соответствующих компетенций и выставляет итоговую оценку за зачет – «зачтено» / «не зачтено»..

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Устный опрос по темам	8x5=40
2	Тесты	8x5=40
3	Зачет (2 теоретических вопроса)	2x10=20
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

4.2.1. Критерии оценивания устного опроса по темам

Устный опрос проводится на каждом занятии, кроме вводного.

Максимальный балл за один опрос – 5 баллов.

Максимальный балл за все опросы – 40 баллов.

Отлично/ зачтено/ 5 баллов	Хорошо/ зачтено/ 4 балла	Удовлетворительно/ зачтено/ 3 балла	Неудовлетворительно/ не зачтено/ 0-2 балла
Обучающийся отлично знает материал, умеет	Обучающийся хорошо знает материал, умеет	Обучающийся знаком с материалом.	Обучающийся не знает основных положений

анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.	анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.	Обучающийся допускает фактические ошибки.	вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.2. Критерии оценивания теста

Тест проводится на каждом занятии, кроме вводного.
Максимальный балл за один тест – 5 баллов.
Максимальный балл за все тесты – 40 баллов.

Тест на каждом занятии включает 5 вопросов. Каждый правильный ответ оценивается в 1 балл.

4.2.3. Критерии оценивания теоретического вопроса зачета

Максимальный балл за один вопрос – 10 баллов.
Максимальный балл за зачет – 20 баллов.

Рекомендуемые к оцениванию составляющие ответа на теоретический вопрос	**Критерии для оценивания**	**Баллы**
полнота, развёрнутость и глубина	степень охвата всех основных элементов, составляющих содержание вопроса; понимание существа раскрываемого вопроса	5
корректность использования терминологического аппарата	формулирование понятий и категорий образующих содержание вопроса, а также объяснение их значения для профессиональной деятельности и правовой культуры специалиста	1
конкретность	умение связать абстрактные знания с конкретными явлениями, показать на примерах основные положения вопроса	1
системность	понимание связей между различными элементами содержания вопроса, а также его взаимосвязей с другими темами курса и материалом иных учебных дисциплин образовательной программы	1
логичность и аргументированность ответа		1
осознанность, самостоятельность мышления		1

Зачтено/6-10 баллов – Дан полный, развёрнутый ответ на основе знания основной литературы, показано умение выделять существенные и несущественные моменты материала; ответ чётко структурирован, выстроен в логической последовательности, изложен грамотным языком.

Не зачтено/0-5 баллов – Ответ не дан, либо дан неполно с существенными нарушениями логики и последовательности изложения, грубыми ошибками, демонстрирующими незнание либо отрывочное представление об учебном вопросе, речь неграмотная.

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются баллы за ответ на зачете, которые суммируются с текущими баллами, полученными за выполнение контрольной и лабораторных работ.

Итого:
Менее 60 – не зачтено
61-100 - зачтено.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы;
   - знает нормативные правовые акты в области защиты информации;
   - знает основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности; организационно-правовые основы режима секретности;
   - 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;
   - 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

- владеет навыками обеспечения использования правовых актов в своей профессиональной деятельности;
- владеет методами предупреждения и конструктивного разрешения конфликтных ситуаций в процессе правоохранительной деятельности, с учетом социальных, культурных, профессиональных и иных различий.

2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо»;
   - знает материал по предмету, но его изложение содержит отдельные пробелы;
   - умеет привести и успешно раскрыть отдельные юридические понятия и определения по предмету;
   - владеет навыком по обоснованию поставленных вопросов при наличии ошибок в выводах и оценках.
3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%;
   - знания носят дискретный характер, имеются множественные пробелы;
   - умеет успешно, но не систематично изложить вопросы темы, присутствуют ошибки;
   - владеет навыком изложения, однако имеются множественные ошибки в выводах и оценках.
4. Низкий уровень соответствует оценке «Неудовлетворительно».
   - фрагментарный характер знаний, вопросы не раскрыты;
   - материал по теме не раскрыт, фрагментарные представления по теме;
   - материал по теме не раскрыт, фрагментарное применение навыков.

Специальность 10.05.01 Компьютерная безопасность
Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Фонд оценочных средств по дисциплине «Организационное и правовое обеспечение информационной безопасности»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 24.02.25	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета математического факультета	согласовано	Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой	согласовано	А. Н. Ручай
Автор (составитель)		А. Н. Ручай

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