Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 17.06.2026 16:06:56
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c8166...

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Организационно-правовое обеспечение информационной безопасности
название дисциплины (модуля)

Направление подготовки	10.04.01 «Информационная безопасность»
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	1

Введение

1. Назначение: данный фонд оценочных предназначен для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» по дисциплине «Организационно-правовое обеспечение информационной безопасности».

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины «Организационно-правовое обеспечение информационной безопасности» в соответствии с образовательной программой 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем».

3. Разработчик Ванина Анна Георгиевна, к.т.н., доцент кафедры организации и технологии защиты информации.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В.И., заведующий кафедрой

Члены экспертной группы: Жук А.П., профессор кафедры

Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком-С»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Организационно-правовое обеспечение информационной безопасности».

5. Срок действия ФОС: определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем				
ПК-3 ИД-1 состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	на низком уровне: знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	в основном знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем
ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	на низком уровне: умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	в основном умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	на высоком профессиональном уровне умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем
ПК-3 ИД-3 выбор оптимального набора технических мер для повышения защищённости киберфизических систем	на низком уровне владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	в основном владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем	на высоком профессиональном уровне владеет навыками выбора оптимального набора технических мер для повышения защищённости киберфизических систем
ПК-3 ИД-4 осуществляет анализ предложений по совершенствованию системы управления информационно	на низком уровне осуществляет анализ предложений по совершенствованию системы управления информационной	в основном осуществляет анализ предложений по совершенствованию системы управления информационной	умеет осуществлять анализ предложений по совершенствованию системы управления информационно	на высоком профессиональном уровне осуществляет анализ предложений по совершенствованию системы

й безопасностью киберфизических систем	безопасностью киберфизических систем	безопасностью киберфизических систем	й безопасностью киберфизических систем	управления информационной безопасностью киберфизических систем

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения очная, семестр 1	
1 семестр			
1.	Государственная система защиты информации	Совокупность органов (субъектов) защиты информации, используемых ими методов и средств, а также системы регулирования отношений, возникающих при осуществлении защиты информации – это:	ПК-3
2.	a)	Организационную основу системы обеспечения информационной безопасности Российской Федерации составляют (все перечисленное вместе): a) Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти b) Совет Федерации Федерального Собрания Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы прокурорской власти c) Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы здравоохранения, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы,	ПК-3

		создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности d) Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти e) Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности	
3.	а)	К органам федеральной службы безопасности относятся (все перечисленное вместе): а) федеральный орган исполнительной власти в области обеспечения безопасности; управления (отделы) федерального органа исполнительной власти в области обеспечения безопасности по отдельным регионам и субъектам Российской Федерации (территориальные органы безопасности); управления (отделы, службы, отряды) федерального органа исполнительной власти в области обеспечения безопасности по пограничной службе (пограничные органы); территориальные органы безопасности; авиационные подразделения, центры специальной подготовки	ПК-3

		b) территориальные органы безопасности, органы безопасности в войсках, пограничные органы и другие органы безопасности являются территориальными органами федерального органа исполнительной власти обеспечения безопасности в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях, а также в их органах управления (органы безопасности в войсках) c) авиационные подразделения, центры специальной подготовки, подразделения специального назначения, предприятия, образовательные и научные организации, экспертные, судебно-экспертные, военно-медицинские подразделения и организации (далее - военно-медицинские организации), военно-строительные подразделения и иные организации и подразделения, предназначенные для обеспечения деятельности федеральной службы безопасности d) федеральный орган исполнительной власти в области обеспечения безопасности, территориальные органы безопасности, органы безопасности в войсках и пограничные органы могут иметь в своем составе подразделения, непосредственно реализующие основные направления деятельности органов федеральной службы безопасности, управленческие и обеспечивающие функции; другие управления (отделы) федерального органа исполнительной власти в области обеспечения безопасности, осуществляющие отдельные полномочия данного органа или обеспечивающие деятельность органов федеральной службы безопасности	
4.	Организационно-технические методы	К каким методам обеспечения информационной безопасности Российской Федерации относится создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи:	ПК-3
5.	Криптографическое преобразование	Преобразование информации при помощи шифрования и (или) выработки имитовставки – это:	ПК-3
6.	a) b) c) d) e) f) g) i)	Основные задачи ФСБ России a) управление органами безопасности, а также организация их деятельности b) информирование Президента Российской Федерации	ПК-3

		c) организация выявления, предупреждения и пресечения разведывательной и иной деятельности специальных служб и организаций иностранных государств, отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации d) организация выявления, предупреждения, пресечения и раскрытия преступлений, осуществление досудебного производства по которым отнесено к ведению органов безопасности e) организация и осуществление борьбы с терроризмом и обеспечение борьбы с диверсионной деятельностью f) формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности g) осуществление в пределах своих полномочий разведывательной деятельности; h) легализация преступных доходов, незаконная миграцией, незаконный оборот оружия, боеприпасов, взрывчатых и отравляющих веществ, наркотических средств и психотропных веществ, специальных технических средств i) осуществление в пределах своих полномочий мер по обеспечению защиты и охраны государственной границы	
7.	Организационные средства обеспечения информационной безопасности	К каким видам средств обеспечения информационной безопасности относятся средства кадрового обеспечения, средства научного обеспечения, средства информационного обеспечения; материальные средства, финансовые средства?	ПК-3
8.	a) b) c) d) e)	Основные виды организационных средств обеспечения информационной безопасности: a) Средства кадрового обеспечения b) Средства научного обеспечения c) Средства информационного обеспечения d) Материальные средства e) Финансовые средства f) Средства технического обеспечения g) Физические средства	ПК-3

		h) Средства логического обеспечения	
9.	b)	Основными источниками угроз информационной безопасности являются все указанное в списке: a) Хищение жестких дисков, подключение к сети, инсайдерство b) Перехват данных, хищение данных, изменение архитектуры системы c) Хищение данных, подкуп системных администраторов, нарушение регламента работы	ПК-3
10.	a)	Политика безопасности в системе (сети) – это комплекс: a) Руководств, требований обеспечения необходимого уровня безопасности b) Инструкций, алгоритмов поведения пользователя в сети c) Нормы информационного права, соблюдаемые в сети	ПК-3
11.	Руководитель	Кто отвечает за основные направления деятельности на предприятии, такие как планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений по непосредственному доступу к конфиденциальной информации своих сотрудников и представителей других организаций; распределение обязанностей и задач между должностными лицами и структурными подразделениями; аналитическая работа?	ПК-3
12.	a) b) c)	Перечислите направления защиты информации a) Правовая защита информации b) Организационная защита информации c) Инженерно-техническая защита информации d) Юридическая защита информации e) Государственная защита информации	ПК-3
13.	Технические средства защиты информации	К каким средствам защиты информации относят устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите?	ПК-3
14.	Угрозы доступности	По аспекту ИБ к каким угрозам ИБ относятся отказ пользователей (нежелание, неумение работать с ИС); внутренний отказ информационной системы (ошибки при переконфигурировании системы, отказы программного и аппаратного обеспечения, разрушение данных); отказ поддерживающей инфраструктуры (нарушение работы систем связи, электропитания, разрушение и повреждение помещений)	ПК-3

15.	a) b) c) d)	Перечислите основания для принятия решения об отмене действия сертификата соответствия: a) невозможность устранения заявителем выявленных несоответствий и их причин b) отказ заявителя от проведения инспекционного контроля c) ликвидация организации заявителя и (или) изготовителя либо снятие по инициативе заявителя продукции с серийного производства d) получение решения органа государственного контроля (надзора), национального органа по аккредитации о необходимости прекращения действия сертификата соответствия e) выявление фактов несоответствия продукции, документации к ней обязательным требованиям f) непредставление заявителем в орган государственного контроля (надзора) информации об исполнении решения органа государственного контроля (надзора)	ПК-3
16.	Пропускной режим	Основные элементы системы организации какого режима перечислены далее: структурное подразделение по защите государственной (коммерческой) тайны (режимно-секретное подразделение); служба безопасности предприятия; бюро пропусков; контрольно-пропускные пункты	ПК-3
17.	a) b) c) d) e)	Основные элементы системы организации пропускного режима: a) структурное подразделение по защите государственной (коммерческой) тайны (режимно-секретное подразделение) b) служба безопасности предприятия c) бюро пропусков d) контрольно-пропускные пункты e) самостоятельные структурные подразделения, использующие высокоэффективные средства защиты информации f) служба финансового контроля	ПК-3
18.	Гражданско-правовой и уголовный характер	Какой характер ответственности одновременно может носить правонарушение, которое обнаружили работники службы безопасности со стороны других лиц?	ПК-3
19.	Пропускной режим	Совокупность правил, регламентирующих порядок входа (выхода) физических лиц, въезда (выезда) транспортных средств на режимный объект, вноса (выноса),	ПК-3

		ввоза (вывоза) документов и вещей, а также совокупность мероприятий по реализации этих правил – это?	
20.	Системы охраны периметра	К каким системам относят Радиолучевые системы, Радиоволновые системы, Инфракрасные системы, Оптоволоконные системы, Емкостные системы, Вибрационные системы, Вибрационно-сейсмические системы, Системы активной охраны?	ПК-3
21.	a) b)	Перечислите виды контрольно-учетных мероприятий a) Пропускной режим b) Внутриобъектовый режим c) Правовой режим d) Инженерно-технический режим e) Организационный режим f) Стратегический режим	ПК-3
22.	a)	Специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе a) правовая защита b) инженерно-техническая защита c) организационная защита d) стратегическое прогнозирование	ПК-3
23.	a) b) c) d)	Какие существуют основные уровни обеспечения защиты информации? a) Законодательный b) Организационно-административный c) Программно-технический (аппаратный) d) Физический e) Вероятностный f) Распределительный	ПК-3
24.	a)	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации называются: a) Государственная тайна b) Профессиональная тайна c) Тайна следствия и судопроизводства	ПК-3

		d) Коммерческая тайна	
25.	Электронная цифровая подпись	Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе?	ПК-3
26.	b)	Защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов называется a) Государственная тайна b) Банковская тайна c) Тайна следствия и судопроизводства d) Коммерческая тайна	ПК-3
27.	a)	Что такое закрытый ключ электронной цифровой подписи? a) Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи. b) Ключ электронной цифровой подписи, который зашифрован с помощью единственного симметричного ключа владельца c) Ключ электронной цифровой подписи, который хранится отдельно от других закрытый ключей d) Ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца	ПК-3
28.	c)	Деяния, предусмотренные частями первой или второй ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения a) до 300 тыс.рублей b) до 200 тыс.рублей c) до 500 тыс.рублей	ПК-3
29.	c)	Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования	ПК-3

		компьютерной информации или нейтрализации средств защиты компьютерной информации наказывается ограничение свободы a) до 2-х лет b) до 3-х лет c) до 4-х лет	
30.	b)	Деяние, предусмотренное частью первой ст.274 УК РФ, если оно повлекло тяжкие последствия или создало угрозу их наступления наказывается принудительными работами на срок a) до 2-х лет b) до 5-х лет c) до 4-х лет	ПК-3
31.	a)	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, наказывается исправительными работами на срок. a) до 1 года b) до 6 месяцев c) до 18 месяцев	ПК-3
32.	показатели защищенности СВТ от НСД	Дискреционный принцип контроля доступа; Мандатный принцип контроля доступа; Очистка памяти; Изоляция модулей; Маркировка документов; Защита ввода и вывода на отчуждаемый физический носитель информации; Сопоставление пользователя с устройством; Идентификация и аутентификация; Гарантии проектирования; Регистрация; Взаимодействие пользователя с КСЗ; Надежное восстановление; Целостность КСЗ; Контроль модификации; Контроль дистрибуции; Гарантии архитектуры; Тестирование; Руководство для пользователя; Руководство по КСЗ; Тестовая документация; Конструкторская (проектная) документация –это	ПК-3
33.	c)	Физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации	ПК-3

		a) Преступник b) Правонарушитель c) Потерпевший	
34.	c)	Деяния, предусмотренные частями первой, второй или третьей ст. 272 УК РФ, если они повлекли тяжкие последствия или создали угрозу их наступления a) наказываются лишением свободы на срок до пяти лет. b) наказываются лишением свободы на срок до пяти лет. c) наказываются лишением свободы на срок до семи лет	ПК-3
35.	a)	Деяние, предусмотренное частью первой ст. 274 УК РФ, если оно повлекло тяжкие последствия или создало угрозу их наступления, наказывается a) принудительными работами на срок до пяти лет либо лишением свободы на тот же срок b) принудительными работами на срок до четырех лет либо лишением свободы на тот же срок c) принудительными работами на срок до двух лет либо лишением свободы на тот же срок.	ПК-3
36.	c)	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается a) ограничением свободы на срок до четырех лет b) ограничением свободы на срок до трех лет c) ограничением свободы на срок до двух лет	ПК-3
37.	a)	Деяния, предусмотренные частями первой или второй ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, наказывается a) ограничением свободы на срок до четырех лет b) ограничением свободы на срок до трех лет c) ограничением свободы на срок до пяти лет	ПК-3
38.	a)	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее	ПК-3

		уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, наказывается a) штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев b) штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев c) штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев	
39.	a)	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или совершенное из корыстной заинтересованности, наказывается a) исправительными работами на срок от одного года до двух лет b) исправительными работами на срок до двух лет c) исправительными работами на срок от 6 месяцев до года	ПК-3
40.	a) b) c)	По УК РФ преступлениями в сфере компьютерной информации являются: a) неправомерный доступ к компьютерной информации b) создание, использование и распространение вредоносных компьютерных программ c) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации d) кража компьютера из офиса e) сломать кредитную карту	ПК-3
41.	a)	Формы защиты интеллектуальной собственности a) авторское, патентное право и коммерческая тайна b) интеллектуальное право и смежные права c) коммерческая и государственная тайна d) гражданское и административное право e) авторское, патентное право и коммерческая тайна	ПК-3
42.	a) b) c) d)	Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности a) уголовная b) административно-правовая	ПК-3

		c) гражданско-правовая d) дисциплинарная e) материальная f) условная g) договорная	
43.	a) b) c)	Какие действия являются реагированием на нарушение режима информационной безопасности организации? a) Локализация и уменьшение вреда b) Выявление нарушителя c) Предупреждение повторных нарушений d) Судебное рассмотрение e) Проведение общего собрания организации	ПК-3
44.	a)	Классификация и виды информационных ресурсов определены a) Законом "Об информации, информатизации и защите информации" b) Гражданским кодексом c) Конституцией d) всеми документами, перечисленными в остальных пунктах	ПК-3
45.	a)	Что такое сертификация? a) Подтверждение соответствия продукции или услуг установленным требованиям или стандартам b) Процесс подготовки к изготовлению программно-технических средств защиты информации c) Документы, по которым происходит процесс засекречивания программно-технических средств d) Административное управление информационной безопасностью e) Подтверждение соответствия продукции или услуг установленным требованиям или стандартам	ПК-3
46.	a)	Задание 3.2.1 Что такое лицензия? a) Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю	ПК-3

		b) Перечень документов, которыми организация пользуется для засекречивания информации c) Осуществление любых видов деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю d) Разрешение на осуществление любого вида деятельности выданное юридическому лицу или индивидуальному предпринимателю e) Документы, подтверждающие уровень защиты информации	
47.		Студент 5-го курса технического ВУЗа Бреньков А. написал в рамках курсовой работы компьютерную программу «TEST PO PO», позволяющую проводить тестирование остаточных знаний по ряду дисциплин: 1. Назовите объекты и субъекты авторского права. 2. Кому принадлежат личные неимущественные и исключительные права на данное программное обеспечение (ПО)?	ПК-3
48.		Индивидуальный предприниматель Берекова А.А. умер. Он являлся единоличным автором двух программных продуктов «XXX» и «HHH», которые пользовались большим спросом на рынке ПО в области игровых программ. При жизни Берекова А.А. не передавал права на данные программные продукты, у него нет наследников и он не оставил завещания: 1. Кому после смерти Берекова А.А. перейдут личные неимущественные и исключительные права на данные программные продукты? 2. Каковы сроки действия этих прав на указанное ПО?	ПК-3
49.		Программисты Оберезко и Гусаров фирмы «Переход» в рамках своих трудовых обязанностей по заданию работодателя создали программный комплекс «JKYT». 1. Кто является автором данного ПО? 2. Кому принадлежат личные неимущественные и исключительные права?	ПК-3
50.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 149)	ПК-3

51.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 126 (выбираем субъектов из статей: 3-24))	ПК-3
52.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 152)	ПК-3
53.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 5485-1)	ПК-3
54.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 98)	ПК-3
55.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 126 (выбираем субъектов из статей: 25-49))	ПК-3

56.		Составить перечень субъектов правовых отношений, привести закрепленное законодательно определение. Указать правосубъектность одного из субъектов правовых отношений. Провести анализ правового статуса одного из субъектов. Необходимо указать отдельно права субъекта. Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей (ФЗ РФ № 126 (выбираем субъектов из статей: 50-74))	ПК-3

2. Описание шкалы оценивания

Оценка «отлично» выставляется обучающемуся, если студент продемонстрировал высокое умение применять полученные знания на практике черезрешение конкретного задания, свободно без затруднений справился с поставленным заданием, показав владение разносторонними приемами и навыками его выполнения,не допустил ошибок и неточностей.

Оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал умение применять полученные знания на практике через решение конкретного задания, справился с поставленным заданием, показав владение необходимыми приемами и навыками его выполнения, при этом допустил не более одной ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретного задания, с трудом справился с поставленным заданием, при этом допустил не более двух ошибок

Оценка «неудовлетворительно» выставляется обучающемуся, если студент не продемонстрировал умение применять полученные знания на практике через решениеконкретного задания, не справился с поставленным заданием или допустил при его решении три и более серьезные ошибки.

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он уверенно разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности; самостоятельно проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «хорошо» выставляется студенту, если он умеет разрабатывать проекты организационно-распорядительной документации по обеспечению информационной безопасности; хорошо проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «удовлетворительно» выставляется студенту, если он частично разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности; плохо проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Оценка «неудовлетворительно» выставляется студенту, если он не умеет разрабатывать проекты организационно-распорядительной документации по обеспечению информационной безопасности; не проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности