Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.12 Управление кадровой безопасностью организации и государственной службы

(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.03 Управление персоналом
(код, наименование направления подготовки)

Управление персоналом организаций и государственной службы
(наименование образовательной программы)

очная форма обучения
(форма обучения)

Год набора – 2026

Донецк

Автор-составитель РПД:

Казанцева Лариса Сергеевна, кандидат наук, доцент, доцент кафедры управления персоналом и экономики труда

Заведующий кафедрой:

Стадник Алла Мироновна, канд. наук по гос. управлению, заведующий кафедрой управления персоналом и экономики труда

Рабочая программа дисциплины *Б1.В.01.12 Управление кадровой безопасностью организации и государственной службы* одобрена на заседании кафедры управления персоналом и экономики труда Донецкого филиала РАНХиГС

протокол № 7 от «04» марта 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели и критерии оценивания
5. Формы аттестации и типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам
6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине
7. Методические материалы по освоению дисциплины
8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»
9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина *Б1.В.01.12 Управление кадровой безопасностью организации и государственной службы* обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
B/02.6. Поиск, привлечение, подбор и отбор персонала 07.003 «СПЕЦИАЛИСТ ПО УПРАВЛЕНИЮ ПЕРСОНАЛОМ», утв. Приказом Минтруда и социальной защиты РФ от 09.03.2022 №109н	ПК-1	ПК-1. Способен управлять процессами поиска, подбора и отбора персонала	ПК-1.4.	Проводит отбор, оценку кандидатов и бюджетирование процесса подбора персонала	*ПК-1.4. З-18* ***Знает*** законодательство Российской Федерации о персональных данных *ПК-1.4. У-8* ***Умеет*** обеспечивать соблюдение требований законодательства Российской Федерации и политик работодателя в области обработки персональных данных и конфиденциальной информации

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общий объем дисциплины:

4,00 з.е., 144 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 54 ак.час на контактную работу с преподавателем, из них 28 ак.час на лекции и 28 ак.час на практические занятия. 59 ак.час на самостоятельную работу обучающихся.

Б1.В.01.12 Управление кадровой безопасностью организации и государственной службы реализуется в 7-м семестре на 4-м курсе после изучения дисциплин:

Основы управления персоналом;

Деловая коммуникация и защита персональных данных;

Технологии кадрового рекрутинга.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	КАТТЭК	К	СРКР	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Раздел 1. Правовые и организационные основы кадровой безопасности при подборе персонала															
Тема 1.1	Кадровая безопасность организации как объект управления	13	4	0	0	4	0	0	0	0	0	0	0	5	Опрос, доклад тестирование,
Тема 1.2	Кадровая безопасность в процессе подбора персонала: угрозы на этапах привлечения, отбора, оценки, принятия решения	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, тестирование, ситуационное задание
Тема 1.3	Нормативно-правовая база обработки персональных	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад

	данных кандидатов и сотрудников														
Тема 1.4	Конфиденциальная информация в рекрутинге	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, Доклад, тестирование
Раздел 2. Обеспечение соблюдения законодательства и политик работодателя при отборе персонала															
Тема 2.1	Политика работодателя в области обработки персональных данных кандидатов: разработка, внедрение в процессы управления персоналом	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад, тестирование
Тема 2.2	Согласие на обработку персональных данных: формы для разных этапов	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад, тестирование
Тема 2.3	Разграничение полномочий при доступе к персональным данным в процессе отбора персонала	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад, ситуационное задание
Тема 2.4	Документирование процедур отбора с соблюдением режима защиты персональных данных	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад
Раздел 3. Специфика кадровой безопасности на государственной службе															

Тема 3.1	Особенности отбора на государственную гражданскую службу	8	2	0	0	2	0	0	0	0	0	0	0	4	Опрос, доклад
Тема 3.2	Корпоративная культура кадровой безопасности	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад
Тема 3.3	Управление рисками кадровой безопасности в процессе отбора	9	2	0	0	2	0	0	0	0	0	0	0	5	Опрос, доклад, тестирование
Тема 3.4	Противодействие угрозам информационной и имущественной безопасности организации со стороны собственного персонала	13	4	0	0	4	0	0	0	0	0	0	0	5	Опрос, доклад, тестирование, ситуационное задание
Промежуточная аттестация		29	0	0	0	0	0	0	2	9	0	0	18	0	Экзамен
Итого		144	28	0	0	28	0	0	2	9	0	0	18	59	

ВЛ – видео лекции.
ЛР – лабораторные работы.
ПЗ – практические занятия (за исключением лабораторных работ).
ИК – индивидуальные консультации.
КСР – контроль самостоятельной работы
КЭ – консультации перед экзаменом
Каттэк – контактная работа на аттестацию в период экзаменационных сессий
СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.
СРэк – самостоятельная работа на подготовку к экзамену.
СР – самостоятельная работа в семестре на подготовку к учебным занятиям

3.2. Содержание дисциплины

Раздел 1. Правовые и организационные основы кадровой безопасности при подборе персонала

Тема 1.1. Кадровая безопасность организации как объект управления. ПК-1.4.

Сущность кадровой безопасности. Роль и место кадровой безопасности в системе управления персоналом. Цель и основные элементы кадровой безопасности организации. Классификация возможных угроз кадровой безопасности по признакам: целевой направленности; характеру потерь от реализованных угроз; источнику угрозы; вероятности практической реализации угрозы. Классификация методов противодействия возможным угрозам кадровой безопасности организации по признакам: времени реализации, характеру действия, степени легитимности. Отраслевая специфика обеспечения кадровой безопасности организаций.

Тема 1.2. Кадровая безопасность в процессе подбора персонала: угрозы на этапах привлечения, отбора, оценки, принятия решения. ПК-1.4.

Угрозы, возникающие на каждом этапе привлечения, отбора, оценки и найма кандидатов, включая риски утечки персональных данных соискателей, несанкционированный доступ к конфиденциальной информации (резюме, рекомендации, результаты тестирования) со стороны недобросовестных рекрутеров или третьих лиц, а также нарушение законодательства о персональных данных при сборе, хранении и передаче сведений о кандидатах без их согласия. Типовые сценарии инцидентов кадровой безопасности в рекрутинге и организационно-правовые меры их предотвращения. Требования законодательства РФ, соблюдение которых не только защищает права соискателей, но и минимизирует репутационные и финансовые риски работодателя.

Тема 1.3. Нормативно-правовая база обработки персональных данных кандидатов и сотрудников. ПК-1.4.

Система законодательных актов РФ, регулирующих сбор, хранение и защиту персональных данных в кадровой сфере (ФЗ № 152-ФЗ «О персональных данных» и ст. 86–90 Трудового кодекса РФ, которые устанавливают принципы законности, согласия субъекта и конфиденциальности. Подзаконные акты (Постановление Правительства № 687, требования Роскомнадзора) и специальные положения для государственной службы (ФЗ о госслужбе, антикоррупционное законодательство). Ответственность за нарушения – административной (ст. 13.11 КоАП РФ), дисциплинарной и гражданско-правовой, что позволяет HR-специалисту выстраивать кадровые процессы в строгом соответствии с правовым полем.

Тема 1.4. Конфиденциальная информация в рекрутинге. ПК-1.4.

Различия между коммерческой тайной работодателя (методики оценки, базы кандидатов), служебной тайной и конфиденциальной информацией самого соискателя, включая результаты психологического тестирования, биометрические данные (при добровольном предоставлении), а также сведения о семейном положении, национальности или состоянии здоровья, если они стали известны в ходе собеседования. Обязанности специалиста кадровой службы по ограничению доступа к таким сведениям, получению отдельного согласия на обработку специальных категорий персональных данных, недопустимости передачи конфиденциальной информации третьим лицам (в том числе внутренним заказчикам без служебной необходимости). Анализ типовых нарушений в рекрутинге: неконтролируемое распространение анкет кандидатов в мессенджерах, хранение оценочных листов в открытом доступе, использование внешних сервисов без оценки их соответствия законодательству о защите информации. Алгоритм работы с конфиденциальными данными соискателя на всех этапах отбора — от получения до уничтожения после закрытия вакансии или истечения сроков хранения.

Раздел 2. Обеспечение соблюдения законодательства и политик работодателя при отборе персонала

Тема 2.1. Политика работодателя в области обработки персональных данных кандидатов: разработка, внедрение в процессы управления персоналом. ПК-1.4.

Обязательные требования к разработке и внедрению политики обработки персональных данных кандидатов согласно 152-ФЗ. Ключевые элементы политики (цели, перечень данных, сроки хранения, порядок уничтожения), этапы её внедрения в HR-процессы (сбор информированного согласия, разграничение доступа, автоматизация хранения) и типовые риски, включая штрафы.

Тема 2.2. Согласие на обработку персональных данных: формы для разных этапов. ПК-1.4.

Правовые и организационные аспекты получения согласия субъекта персональных данных (ПДн) в зависимости от этапа взаимодействия с работодателем: от первичного контакта с кандидатом до увольнения сотрудника и последующего архивного хранения. Требования Федерального закона № 152-ФЗ к форме, содержанию и срокам действия согласия, а также отличия в объёме обрабатываемых данных для разных целей (отбор, проверка службы безопасности, передача данных аутсорсеру, включение в кадровый резерв). Шаблоны и формулировки для ситуаций: согласие на

обработку ПДн при направлении резюме, согласие на проведение дополнительных проверок (в том числе сведений о судимости), согласие на передачу данных бывшему работодателю для получения рекомендации, а также порядок отзыва согласия и уничтожения данных. Нюансы работы с кандидатами на государственную службу (сведения о доходах супруга) и обработке специальных категорий ПДн (биометрия, состояние здоровья).

Тема 2.3. Разграничение полномочий при доступе к персональным данным в процессе отбора персонала

Принципы и механизмы ограничения доступа к персональным данным (ПДн) кандидатов в зависимости от должностных обязанностей сотрудников, участвующих в отборе. Принцип «служебной необходимости». Способы документального закрепления разграничения: перечни должностей с правом доступа, журналы учёта обращений, запрет на копирование и передачу данных через открытые каналы. Типовые нарушения (предоставление доступа сотрудникам, не участвующим в отборе, передача анкет в мессенджерах) и ответственности за превышение полномочий (дисциплинарная, вплоть до увольнения). Алгоритм построения системы контролируемого доступа, обеспечивающей соблюдение ФЗ-152 и внутренних политик работодателя.

Тема 2.4. Документирование процедур отбора с соблюдением режима защиты персональных данных

Порядок организации документооборота в процессе подбора персонала, обеспечивающего защиту персональных данных (ПДн) кандидатов на всех этапах: от получения резюме до принятия решения о найме или отказа. Виды документов, содержащих ПДн соискателей (анкеты, резюме, оценочные листы, заключения службы безопасности), требования к их оформлению (гриф «Конфиденциально», регистрация в журналах учёта), хранению (сейфы, защищённые электронные папки с разграничением доступа), передаче (только по служебной необходимости под подпись) и уничтожению (по акту после закрытия вакансии или истечения срока хранения). Алгоритм построения системы кадрового делопроизводства, исключающей утечки и нарушения прав субъектов ПДн.

Раздел 3. Специфика кадровой безопасности на государственной службе

Тема 3.1. Особенности отбора на государственную гражданскую службу. ПК-1.4.

Специфика процедур подбора кандидатов на государственную гражданскую службу, обусловленную повышенными требованиями к кадровой безопасности, антикоррупционной защищённости и контролю за

достоверностью персональных данных. Правовые основы: Федеральный закон «О государственной гражданской службе РФ» (ст. 26, 27), антикоррупционное законодательство, а также нормы о допуске к государственной тайне и проверке достоверности иных персональных данных. Дополнительные меры кадровой безопасности: обязательное получение согласия на обработку ПДн в расширенном объёме (включая данные о родственниках, судимостях, выездах за рубеж), взаимодействие с правоохранительными органами и спецслужбами при проведении проверочных мероприятий, а также ограничения, связанные с близким родством. Типовые риски нарушения законодательства о персональных данных при отборе.

Тема 3.2. Корпоративная культура кадровой безопасности. ПК-1.4.

Тема посвящена формированию устойчивого безопасного поведения HR-специалистов и рекрутеров как ключевому фактору предотвращения утечек персональных данных и нарушений законодательства в процессе подбора персонала. Элементы корпоративной культуры кадровой безопасности: обязательное обучение работников, имеющих доступ к персональным данным кандидатов, разработка внутренних памяток и стандартов работы с конфиденциальной информацией, а также механизмы мотивации соблюдения политик. Внутренний контроль как непрерывный процесс: регулярные аудиты действий рекрутеров (проверка журналов доступа, обоснованности передачи данных, соблюдения сроков уничтожения), анонимные опросы о культуре безопасности, тестирование сотрудников.

Тема 3.3. Управление рисками кадровой безопасности в процессе отбора. ПК-1.4.

Понятие риска применительно к обработке персональных данных (ПДн) и конфиденциальной информации кандидатов. Методы идентификации рисков и подходы к их оценке по двум критериям — вероятность наступления и тяжесть последствий. Матрица рисков для рекрутинга и меры их минимизации: организационные, правовые (и технические. Агоритм действий при обнаружении утечки базы кандидатов или нарушении их прав.

Тема 3.4. Противодействие угрозам информационной и имущественной безопасности организации со стороны собственного персонала. ПК-1.4.

Субъекты и формы реализации угроз информационной и имущественной безопасности Комплекс мер, направленных на выявление, предотвращение и нейтрализацию внутренних угроз, исходящих от

сотрудников организации, которые могут нанести ущерб информационной или имущественной безопасности.

Организационно-правовые методы противодействия угрозам информационной и имущественной безопасности организации.

Технические средства защиты и психологические аспекты противодействия угрозам информационной и имущественной безопасности организации.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине *Б1.В.01.12 Управление кадровой безопасности организации и государственной службы* входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа – это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа.	Ответ считается верным, если правильно указана вся последовательность цифр

		3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
90-100	Отлично	Зачтено	A	P/ Passed
80-89	Хорошо		B	P/ Passed
75-79			C	P/ Passed
70-74	Удовлетворительно		B	P/ Passed
60-69			E	P/ Passed
0-59	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
100 баллов	100 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины *Б1.В.01.12 Управление кадровой безопасностью организации и государственной службы* используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

опрос, доклад, тестирование, контрольные задания (ситуационные).

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Раздел 1. Правовые и организационные основы кадровой безопасности при подборе персонала

Тема 1.1. Кадровая безопасность организации как объект управления. ПК-1.4.

Вопросы для опроса:

1. Дайте определение кадровой безопасности организации. В чем ее отличие от общей безопасности предприятия?
2. Назовите основные цели и задачи системы кадровой безопасности.
3. Какое место занимает кадровая безопасность в общей структуре экономической, информационной и организационной безопасности?
4. Перечислите внутренние угрозы кадровой безопасности. Приведите примеры.

Темы для доклада:

1. Эволюция подходов к управлению кадровой безопасностью: от защиты секретов к управлению рисками человеческого капитала.
2. Модели интеграции кадровой безопасности в систему корпоративного управления: служба безопасности, служба управления персоналом.
3. Кадровая безопасность как объект стратегического управления: взаимосвязь с кадровой политикой и брендом работодателя.

Тестовые задания:

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Кадровая безопасность организации как объект управления представляет собой:

А) процесс обеспечения охраны труда и техники безопасности на рабочих местах

Б) систему защиты экономических интересов организации от угроз, связанных с персоналом, его действиями и информацией, которой он обладает

В) совокупность мероприятий по подбору и расстановке кадров

Г) исключительно правовой механизм защиты персональных данных работников

Что из перечисленного относится к внешним угрозам кадровой безопасности организации?

А) увольнение ключевого сотрудника к конкуренту

Б) разглашение работником коммерческой тайны по неосторожности

В) переманивание (хедхантинг) ценных специалистов конкурирующей компанией

Г) саботаж со стороны недовольного работника

Какой принцип управления кадровой безопасностью предполагает разграничение прав доступа сотрудников к конфиденциальной информации в зависимости от их должностных обязанностей?

А) принцип законности

Б) принцип служебной необходимости

В) принцип неотвратимости ответственности

Г) принцип непрерывности

Тест 2.

Прочитайте текст и установите соответствие. Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите соответствие между видом угрозы кадровой безопасности и ее конкретным проявлением. Каждому пункту левого столбца соответствует один правильный пункт правого.

№	Виды угроз	№	Проявление
1	Внутренняя умышленная угроза	А	Сотрудник случайно отправил конфиденциальный документ на личную почту, не зная правил
2	Внутренняя неумышленная (случайная) угроза	Б	Конкуренты разместили фальшивые вакансии с целью сбора резюме сотрудников организации
3	Внешняя угроза	В	Увольняющийся программист скопировал базу клиентов перед уходом
4	Комбинированная угроза (внешне-внутренняя)	Г	Работник за вознаграждение передал постороннему лицу пароли доступа к внутренней системе

Тема 1.2. Кадровая безопасность в процессе подбора персонала: угрозы на этапах привлечения, отбора, оценки, принятия решения. ПК-1.4.

Вопросы для опроса.

1 Какие угрозы кадровой безопасности характерны для этапа привлечения кандидатов (размещение вакансий, обработка входящих резюме)?

2. Охарактеризуйте угрозы, возникающие на этапе отбора (скрининг резюме, телефонное интервью, первичное собеседование). Приведите конкретные примеры.

3. Какие угрозы возникают на этапе принятия решения о найме и оформления кандидата на работу? Назовите не менее трёх.

Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

На этапе привлечения кандидатов (размещение вакансии на сайте-агрегаторе) угрозой кадровой безопасности является:

А) низкий отклик на вакансию из-за неправильного описания требований

Б) сбор резюме конкурентами под видом соискателей для анализа штатного расписания

В) превышение бюджета на публикацию вакансии

Г) неверное оформление трудового договора с кандидатом

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранных вариантов ответа.

Какие угрозы кадровой безопасности характерны для этапа привлечения кандидатов (размещение вакансий, сбор резюме)?

А) размещение фальшивых вакансий конкурентами с целью сбора резюме ценных специалистов

Б) утечка персональных данных соискателей через незащищённые формы сбора резюме на сайте

В) неверное определение KPI рекрутера по скорости закрытия вакансии

Г) перехват откликов кандидатов третьими лицами при использовании открытых каналов связи (например, электронной почты без шифрования)

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность действий HR-специалиста при работе с персональными данными кандидата с момента получения резюме до завершения отбора (с точки зрения обеспечения кадровой безопасности).

А) Получение письменного согласия кандидата на обработку персональных данных в целях отбора

Б) Предоставление доступа к персональным данным кандидата только тем сотрудникам, для которых это необходимо по должностным обязанностям (принцип служебной необходимости)

В) Уничтожение персональных данных кандидата (или передача их на архивное хранение по отдельному соглашению) после завершения отбора и истечения срока хранения

Г) Получение и первичная обработка резюме кандидата с фиксацией в журнале учёта

Расположите в правильном порядке действия HR-специалиста и службы безопасности при обнаружении факта несанкционированной передачи персональных данных кандидатов третьим лицам в процессе отбора персонала.

А) Уведомление Роскомнадзора (в случае, если инцидент относится к категории значимых утечек персональных данных)

Б) Фиксация факта инцидента (составление акта, скриншоты, логи доступа)

В) Временное отстранение сотрудника, подозреваемого в нарушении, от работы с персональными данными (с сохранением заработной платы на период проверки)

Г) Проведение внутреннего служебного расследования (опросы, анализ систебм безопасности, проверка цепочки передачи данных)

Ситуационные задания

Задание 1.

Прочитайте текст и запишите развернутый обоснованный ответ.

«Вы руководитель отдела подбора персонала. На этапе оценки кандидата на должность финансового директора рекрутер без согласия соискателя направил его резюме, паспортные данные и результаты психологического тестирования в службу безопасности и в бухгалтерию «для проверки». При этом руководитель бухгалтерии переслал эти данные на свой личный ноутбук».

Вопросы к ситуации:

1. Какие угрозы кадровой безопасности возникли на этапе оценки и принятия решения?
2. Какие статьи законодательства о персональных данных нарушены?
3. Какие организационные меры вы предложите, чтобы исключить повторение такого инцидента в будущем?

Тема 1.3. Нормативно-правовая база обработки персональных данных кандидатов и сотрудников. ПК-1.4.

Вопросы для опроса:

1. Какие федеральные законы Российской Федерации составляют основу правового регулирования обработки персональных данных кандидатов и сотрудников? Назовите не менее трёх и кратко охарактеризуйте предмет каждого.
2. Какие требования к обработке персональных данных работника закреплены в статьях 86–90 Трудового кодекса РФ?
3. Каковы основные принципы обработки персональных данных, установленные статьёй 5 Федерального закона № 152-ФЗ? Как они применяются в отношении кандидатов при трудоустройстве?

Темы для доклада:

1. Сравнительный анализ ФЗ-152 «О персональных данных» и статей 86–90 Трудового кодекса РФ: общее и особенное в регулировании обработки ПДн работников и кандидатов
2. Постановление Правительства РФ № 687: требования к обработке персональных данных на бумажных носителях и их значение для кадрового делопроизводства

Тема 1.4. Конфиденциальная информация в рекрутинге. ПК-1.4.

Вопросы для опроса:

1. Что понимается под конфиденциальной информацией в рекрутинге?
2. Чем конфиденциальная информация о кандидате отличается от персональных данных в понимании ФЗ-152?
3. Какие виды конфиденциальной информации, получаемой в процессе рекрутинга, могут относиться к коммерческой тайне работодателя?

4. Может ли работодатель без согласия кандидата передавать его резюме и результаты тестирования внутренним заказчикам (руководителям подразделений)? Почему?

Темы для доклада:

1. Понятие и виды конфиденциальной информации о кандидате: от персональных данных до коммерческой тайны работодателя
2. Правовые последствия разглашения конфиденциальной информации о кандидате: административная, дисциплинарная и гражданско-правовая ответственность

Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Что из перечисленного относится к конфиденциальной информации о кандидате, полученной в процессе рекрутинга, и подлежит защите?

А) ФИО кандидата, указанное в резюме, размещённом на открытом сайте-агрегаторе

Б) результаты психологического тестирования, проведённого работодателем, с пометкой «конфиденциально»

В) информация о вакансии, опубликованная на официальном сайте компании

Г) название должности, на которую претендует кандидат

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранных вариантов ответа.

Какие из перечисленных сведений о кандидате, полученные в процессе рекрутинга, относятся к конфиденциальной информации и требуют особой защиты? (выбрать все верные ответы)

А) фамилия, имя, отчество кандидата, указанные в открытом резюме на сайте по поиску работы

Б) аудиозапись собеседования с кандидатом (без его письменного согласия)

В) результаты проверки службы безопасности, содержащие выводы о возможной неблагонадежности кандидата

Г) информация о профессиональных навыках, добровольно переданная кандидатом на собеседовании

Тест 3.

Прочитайте текст и установите соответствие. Установите соответствие между действием рекрутера (левый столбец) и его последствием с точки зрения защиты конфиденциальной информации (правый столбец). Каждому действию соответствует одно последствие.

№	Действие рекрутера	№	Последствие / характеристика
1	Передача резюме кандидата руководителю через корпоративную защищённую почту после получения согласия	А	Нарушение режима конфиденциальности, риск утечки через мессенджер
2	Хранение оценочных листов кандидатов в открытой облачной папке (Yandex Диск) без пароля	Б	Прямое нарушение ФЗ-152 и принципа конфиденциальности, административная ответственность
3	Отправка аудиозаписи собеседования с кандидатом в Telegram-чат отдела подбора без согласия кандидата	В	Правомерное действие, соответствующее законодательству и политикам (при наличии закреплённой процедуры уничтожения)
4	Уничтожение анкет непрошедших кандидатов по акту по истечении срока хранения	Г	Правомерное действие, соответствующее законодательству и политикам

Раздел 2. Обеспечение соблюдения законодательства и политик работодателя при отборе персонала

Тема 2.1. Политика работодателя в области обработки персональных данных кандидатов: разработка, внедрение в процессы управления персоналом. ПК-1.4.

Вопросы для опроса:

1. Что такое политика обработки персональных данных (ПДн) кандидатов и чем она отличается от аналогичной политики для сотрудников?
2. Какие нормативные требования (ФЗ-152, ТК РФ, подзаконные акты) необходимо учитывать при разработке политики в отношении кандидатов?
3. Какие обязательные разделы должна содержать политика обработки ПДн кандидатов? Назовите не менее четырёх.
4. В чём заключается принцип «целевого использования» ПДн кандидата и как он отражается в тексте политики?

Доклады

1. Структура и содержание политики обработки персональных данных кандидатов: обязательные разделы в соответствии с требованиями Роскомнадзора
2. Принципы законности и соразмерности при сборе персональных данных кандидата: как отразить их в политике
3. Согласие кандидата на обработку персональных данных: формы, сроки, порядок отзыва – рекомендации для включения в политику

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Какой раздел является обязательным для включения в Политику обработки персональных данных кандидатов в соответствии с требованиями Роскомнадзора?

А) Порядок материального поощрения кандидатов за предоставление дополнительных данных

Б) Категории обрабатываемых персональных данных кандидатов и цели их обработки

В) Описание процедуры проведения ассессмент-центра для кандидатов

Г) График отпусков сотрудников кадровой службы

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранных вариантов ответа.

Какие из перечисленных положений обязательно должны быть включены в Политику обработки персональных данных кандидатов в соответствии с требованиями ФЗ-152 и рекомендациями Роскомнадзора?

А) перечень категорий персональных данных кандидатов, которые обрабатываются работодателем

Б) порядок оплаты труда рекрутеров за успешное закрытие вакансий

В) цели обработки персональных данных кандидатов (например, отбор на вакансию, формирование кадрового резерва)

Г) сроки хранения и порядок уничтожения персональных данных кандидатов

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность шагов при разработке и утверждении Политики обработки персональных данных кандидатов в организации.

Варианты ответов (порядок действий):

А) Утверждение Политики руководителем организации (издание приказа)

Б) Назначение ответственного за организацию обработки персональных данных

В) Анализ требований ФЗ-152, ТК РФ и подзаконных актов к содержанию Политики

Г) Разработка проекта Политики (структура, разделы, формулировки)

Тема 2.2. Согласие на обработку персональных данных: формы для разных этапов. ПК-1.4.

Вопросы для опроса:

1. Что такое согласие на обработку персональных данных (ПДн) с точки зрения ФЗ-152? В чем его правовая природа?

2. В каких случаях обработка ПДн кандидата или сотрудника возможна без получения согласия? Назовите не менее двух исключений.

3. Какие обязательные элементы должно содержать письменное согласие на обработку ПДн (согласно ст. 9 ФЗ-152)?

4. Чем отличается форма согласия для кандидата (на этапе отбора) от формы согласия для уже принятого сотрудника (в рамках трудового договора)?

Темы для доклада:

1. Правовая природа согласия на обработку ПДн: требования ст. 9 ФЗ-152 и последствия отсутствия согласия
2. Обязательные элементы письменного согласия на обработку ПДн: структура, формулировки, реквизиты
3. Сравнительный анализ формы согласия для кандидата (этап отбора) и для сотрудника (в рамках трудового договора)

Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

В соответствии со ст. 9 Федерального закона № 152-ФЗ, обязанность получить письменное согласие на обработку персональных данных возникает в случае:

А) обработки ПДн в рамках трудового договора, необходимой для начисления заработной платы

Б) обработки специальных категорий ПДн (о судимости, биометрии) и передачи данных третьим лицам

В) обработки общедоступных ПДн кандидата из открытого резюме на сайте-агрегаторе

Г) обработки ПДн государственного служащего в рамках проверки достоверности сведений о доходах

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ. Обосновать свой выбор

Записать букву выбранного варианта и кратко обосновать свой выбор.

Рекрутер получил резюме кандидата с сайта по поиску работы. На сайте была галочка «Я согласен на обработку моих персональных данных». Должен ли рекрутер дополнительно получить от кандидата отдельное письменное согласие на обработку ПДн для целей конкретной вакансии в организации?

Варианты ответа:

А) Нет, достаточно галочки на сайте-агрегаторе, так как это уже письменное согласие в электронной форме.

Б) Да, необходимо получить отдельное письменное согласие (в том числе в форме электронного документа) с указанием конкретного оператора и целей обработки, если сайт-агрегатор не является оператором.

В) Да, но только если кандидат запрашивает ознакомление с Политикой.

Г) Нет, согласие не требуется, так как резюме является общедоступной информацией.

Тест 3

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность действий рекрутера при получении согласия на обработку персональных данных от кандидата на этапе отбора.

Варианты ответов (порядок действий):

А) Получение подписанного кандидатом бланка согласия (на бумаге или в электронной форме)

Б) Предоставление кандидату для ознакомления Политики обработки персональных данных

В) Разъяснение кандидату целей обработки его ПДн (трудоустройство, проверка службы безопасности, формирование резерва)

Г) Начало сбора и обработки ПДн кандидата (резюме, анкета, собеседование)

Тема 2.3. Разграничение полномочий при доступе к персональным данным в процессе отбора персонала

Вопросы для опроса:

1. Что означает принцип «служебной необходимости» применительно к доступу к персональным данным кандидатов?

2. Какие категории сотрудников организации обычно имеют доступ к персональным данным кандидатов в процессе отбора? Назовите не менее трёх.

3. Какой объём персональных данных кандидата вправе получать руководитель подразделения, в котором открыта вакансия?

4. В каком объёме и при каких условиях служба безопасности организации может получить доступ к персональным данным кандидата?

Темы для доклада:

1. Принцип «служебной необходимости» как основа разграничения доступа к ПДн кандидатов: понятие, правовое закрепление, практическая реализация
2. Перечень должностей, имеющих доступ к ПДн кандидатов: порядок разработки, утверждения и актуализации
3. Объёмы доступа к ПДн кандидатов для разных категорий сотрудников (рекрутер, руководитель, служба безопасности, бухгалтерия, юрист)

Ситуационное задание

Задание 1.

Прочитайте текст и запишите развернутый обоснованный ответ.

В компании «Гамма» рекрутер Иванова получила резюме кандидата на должность ведущего инженера. Руководитель IT-отдела (где открыта вакансия) попросил прислать ему резюме и результаты первичного тестирования кандидата. Также к рекрутеру обратился начальник смежного отдела логистики с просьбой «просто посмотреть резюме интересного кандидата, может, себе заберу». Рекрутер передала полные пакеты данных обоим. Служба безопасности узнала об этом и инициировала проверку.

Вопросы к ситуации:

1. Нарушен ли принцип разграничения полномочий? Если да, то в какой части?
2. Какие действия рекрутера были правомерными, а какие – нет?
3. Какие меры необходимо принять организации для предотвращения подобных ситуаций?

Тема 2.4. Документирование процедур отбора с соблюдением режима защиты персональных данных

Вопросы для опроса:

1. Какие документы, содержащие персональные данные кандидатов, создаются на этапах привлечения, отбора, оценки и принятия решения о найме?

2. Какие обязательные реквизиты и пометки (например, гриф «Конфиденциально») должны быть на документах, содержащих ПДн кандидатов?

3. Каков порядок регистрации входящих резюме и анкет кандидатов в журнале учёта? Для чего это необходимо?

4. Как правильно оформить акт об уничтожении персональных данных непрошедшего кандидата? Какие сведения в него вносятся?

Темы для доклада:

1. Виды документов, создаваемых в процессе отбора персонала, и их роль в обеспечении кадровой безопасности
2. Требования к оформлению документов с персональными данными кандидатов: гриф «Конфиденциально», регистрация, реквизиты
3. Журнал учёта кандидатов: структура, порядок ведения, сроки хранения

Раздел 3. Специфика кадровой безопасности на государственной службе

Тема 3.1. Особенности отбора на государственную гражданскую службу. ПК-1.4.

Вопросы для опроса:

1. Какими нормативными правовыми актами регулируется порядок отбора на государственную гражданскую службу? Назовите не менее трёх.
2. В чем отличие процедуры отбора на государственную службу от отбора в коммерческую организацию с точки зрения объёма запрашиваемых персональных данных?
3. Какие сведения о доходах, расходах и имуществе обязан представить кандидат на должность государственной гражданской службы, и касается ли это членов его семьи?
4. Какие дополнительные проверки (помимо стандартной проверки персональных данных) проводятся в отношении кандидатов на государственную службу?

Темы для доклада:

1. Нормативно-правовая основа отбора на государственную гражданскую службу: ФЗ «О государственной гражданской службе РФ», антикоррупционное законодательство, указы Президента

2. Представление сведений о доходах, расходах и имуществе кандидатом и членами его семьи: объём данных, порядок проверки, ответственность за недостоверность

3. Проверка достоверности персональных данных кандидатов на государственную службу: взаимодействие кадровой службы с правоохранительными органами и спецслужбами

Тема 3.2. Корпоративная культура кадровой безопасности. ПК-1.4.

Вопросы для опроса:

1. Дайте определение корпоративной культуры кадровой безопасности. Из каких элементов она состоит?
2. Почему технические и правовые меры защиты персональных данных недостаточны без сформированной культуры безопасности среди персонала?
3. Какие цели преследует формирование корпоративной культуры кадровой безопасности в организации?

Темы для доклада:

1. Понятие и структура корпоративной культуры кадровой безопасности: ценности, нормы, модели поведения
2. Роль топ-менеджмента в формировании культуры кадровой безопасности: личный пример и организационная поддержка
3. Обучение персонала основам кадровой безопасности: программы вводного инструктажа, периодического повышения квалификации, тренинги

Тема 3.3. Управление рисками кадровой безопасности в процессе отбора. ПК-1.4.

Вопросы для опроса:

1. Дайте определение понятию «риск кадровой безопасности» применительно к процессу отбора персонала. Приведите пример риска.
2. Какие основные группы рисков кадровой безопасности возникают на этапах привлечения, отбора, оценки и принятия решения о найме?
3. Что такое идентификация рисков в контексте рекрутинга? Какие методы идентификации вы знаете (мозговой штурм, анализ инцидентов, анкетирование HR-специалистов)?
4. По каким критериям оцениваются выявленные риски (вероятность наступления, тяжесть последствий, возможность обнаружения)?

Темы для доклада:

1. Понятие и классификация рисков кадровой безопасности в рекрутинге: внутренние и внешние, умышленные и непреднамеренные
2. Методы идентификации рисков при отборе персонала: анализ инцидентов, экспертные оценки, анкетирование HR-специалистов
3. Оценка рисков: критерии вероятности и тяжести последствий (финансовые, репутационные, правовые)

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Что из перечисленного относится к организационной мере минимизации риска утечки персональных данных кандидатов?

А) установка системы DLP (Data Loss Prevention) на рабочих станциях рекрутеров

Б) шифрование электронных анкет кандидатов при передаче по корпоративной почте

В) утверждение перечня должностей, имеющих доступ к ПДн кандидатов, и журнала учёта обращений

Г) использование двухфакторной аутентификации для входа в HR-систему

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранных вариантов ответа.

Какие из перечисленных рисков относятся к рискам утечки персональных данных кандидатов на этапе отбора?

А) хранение анкет кандидатов в открытой общей папке на сервере без ограничения доступа

Б) завышение требований к кандидату в вакансии, что снижает количество откликов

В) передача резюме кандидата в мессенджере (Telegram) руководителю подразделения без шифрования

Г) использование личных ноутбуков рекрутерами для обработки ПДн без установленного антивируса и шифрования

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность шагов при выявлении и оценке риска кадровой безопасности, связанного с передачей персональных данных кандидатов через мессенджеры.

А) Оценка тяжести последствий (штрафы, репутационные потери)

Б) Идентификация риска: использование мессенджеров для передачи ПДн кандидатов

В) Оценка вероятности наступления инцидента (например, высокая, средняя, низкая)

Г) Отнесение риска к зоне матрицы (критическая, высокая, средняя, низкая)

Тема 3.4. Противодействие угрозам информационной и имущественной безопасности организации со стороны собственного персонала. ПК-1.4.

Вопросы для опроса:

1. Какие виды угроз информационной безопасности могут исходить от собственного персонала (назовите не менее трёх)?
2. Чем отличаются умышленные угрозы (например, кража данных) от неумышленных (халатность, ошибка) с точки зрения методов противодействия?
3. Какие типы сотрудников относятся к группе «потенциально неблагонадёжных» с точки зрения внутренних угроз? Назовите основные признаки.
4. Какие организационные меры (политики, регламенты, инструкции) должны быть разработаны для предотвращения утечек конфиденциальной информации со стороны персонала?

Темы для доклада:

1. Классификация внутренних угроз: умышленные (хищение, саботаж, инсайдерство) и неумышленные (халатность, ошибки) – методы выявления и предотвращения
2. Портрет потенциально неблагонадёжного сотрудника: признаки, факторы риска, методы ранней диагностики
3. Организационно-правовые меры противодействия: политика коммерческой тайны, соглашения о неразглашении, материальная ответственность

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Какое действие сотрудника относится к неумышленной (неосторожной) угрозе информационной безопасности организации?

А) копирование базы клиентов на личную флешку для продажи конкуренту

Б) случайная отправка файла с коммерческой тайной на личную почту вместо корпоративной

В) умышленное уничтожение документов после уведомления об увольнении

Г) фиктивное списание материалов с последующей продажей через подставное лицо

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать несколько правильных ответов.

Записать только буквы выбранных вариантов ответа.

Какие из перечисленных мер относятся к организационным мерам противодействия внутренним угрозам информационной безопасности?

А) внедрение DLP-системы для контроля передачи данных

Б) утверждение перечня сведений, составляющих коммерческую тайну

В) подписание с сотрудниками соглашений о неразглашении

Г) использование шифрования на съёмных носителях

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

Внимательно прочитать предложенные варианты ответа.

Построить верную последовательность из предложенных элементов.

Записать буквы (в зависимости от задания) вариантов ответа в нужной последовательности.

Установите правильную последовательность действий работодателя при обнаружении факта несанкционированной передачи сотрудником конфиденциальных документов третьим лицам.

А) Проведение служебного расследования (опрос свидетелей, анализ логов, экспертиза)

Б) Фиксация факта нарушения (акт, скриншоты, логи доступа)

В) Применение дисциплинарного взыскания (вплоть до увольнения) и обращение в правоохранительные органы

Г) Временное отстранение сотрудника от доступа к конфиденциальной информации и блокировка его учётных записей

Ситуационные задания

В бухгалтерии организации «Регион» сотрудница Смирнова в течение года переводила на свой банковский счет небольшие суммы (от 5 до 15 тыс. руб.) под видом оплаты фиктивных счетов поставщиков. Всего она похитила 450 тыс. руб. Ревизия выявила расхождение, так как реальные поставщики подтвердили отсутствие таких счетов. Смирнова призналась и вернула часть суммы.

Вопросы:

1. К какому виду угроз имущественной безопасности относится данное деяние?
2. Какие меры контроля должны быть введены в бухгалтерии, чтобы исключить подобные действия?
3. Какую ответственность понесёт Смирнова? Каковы действия работодателя?

5.3. Каждый раздел дисциплины завершается контрольной точкой (далее – КТ). Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,1	10
КТ 2	100	0,1	10
КТ 3	100	0,1	10
Итого:	х	0,3	30

Формула расчета результата контрольной точки:

Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ – 1 (Темы 1.1-1.4)

Опрос по темам 1.1-1.4

1. Охарактеризуйте внешние угрозы кадровой безопасности (со стороны кандидатов, контрагентов, конкурентов).

2. Какие объекты входят в систему управления кадровой безопасностью (персонал, документы, информация, активы)?
3. Назовите субъекты управления кадровой безопасностью в организации и на государственной службе.
4. Как неправомерный сбор и обработка персональных данных кандидата (без его согласия) на этапе отбора может повлиять на репутацию и финансовое положение организации?
5. Каким образом конкурент может использовать открытые вакансии организации для сбора конфиденциальной информации о структуре штата и уровне оплаты труда?
6. В чём разница между обработкой персональных данных кандидата и обработкой ПДн уже принятого сотрудника с точки зрения правовых оснований (ФЗ-152 и ТК РФ)?
7. Какие подзаконные нормативные акты регулируют вопросы защиты персональных данных при их обработке без использования средств автоматизации? Назовите основной документ и его ключевое требование.
8. Какие данные о кандидате относятся к специальным категориям персональных данных (ст. 10 ФЗ-152) и как их обработка связана с конфиденциальностью в рекрутинге?
9. Какие риски возникают при хранении оценочных листов кандидатов в открытой общей папке на сервере или при передаче их через мессенджеры?
10. Какую информацию о кандидате работодатель вправе получать от предыдущего работодателя без нарушения конфиденциальности? Что для этого необходимо?
11. Каковы правовые последствия для HR-специалиста, который разгласил конфиденциальную информацию о кандидате (например, его заработную плату на предыдущем месте работы) третьим лицам без согласия?

Каждый вопрос предполагает свободный ответ. Рекомендуемое время на один ответ – 2–3 минуты. Оценка зависит от полноты, точности ссылок на статьи законов и примеров

Доклад

Примерная тематика докладов в рамках КТ 1

1. Сравнительный анализ систем кадровой безопасности в коммерческих организациях и на государственной гражданской службе
2. Индикаторы и диагностика уровня кадровой безопасности: как измерить эффективность системы.
3. Изменения в законодательстве о персональных данных за последние 3 года (обзор поправок в ФЗ-152 и КоАП РФ) и их влияние на HR-процессы

4. Ответственность за утечку персональных данных кандидатов: сравнительный анализ судебной и административной практики по ст. 13.11 КоАП РФ и ст. 137 УК РФ

5. Специальные категории персональных данных кандидата (ст. 10 ФЗ-152): особенности обработки и защиты в рекрутинге

6. Роль согласия кандидата в обеспечении конфиденциальности: когда оно необходимо, а когда — нет?

7. Технические и организационные меры защиты конфиденциальной информации о кандидатах: от сейфов до DLP-систем

8. Типичные ошибки рекрутеров при работе с конфиденциальной информацией и способы их предотвращения (анализ реальных кейсов)

Методические рекомендации по подготовке доклада

Подготовка доклада развивает исследовательские навыки, расширяет кругозор и учит критически оценивать информацию. При работе над докладом по указанной теме необходимо составить план и отобрать ключевые источники. Изучая их, студент систематизирует полученные данные, формулирует выводы и обобщения.

Такая деятельность требует высокой степени самостоятельности и серьёзной интеллектуальной работы. Наибольшую пользу она принесёт при соблюдении следующих этапов:

ознакомление с основными научными трудами по теме (список рекомендует преподаватель);

анализ изученного материала, выделение наиболее важных фактов, точек зрения учёных и научных положений;

обобщение и логическое выстраивание материала (например, в виде развёрнутого плана);

написание текста доклада в научном стиле.

Структура доклада традиционно включает три части: введение, основную часть и заключение.

Во введении обозначают тему, показывают её связь с другими вопросами или место среди смежных проблем, кратко характеризуют использованные источники.

Основная часть строится логично и последовательно, в ней полностью раскрывается тема.

В заключении подводят итоги, формулируют выводы, подчёркивают значимость рассмотренной проблемы.

Тестовые задания:

Тип: с одним правильным ответом

Что из перечисленного относится к внешним угрозам кадровой безопасности организации?

А) увольнение ключевого сотрудника к конкуренту

Б) разглашение работником коммерческой тайны по неосторожности

В) переманивание (хедхантинг) ценных специалистов конкурирующей компанией

Г) саботаж со стороны недовольного работника

Тип: с одним правильным ответом

Какое действие рекрутера на этапе отбора кандидатов является прямым нарушением законодательства о персональных данных и создаёт угрозу кадровой безопасности?

А) проверка паспортных данных кандидата после получения его письменного согласия

Б) направление резюме кандидата в службу безопасности без его согласия на обработку персональных данных

В) ведение журнала учёта кандидатов с указанием ФИО и даты собеседования

Г) уничтожение анкет непрошедших кандидатов по истечении срока хранения

Тип: с одним правильным ответом

Какое действие рекрутера является нарушением режима конфиденциальности в отношении кандидата?

А) уничтожение анкеты кандидата, не прошедшего отбор, по истечении срока хранения

Б) передача резюме кандидата руководителю отдела, в котором открыта вакансия, после получения согласия кандидата

В) направление оценочного листа кандидата в мессенджере (WhatsApp) руководителю без шифрования

Г) хранение резюме кандидата в сейфе с ограниченным доступом

Тип: с несколькими правильными ответами

Какие действия рекрутера на этапе оценки кандидатов создают реальные угрозы кадровой безопасности и/или нарушают законодательство о персональных данных? (Выберите все верные варианты)

А) проведение тестирования кандидата с использованием методики, являющейся коммерческой тайной работодателя, без подписания соглашения о неразглашении

Б передача результатов ассессмент-центра руководителю подразделения, не участвующему в отборе, «для ознакомления»

В) хранение заполненных тестов и оценочных листов кандидата в открытой общей папке на сервере

Г) устное информирование кандидата о предварительных результатах оценки без фиксации в документах

Тип: с несколькими правильными ответами

Какие меры работодателя обеспечивают защиту конфиденциальной информации о кандидатах в процессе рекрутинга? (выбрать все верные ответы)

А) хранение анкет и оценочных листов кандидатов в сейфе или ином запираемом шкафу

Б) рассылка резюме всех кандидатов по электронной почте всем сотрудникам организации «для ознакомления»

В) включение в договор с рекрутинговым агентством условия о неразглашении конфиденциальной информации

Г) использование корпоративного защищённого документооборота (СЭД) вместо публичных облачных сервисов

Тип: на установление соответствия

Установите соответствие между субъектом управления кадровой безопасностью (левый столбец) и его типичной функцией (правый столбец). Каждому субъекту соответствует одна функция.

№	Субъект управления	№	Функция
1	Руководитель организации (директор)	А	Проведение инструктажей и обучение персонала правилам работы с персональными данными
2	Служба безопасности	Б	Утверждение политики кадровой безопасности и выделение ресурсов
3	Отдел кадров	В	Осуществление проверки кандидатов при приеме на работу
4	Уполномоченный по персональным данным (внутренний или внешний	Г	Контроль соблюдения законодательства о персональных данных и ведение реестра согласий

Тип: на установление соответствия

Установите соответствие между видом конфиденциальной информации в рекрутинге (левый столбец) и её конкретным примером (правый столбец)..

Каждому виду из левого столбца соответствует один пример в правом.

№	Вид информации	№	Пример
1	Персональные данные кандидата (общая категория)	А	Аудиозапись интервью с кандидатом, сделанная без его письменного согласия
2	Специальные категории персональных данных (ст. 10 ФЗ-152)	Б	Заключение службы безопасности о наличии судимости у кандидата
3	Коммерческая тайна работодателя	В	Паспортные данные кандидата, полученные с его согласия
4	Иная конфиденциальная информация (не ПДн)	Г	Методика оценки компетенций кандидатов, разработанная внутри организации

Тип: на установление последовательности

Расположите в правильном порядке действия HR-специалиста и службы безопасности при обнаружении факта несанкционированной передачи персональных данных кандидатов третьим лицам в процессе отбора персонала.

А) Уведомление Роскомнадзора (в случае, если инцидент относится к категории значимых утечек персональных данных)

Б) Фиксация факта инцидента (составление акта, скриншоты, логи доступа)

В) Временное отстранение сотрудника, подозреваемого в нарушении, от работы с персональными данными (с сохранением заработной платы на период проверки)

Г) Проведение внутреннего служебного расследования (опросы, анализ систем безопасности, проверка цепочки передачи данных)

Ситуационное задание

Прочитайте текст и запишите развернутый обоснованный ответ.

Компания «Альфа» (крупный ритейлер) через рекрутинговое агентство «Бета» искала кандидата на должность коммерческого директора. В процессе отбора рекрутер агентства «Бета» направил руководителю отдела безопасности компании «Альфа» и финансовому директору (оба участвовали в отборе) по корпоративной электронной почте следующие документы кандидата Смирнова П.А.:

резюме (ФИО, возраст, образование, опыт работы, контакты);

паспортные данные (скан паспорта, ИНН, СНИЛС);

справку о доходах за 2 года (конфиденциальный документ с места работы кандидата);

результаты психологического тестирования, проведённого агентством;

аудиозапись интервью с кандидатом (без его письменного согласия на запись).

При этом:

Письменное согласие на обработку ПДн кандидат подписал только на передачу резюме и проверку рекомендаций.

Согласия на передачу справки о доходах, паспортных данных и аудиозаписи кандидат не давал.

Финансовый директор, получив письмо, переслал все документы на свой личный ноутбук и в нерабочий мессенджер (WhatsApp) супруге «для консультации».

Через неделю справка о доходах кандидата и его паспортные данные появились в открытом доступе на форуме.

Кандидат Смирнов обратился в суд с иском к компании «Альфа» и рекрутинговому агентству «Бета» о компенсации морального вреда и убытков, а также написал жалобу в Роскомнадзор.

Вопросы к заданию:

1. Какие угрозы кадровой безопасности возникли на этапах отбора, оценки и принятия решения? Перечислите не менее 4 угроз.
2. Кто из участников (рекрутер, агентство «Бета», компания «Альфа», финансовый директор) и за что несёт ответственность?
3. Какие организационные и технические меры необходимо было принять, чтобы предотвратить инцидент?
4. Какова должна быть правильная последовательность действий HR-службы и службы безопасности при обнаружении факта утечки?

КТ – 2 (Темы 2.1-2.4)

Опрос по темам 21.1-2.4

1. Как в политике работодателя должно быть прописано получение, форма и срок действия согласия кандидата на обработку его ПДн?
2. Какие категории персональных данных кандидата относятся к специальным (ст. 10 ФЗ-152) и как политика должна регулировать их обработку?
3. Каким образом политика определяет порядок доступа к ПДн кандидатов для различных категорий сотрудников (рекрутер, руководитель, служба безопасности)?

4. Как в политике описываются сроки хранения ПДн кандидатов и процедура их уничтожения после отказа в трудоустройстве или истечения срока хранения?
5. Какие особенности имеет согласие на обработку специальных категорий ПДн (судимость, здоровье, биометрия)? Требуется ли отдельная форма?
6. Как оформляется согласие на обработку ПДн при передаче данных третьим лицам (например, рекрутинговому агентству, аутсорсеру, службе безопасности)?
7. В какой форме может быть получено согласие: только письменная, или допустима электронная / конклюдентная (например, отметка на сайте)? Приведите примеры.
8. Каков порядок отзыва согласия кандидатом или сотрудником? Какие обязанности возникают у работодателя после отзыва?
9. Какие требования предъявляются к хранению бумажных носителей с ПДн кандидатов (сейфы, запираемые шкафы, опечатывание)?
10. Каковы правила передачи документов с ПДн кандидата между сотрудниками (рекрутер – руководитель – служба безопасности) с точки зрения фиксации передачи?
11. В чем особенности оформления электронных документов с ПДн кандидатов? Какие системы электронного документооборота допустимы?
12. Какие сроки хранения документов, содержащих ПДн кандидатов, установлены в организации и как они соотносятся с требованиями ФЗ-152?

Каждый вопрос предполагает свободный ответ. Рекомендуемое время на один ответ – 2–3 минуты. Оценка зависит от полноты, точности ссылок на статьи законов и примеров.

Доклад

Примерная тематика докладов в рамках КТ 2

1. Особенности обработки специальных категорий ПДн кандидатов (судимость, здоровье, биометрия) в политике работодателя

4. Сроки хранения и процедура уничтожения ПДн кандидатов: как закрепить в политике и в кадровом делопроизводстве

5. Разграничение доступа к ПДн кандидатов: принцип служебной необходимости в тексте политики и на практике

2. Особенности согласия на обработку специальных категорий ПДн (судимость, здоровье, биометрия): отдельная форма или включение в общее согласие

3. Согласие на передачу персональных данных третьим лицам (рекрутинговым агентствам, аутсорсерам, службе безопасности): правовые риски и образцы

4. Электронная форма согласия: конклюдентные действия (галочка на сайте), электронная подпись, фиксация в информационной системе
5. Документальное оформление доступа к ПДн кандидатов: журналы учёта, подписки о неразглашении, разрешительные записки
6. Технические средства разграничения доступа к электронным носителям с ПДн кандидатов (парольная защита, шифрование, DLP-системы, контроль съёмных носителей)
7. Ответственность за нарушение порядка доступа к ПДн кандидатов (дисциплинарная, административная, гражданско-правовая)
8. Акт об уничтожении персональных данных непрошедших кандидатов: образец, юридическое значение, ответственность за отсутствие
9. Правила хранения бумажных носителей с ПДн кандидатов (сейфы, опечатывание, доступ по списку)
10. Документальное оформление передачи ПДн кандидата между сотрудниками (рекрутер – руководитель – служба безопасности)

Методические рекомендации по подготовке доклада

Подготовка доклада развивает исследовательские навыки, расширяет кругозор и учит критически оценивать информацию. При работе над докладом по указанной теме необходимо составить план и отобрать ключевые источники. Изучая их, студент систематизирует полученные данные, формулирует выводы и обобщения.

Такая деятельность требует высокой степени самостоятельности и серьёзной интеллектуальной работы. Наибольшую пользу она принесёт при соблюдении следующих этапов:

ознакомление с основными научными трудами по теме (список рекомендует преподаватель);

анализ изученного материала, выделение наиболее важных фактов, точек зрения учёных и научных положений;

обобщение и логическое выстраивание материала (например, в виде развёрнутого плана);

написание текста доклада в научном стиле.

Структура доклада традиционно включает три части: введение, основную часть и заключение.

Во введении обозначают тему, показывают её связь с другими вопросами или место среди смежных проблем, кратко характеризуют использованные источники.

Основная часть строится логично и последовательно, в ней полностью раскрывается тема.

В заключении подводят итоги, формулируют выводы, подчёркивают значимость рассмотренной проблемы.

Тестовые задания:

Тип: с одним правильным ответом

Согласно принципам разработки Политики обработки персональных данных кандидатов, срок хранения персональных данных непрошедшего кандидата определяется:

А) произвольно рекрутером, исходя из личного усмотрения

Б) бессрочно, так как кандидат может ещё понадобиться в будущем

В) исходя из установленных работодателем сроков, но не дольше, чем требуют цели обработки (например, до закрытия вакансии плюс разумный срок)

Г) сроком на 75 лет в соответствии с архивным законодательством

Тип: с одним правильным ответом

Какой элемент не является обязательным для включения в письменное согласие на обработку персональных данных согласно ст. 9 ФЗ-152?

А) фамилия, имя, отчество и адрес субъекта ПДн (кандидата)

Б) перечень действий с ПДн (сбор, систематизация, накопление, хранение и др.)

В) гарантии работодателя по сохранению заработной платы сотрудника

К) срок действия согласия и порядок его отзыва

Тип: с несколькими правильными ответами

Какие действия работодателя являются правильными при внедрении Политики обработки ПДн кандидатов в процессы управления персоналом?

А) разместить текст Политики в открытом доступе на сайте организации (в разделе для соискателей)

Б) требовать от кандидата ознакомления с Политикой и подписания согласия на обработку ПДн до направления резюме

В) хранить резюме и анкеты непрошедших кандидатов неограниченно долго «на всякий случай»

Г) назначить ответственного за организацию обработки ПДн и включить контроль соблюдения Политики в должностные инструкции рекрутеров

Тип: с несколькими правильными ответами

На этапе отбора кандидат подписал согласие на обработку ПДн для целей трудоустройства на конкретную должность. После отказа в приёме на работу работодатель предлагает кандидату остаться в кадровом резерве и хранить его данные ещё 2 года. Какое действие работодателя является корректным с точки зрения формы согласия?

А) Работодатель может хранить данные кандидата в кадровом резерве без дополнительного согласия, так как оно уже получено.

Б) Необходимо получить новое, отдельное согласие на обработку ПДн для целей формирования и ведения кадрового резерва с указанием новых целей и срока хранения.

В) Достаточно устного согласия кандидата, зафиксированного в аудиозаписи.

Г) Работодатель не имеет права предлагать кандидату остаться в резерве, данные должны быть немедленно уничтожены.

Тип: на установление последовательности

Расположите в правильном порядке действия работодателя по внедрению Политики обработки ПДн кандидатов в процессы управления персоналом.

А) Размещение текста Политики в открытом доступе на сайте организации (в разделе для соискателей)

Б) Проведение инструктажа (обучения) рекрутеров и сотрудников, имеющих доступ к ПДн кандидатов

В) Внесение изменений в формы документов (анкеты кандидата, бланки согласий) в соответствии с Политикой

Г) Ознакомление кандидатов с Политикой до начала сбора их персональных данных

Тип: на установление последовательности

Расположите в правильном порядке действия работодателя после получения от сотрудника заявления об отзыве согласия на обработку персональных данных.

А) Уведомление сотрудника о прекращении обработки (кроме случаев, когда обработка обязательна по закону)

Б) Проверка наличия иных законных оснований для обработки ПДн (исполнение трудового договора, налоговые обязанности)

В) Приём и регистрация заявления сотрудника об отзыве согласия (в журнале входящих документов)

Г) Уничтожение ПДн (или прекращение обработки) в части, не требующейся для исполнения требований законодательства

Ситуационные задания

Прочитайте текст и запишите развернутый обоснованный ответ

В организации «Дельта» на этапе отбора на должность финансового директора служба безопасности запросила у рекрутера копию паспорта, ИНН, СНИЛС и сведения о судимости кандидата. Рекрутер передала запрошенные данные, хотя кандидат давал письменное согласие только на проверку рекомендаций и профессиональных навыков. Служба безопасности также передала эти данные начальнику отдела кадров для «оформления допуска», хотя отдел кадров не запрашивал их. Через некоторое время выяснилось, что

данные кандидата были скопированы на личную флешку сотрудника службы безопасности.

Вопросы к ситуации:

1. Было ли нарушено разграничение полномочий при доступе к ПДн?
2. Какие нормы законодательства о персональных данных нарушены?
3. Какая ответственность грозит рекрутеру, сотруднику службы безопасности и организации?

КТ – 3 (Темы 3.1-3.4)

Опрос по темам 3.1-3.4

1. Как оформляется допуск к государственной тайне в процессе отбора на гражданскую службу, и связан ли он с обработкой персональных данных?
2. В каких случаях кандидату может быть отказано в приёме на государственную гражданскую службу по результатам проверки персональных данных?
3. Какие ограничения, связанные с близким родством, установлены при отборе на государственную службу (статья 27 ФЗ «О государственной гражданской службе РФ»)?
4. Требуется ли согласие кандидата на обработку персональных данных о его супруге (супруги) и несовершеннолетних детях при поступлении на госслужбу? Если да, то на каком основании?
5. Назовите основные принципы, на которых базируется культура кадровой безопасности (например, личная ответственность, неразглашение, осведомлённость).
6. Какие категории персонала в первую очередь нуждаются в обучении правилам кадровой безопасности и почему?
7. Какие методы обучения персонала правилам работы с персональными данными и конфиденциальной информацией вы знаете? Назовите не менее трёх.
8. Как можно мотивировать сотрудников (включая рекрутеров и HR-специалистов) соблюдать политики кадровой безопасности? Приведите примеры нематериальной и материальной мотивации.
9. Что такое «внутренний контроль» в контексте корпоративной культуры кадровой безопасности? Какие формы контроля существуют?
10. Как построить матрицу рисков для рекрутинговых процессов? Что располагается на осях матрицы и какие зоны (критическая, высокая, средняя, низкая) выделяются?
11. Назовите не менее пяти типовых рисков кадровой безопасности при сборе и обработке резюме кандидатов (например, утечка через незащищённую форму на сайте).
12. Какие риски связаны с передачей персональных данных кандидатов через мессенджеры MAX, Telegram) и открытые облачные сервисы?

13. Как оценивается риск неправомерного отказа кандидату на основании недостоверных или незаконно полученных сведений? Каковы правовые последствия?
14. Что такое «политика чистого стола» и «чистого экрана», и как они помогают в защите информационной безопасности?
15. Какие технические средства (DLP, контроль съёмных носителей, видеонаблюдение, логирование доступа) наиболее эффективны для выявления и блокировки действий недобросовестных сотрудников?
16. Какую ответственность (дисциплинарную, материальную, административную, уголовную) может понести сотрудник за разглашение коммерческой тайны или хищение имущества?
17. Каков порядок действий работодателя при выявлении факта хищения имущества сотрудником (документирование, инвентаризация, обращение в полицию)?

Каждый вопрос предполагает свободный ответ. Рекомендуемое время – 2–3 минуты на вопрос. Оценка зависит от полноты ответа, ссылок на статьи законов и примеров из практики.

Доклад

Примерная тематика докладов в рамках КТ 3.

1. Допуск к государственной тайне как этап отбора на отдельные должности государственной гражданской службы
2. Ограничения и запреты при приёме на государственную службу: близкое родство, гражданство, наличие судимости и иные требования
3. Согласие на обработку персональных данных при поступлении на государственную службу: особенности объёма данных (включая сведения о родственниках) и отличия от коммерческого сектора
4. Мотивация соблюдения политик безопасности: KPI, премирование, нематериальное поощрение (награды, статус «Лучший по безопасности»)
5. Внутренний контроль и аудит как элементы корпоративной культуры: регулярные проверки, самодиагностика, тестирование сотрудников
6. Индикаторы низкой культуры кадровой безопасности (игнорирование регламентов, передача паролей, небрежное хранение документов) и методы их устранения
7. Матрица рисков для рекрутинговых процессов: построение, зонирование (критическая, высокая, средняя, низкая области) и интерпретация
8. Типовые риски при сборе и хранении персональных данных кандидатов (незащищённые формы, облачные сервисы, мессенджеры) и способы их минимизации
9. Риски, связанные с передачей данных кандидатов третьим лицам (службе безопасности, аутсорсерам, внутренним заказчикам) без соблюдения служебной необходимости
10. Технические средства защиты информации от внутренних угроз: DLP-системы, контроль съёмных носителей, журналы доступа, видеонаблюдение

11.Политика «чистого стола» и «чистого экрана» как элемент повседневной культуры безопасности: внедрение и контроль

12.Материальная и дисциплинарная ответственность сотрудников за хищение имущества и разглашение информации: правовые механизмы и судебная практика

Методические рекомендации по подготовке доклада

Подготовка доклада развивает исследовательские навыки, расширяет кругозор и учит критически оценивать информацию. При работе над докладом по указанной теме необходимо составить план и отобрать ключевые источники. Изучая их, студент систематизирует полученные данные, формулирует выводы и обобщения.

Такая деятельность требует высокой степени самостоятельности и серьёзной интеллектуальной работы. Наибольшую пользу она принесёт при соблюдении следующих этапов:

ознакомление с основными научными трудами по теме (список рекомендует преподаватель);

анализ изученного материала, выделение наиболее важных фактов, точек зрения учёных и научных положений;

обобщение и логическое выстраивание материала (например, в виде развёрнутого плана);

написание текста доклада в научном стиле.

Структура доклада традиционно включает три части: введение, основную часть и заключение.

Во введении обозначают тему, показывают её связь с другими вопросами или место среди смежных проблем, кратко характеризуют использованные источники.

Основная часть строится логично и последовательно, в ней полностью раскрывается тема.

В заключении подводят итоги, формулируют выводы, подчёркивают значимость рассмотренной проблемы.

Тестовые задания:

Тип: с одним правильным ответом

В матрице рисков кадровой безопасности риск с высокой вероятностью наступления и тяжёлыми последствиями (например, утечка паспортных данных всех кандидатов за год через незащищённый облачный сервис) относится к зоне:

А) низкого приоритета (принимать без мер)

Б) средней зоны (наблюдать)

В) критической зоны (требует немедленного принятия мер)

Г) зоны умеренного риска (плановые меры в течение квартала)

Тип: с одним правильным ответом

Какой документ необходимо в первую очередь подписать с сотрудником, имеющим доступ к коммерческой тайне, чтобы иметь возможность привлечь его к ответственности за разглашение?

А) трудовой договор (без специальных условий)

Б) соглашение о неразглашении (конфиденциальности) и ознакомление с перечнем сведений, составляющих коммерческую тайну

В) договор о полной материальной ответственности

Г) заявление о добровольном возмещении ущерба

Тип: с несколькими правильными ответами

Какие меры минимизации рисков кадровой безопасности в процессе отбора относятся к организационным?

А) утверждение перечня должностей с правом доступа к ПДн кандидатов

Б) установка системы DLP (контроль передачи данных)

В) проведение регулярных инструктажей и обучения рекрутеров

Г) использование двухфакторной аутентификации в HR-системе

Тип: с несколькими правильными ответами

Какие признаки могут свидетельствовать о том, что сотрудник представляет потенциальную угрозу имущественной безопасности организации (склонен к хищениям или злоупотреблениям)?

А) систематические отказы от повышения квалификации

Б) частые мелкие ошибки в учёте при отсутствии контроля

В) жизнь не по средствам (резкое увеличение расходов, несоответствие зарплате)

Г) активное участие в корпоративных волонтёрских программах

Тип: на установление последовательности

Расположите в правильном порядке действия HR-службы при разработке мер по минимизации риска утечки персональных данных кандидатов через незащищённые облачные сервисы.

А) Выбор организационных мер (запрет на использование облачных сервисов, перечень разрешённых инструментов)

Б) Анализ существующих регламентов и выявление пробелов в защите ПДн

В) Внедрение выбранных мер (издание приказа, обучение сотрудников, настройка технических средств)

Г) Выбор технических мер (шифрование, DLP, двухфакторная аутентификация)

Тип: на установление последовательности

Расположите в правильном порядке этапы внедрения в организации системы противодействия утечкам информации со стороны персонала.

А) Выбор и установка технических средств защиты (DLP, контроль съёмных носителей)
Б) Оценка рисков и определение перечня сведений, подлежащих защите
В) Разработка и утверждение локальных актов (положение о коммерческой тайне, соглашения о неразглашении)
Г) Обучение сотрудников и контроль соблюдения установленных правил

Ситуационные задания

В компании «Омега» (разработка ПО) системный администратор Петров, увольняясь по собственному желанию, скопировал на личную флешку исходные коды нового продукта, а также базу данных клиентов с их персональными данными. Через два дня эти материалы появились на теневом форуме. Служба безопасности обнаружила факт копирования по логам доступа к серверу. Петров отрицает свою вину, утверждая, что флешка была утеряна, а данные с неё скопировали третьи лица.

Вопросы:

1. Какие виды внутренних угроз продемонстрировал Петров?
2. Какие организационные и технические меры позволили бы предотвратить или своевременно выявить данное действие?
3. Какая ответственность грозит Петрову? Какие действия должна предпринять компания?

КРИТЕРИИ ОЦЕНИВАНИЯ КАЖДОГО ИЗ ЗАДАНИЙ

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать

	свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
85-100	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
65-84	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
55-64	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.

0-54	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

Критерии оценивания ситуационных заданий:

Диапазон баллов	Описание критерия
85-100	Обучающимся задание выполнено без ошибок и в полном объеме.
65-84	Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
55-64	Обучающимся допущены отдельные ошибки при выполнении задания
0-54	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

Общая оценка по КТ 1-3 определяется путем нахождения среднего балла по всем заданиям, используемым в контрольной работе.

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (при необходимости).

Для решения контрольных заданий обучающемуся разрешается использование калькулятора.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация (экзамен) проводится в письменной форме. Обучающийся получает экзаменационный билет с вариантами задний. Обучающийся получает чистые маркированные листы бумаги для записей к подготовке ответов. Необходимо дать ответ в письменном виде, подробно изложив ход мыслей.

6.2. Типовые оценочные материалы промежуточной аттестации

Тема 1.1. Кадровая безопасность организации как объект управления

Экзаменационные вопросы открытого типа

1. Дайте определение кадровой безопасности организации. В чем ее отличие от общей безопасности предприятия?
2. Какие нормативно-правовые акты РФ составляют основу управления кадровой безопасностью?

3. Охарактеризуйте роль кадровой службы в обеспечении кадровой безопасности на этапах подбора, адаптации, мотивации и увольнения персонала.

Экзаменационное задание

Проведите классификацию основных угроз безопасности организации со стороны ее персонала, заполнив для этого соответствующие графы таблицы:

Типовые угрозы информационной безопасности организации	Типовые угрозы имущественной безопасности организации

Тема 1.2. Кадровая безопасность в процессе подбора персонала: угрозы на этапах привлечения, отбора, оценки, принятия решения

Экзаменационные вопросы открытого типа

1 Какие угрозы кадровой безопасности характерны для этапа привлечения кандидатов (размещение вакансий, обработка входящих резюме)?

2. Охарактеризуйте угрозы, возникающие на этапе отбора (скрининг резюме, телефонное интервью, первичное собеседование). Приведите конкретные примеры.

3. Какие угрозы возникают на этапе принятия решения о найме и оформления кандидата на работу? Назовите не менее трёх.

Экзаменационное задание

Прочитайте текст и ответьте на вопросы

«Вы руководитель отдела подбора персонала. На этапе оценки кандидата на должность финансового директора рекрутер без согласия соискателя направил его резюме, паспортные данные и результаты психологического тестирования в службу безопасности и в бухгалтерию «для проверки». При этом руководитель бухгалтерии переслал эти данные на свой личный ноутбук».

Вопросы к ситуации:

1. Какие угрозы кадровой безопасности возникли на этапе оценки и принятия решения?

2. Какие статьи законодательства о персональных данных нарушены?

3. Какие организационные меры вы предложите, чтобы исключить повторение такого инцидента в будущем?

Тема 1.3. Нормативно-правовая база обработки персональных данных кандидатов и сотрудников. ПК-1.4.

Экзаменационные вопросы открытого типа

1. Укажите федеральные законы Российской Федерации, составляющие основу правового регулирования обработки персональных данных кандидатов и сотрудников?

2. Поясните, в чём разница между обработкой персональных данных кандидата и обработкой ПДн уже принятого сотрудника с точки зрения правовых оснований (ФЗ-152 и ТК РФ).

3. Укажите виды ответственности, предусмотренной за нарушение законодательства о персональных данных при обработке данных кандидата.

Экзаменационное задание

Прочитайте ситуацию и ответьте на нижеприведенные вопросы.

При приёме на работу менеджера по закупкам кандидат Иванов заполнил анкету, в которой указал паспортные данные, ИНН, СНИЛС, семейное положение, наличие судимости (погашенной). Рекрутер попросил также предоставить справку о доходах с предыдущего места работы и характеристику от бывшего руководителя. Кандидат предоставил справку, но от характеристики отказался. Рекрутер направил его анкету и справку о доходах руководителю отдела закупок и в службу безопасности через корпоративную почту. Письменного согласия на обработку персональных данных (ПДн) рекрутер у кандидата не брал, сославшись на то, что «кандидат сам пришёл и заполнил анкету – это и есть согласие».

Вопросы:

1.Нарушены ли требования законодательства о персональных данных? Если да, то какие именно нормы (укажите статьи ФЗ-152 и/или ТК РФ)?

2. Требовалось ли письменное согласие на обработку ПДн в данном случае?

3. Правомерен ли сбор справки о доходах и характеристики?

4. Какие действия рекрутера являются неправомерными?

Тема 1.4. Конфиденциальная информация в рекрутинге.

Экзаменационные вопросы открытого типа

1. Поясните, что понимается под конфиденциальной информацией в рекрутинге?

2. Укажите, чем конфиденциальная информация о кандидате отличается от персональных данных в понимании ФЗ-152?

3. Назовите виды конфиденциальной информации, получаемой в процессе рекрутинга, могут относиться к коммерческой тайне работодателя?

Экзаменационное задание

Составьте перечень организационных мер, которые должен принять работодатель, чтобы обеспечить защиту конфиденциальной информации о кандидатах на этапах отбора и оценки?

Тема 2.1. Политика работодателя в области обработки персональных данных кандидатов: разработка, внедрение в процессы управления персоналом

Экзаменационные вопросы открытого типа

1. Раскройте сущность политики обработки персональных данных (ПДн) кандидатов и чем она отличается от аналогичной политики для сотрудников?
2. Перечислите требования к защите персональных данных (ПДн) кандидатов (организационные и технические), которые должны быть закреплены в политике?
3. Опишите порядок внедрения политики в процессы управления персоналом

Экзаменационное задание

Компания «ТехноСервис» (IT-разработка, 80 сотрудников) решила разработать и внедрить Политику обработки персональных данных кандидатов. Разработайте три обязательных раздела Политики обработки персональных данных кандидатов:

1. «Категории обрабатываемых персональных данных кандидатов и цели их обработки» (перечислить минимум 5 категорий данных и 3 цели).
2. «Порядок получения согласия кандидата на обработку персональных данных» (описать форму согласия, сроки, процедуру отзыва).
3. «Сроки хранения и порядок уничтожения персональных данных кандидатов» (указать типовые сроки и процедуру составления акта об уничтожении).

Тема 2.2. Согласие на обработку персональных данных: формы для разных этапов

Экзаменационные вопросы открытого типа

1. Раскройте сущность и содержание согласия на обработку персональных данных (ПДн) с точки зрения ФЗ-152?
2. Укажите, какие особенности согласия на обработку ПДн установлены для государственных гражданских служащих (в части предоставления сведений о доходах, проверок)?
3. Укажите случаи, в которых обработка ПДн кандидата или сотрудника возможна без получения согласия? Назовите не менее двух исключений.

Экзаменационное задание

Прочитайте текст и ответьте на вопросы.

Сотрудница Петрова Н.И. работает бухгалтером. Компания решает передать её персональные данные (ФИО, паспортные данные, ИНН, СНИЛС, адрес) в банк для оформления корпоративной зарплатной карты (с согласия сотрудницы). Кроме того, руководство просит передать эти же данные страховой компании для оформления ДМС (добровольного медицинского страхования) и в рекрутинговое агентство (для участия в конкурсе «Лучший бухгалтер года» – инициатива отдела кадров, не связанная с трудовой функцией).

Вопросы:

1. Требуется ли получать отдельное согласие на передачу ПДн в банк для зарплатного проекта? Почему? (Обосновать ссылкой на закон).
2. Требуется ли отдельное согласие на передачу ПДн в страховую компанию для ДМС? Если да, то обязательно ли письменное или достаточно устного?
3. Правомерно ли передавать данные сотрудницы в рекрутинговое агентство для участия в конкурсе без её согласия? Какую форму согласия необходимо получить?
4. Какие последствия могут наступить для компании, если передача данных в агентство произойдёт без согласия?

Тема 2.3. Разграничение полномочий при доступе к персональным данным в процессе отбора персонала

Экзаменационные вопросы открытого типа

1. Назовите категории сотрудников организации, которые обычно имеют доступ к персональным данным кандидатов в процессе отбора.
2. Опишите порядок действий рекрутера, если к нему обратился сотрудник, не включённый в перечень должностей, с просьбой предоставить данные кандидата.
3. Раскройте принцип «служебной необходимости» применительно к доступу к персональным данным кандидатов.

Экзаменационное задание

Прочитайте текст и ответьте на вопросы.

HR-менеджер Петров в процессе отбора на должность менеджера по продажам получил от кандидата письменное согласие на обработку ПДн в целях трудоустройства. При этом Петров внёс все данные кандидата (включая домашний адрес, паспортные данные) в общую электронную таблицу на корпоративном Google Диске, доступ к которой имели все сотрудники отдела персонала (10 человек), а также открыл доступ для руководителя отдела продаж и бухгалтера. Часть сотрудников отдела персонала не участвовала в отборе. В результате данные кандидата случайно удалил сотрудник, не имевший к отбору отношения, из-за чего информация была утеряна.

Вопросы к ситуации:

1. Какие нарушения разграничения полномочий допущены?

2. Какие требования к защите ПДн при хранении и доступе были проигнорированы?
3. Предложите корректный порядок действий Петрова.

Тема 2.4. Документирование процедур отбора с соблюдением режима защиты персональных данных

Экзаменационные вопросы открытого типа

1. Перечислите документы, содержащие персональные данные кандидатов, которые создаются на этапах привлечения, отбора, оценки и принятия решения о найме?
2. Перечислите наиболее типичные нарушения в документировании процедур отбора являются и ответственность за них.
3. Опишите порядок документального подтверждения, факта ознакомления кандидата с Политикой обработки ПДн и получение от него согласие на их обработку

Экзаменационное задание

Прочитайте текст и ответьте на вопросы.

В организации «Дельта» на этапе отбора на должность финансового директора служба безопасности запросила у рекрутера копию паспорта, ИНН, СНИЛС и сведения о судимости кандидата. Рекрутер передала запрошенные данные, хотя кандидат давал письменное согласие только на проверку рекомендаций и профессиональных навыков. Служба безопасности также передала эти данные начальнику отдела кадров для «оформления допуска», хотя отдел кадров не запрашивал их. Через некоторое время выяснилось, что данные кандидата были скопированы на личную флешку сотрудника службы безопасности.

Вопросы к ситуации:

1. Было ли нарушено разграничение полномочий при доступе к ПДн?
2. Какие нормы законодательства о персональных данных нарушены?
3. Какая ответственность грозит рекрутеру, сотруднику службы безопасности и организации?

Тема 3.1. Особенности отбора на государственную гражданскую службу

Экзаменационные вопросы открытого типа

1. Укажите, в чем заключается отличие процедуры отбора на государственную гражданскую службу от отбора в коммерческую организацию с точки зрения объёма запрашиваемых персональных данных?

2. Укажите меры кадровой безопасности, которые применяются после отказа кандидату (хранение, уничтожение его персональных данных) на государственной службе?

3. Назовите виды ответственности, которую несёт должностное лицо кадровой службы государственного органа за разглашение персональных данных кандидата, полученных в ходе проверки.

Экзаменационное задание

Прочитайте текст и выполните задания.

Кандидат Иванов поступает на должность в налоговую инспекцию. Кадровая служба требует:

Согласие на обработку ПДн (включая данные о доходах его жены и сына).

Справку о судимости и медицинскую справку.

Сообщить о родственниках, работающих в той же инспекции.

Передать данные в банки и полицию для проверки.

Кандидат отказывается:

Давать данные о доходах жены (ссылается на её тайну частной жизни).

Сообщать о родственниках (говорит, что это не обязательно).

Задание:

1. Отметьте законные требования кадровой службы (поставьте «+» рядом с каждым требованием, которое соответствует закону):

согласие на ПДн с данными о доходах семьи ___

справка о судимости ___

медицинская справка ___

сообщение о родственниках ___

передача данных в банки и полицию ___

2. Ответьте коротко (одним предложением на каждый пункт):

Правомерен ли отказ кандидата давать сведения о доходах жены?

Обязан ли кандидат сообщать о родственниках на госслужбе?

На каком законе основана передача ПДн в полицию без согласия?

Тема 3.2. Корпоративная культура кадровой безопасности

Экзаменационные вопросы открытого типа

1. Дайте определение корпоративной культуры кадровой безопасности. Из каких элементов она состоит?

2. Назовите основные принципы, на которых базируется культура кадровой безопасности

3. Перечислите категории персонала, которые в первую очередь нуждаются в обучении правилам кадровой безопасности, объясните почему.

Экзаменационное задание

Составьте короткий план из 3 шагов для внедрения культуры кадровой безопасности в компании.

Тема 3.3. Управление рисками кадровой безопасности в процессе отбора

Экзаменационные вопросы открытого типа

1. Дайте определение понятию «риск кадровой безопасности» применительно к процессу отбора персонала. Приведите пример риска.

2. Назовите основные группы рисков кадровой безопасности, которые возникают на этапах привлечения, отбора, оценки и принятия решения о найме?

3. Назовите основные организационные и технические меры минимизации рисков кадровой безопасности» применительно к процессу отбора персонала.

Экзаменационное задание

Прочитайте текст и выполните задание.

В компании «СтройКом» при подборе персонала выявлены следующие риски:

Резюме кандидатов хранятся в открытой папке на Яндекс.Диске, доступ к которой есть у всех 50 сотрудников.

Рекрутеры пересылают анкеты и результаты тестов руководителям через WhatsApp.

Служба безопасности проверяет кандидатов без их письменного согласия.

Данные непрошедших кандидатов не уничтожаются, а копятся годами.

Задание:

Составьте короткий план из 3 шагов по управлению рисками для данной компании:

Тема 3.4. Противодействие угрозам информационной и имущественной безопасности организации со стороны собственного персонала

Экзаменационные вопросы открытого типа

1. Назовите основные виды угроз информационной безопасности, которые могут исходить от собственного персонала

2. Перечислите типовые причины и формы угроз имущественной безопасности организации с участием ее персонала

3. Назовите основные методы противодействия угрозам имущественной безопасности организации со стороны ее персонала

Экзаменационное задание

Определите санкции за указанные ниже нарушения конкретным сотрудником правил обеспечения информационной безопасности работодателя, заполнив для этого правую графу таблицы.

Нарушение	Санкции
Неумышленное нарушение правил обеспечения компьютерной безопасности, допущенное вторично	

Разглашение конфиденциальной информации в присутствии коллег по работе	
Умышленная передача конкурентам информации, составляющей коммерческую тайну	
Зафиксированная попытка несанкционированного проникновения в конфиденциальные базы данных	

6.3. Критерии и шкала оценивания на основе БРС Донецкого филиала РАНХиГС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	100-90
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	75-89
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	60-74
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на	1-59

вопросы даже при дополнительных наводящих вопросах преподавателя.	

7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная,

кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Тестирование.
6. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность -до 15 минут. Вторая часть -выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность – до 20 минут. После

докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15 минут. Если по теме программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – до 15 минут. Также на занятиях предусмотрено проведение тестирования (тесты разных уровней сложности) Примерная продолжительность – до 15 минут. Практическое занятие заканчивается подведением итогов. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность -5 минут.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Махмудова, И. Н. Кадровая безопасность: организация и управление : учебное пособие / И. Н. Махмудова, Н. В. Соловова. — Самара : Самарский университет, 2022. — 96 с. — ISBN 978-5-7883-1755-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336590. — Режим доступа: для авториз. пользователей.

2. Андруник, А. П. Кадровая безопасность 2.0: теория и практика : монография / А. П. Андруник. — Москва : Дашков и К, 2024. — 570 с. — ISBN 978-5-394-05455-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/429761. — Режим доступа: для авториз. пользователей.

3. Карзаева, Н. Н. Кадровая безопасность: учебное пособие / Н.Н. Карзаева, Е.В. Каранина. — Москва: ИНФРА-М, 2023 — (Высшее образование) — С. 2 — Текст : электронный. — URL: https://znanium.ru/read?id=431366&page=2. – Режим доступа: по подписке.

4. Боровских, Н.В. Обеспечение кадровой безопасности промышленного предприятия / Н. В. Боровских, N. V. Borovskih // Научно-методический электронный журнал "Концепт". — 2024. — № 11. — С. 421-427. — ISSN 2304-120X. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/367094. — Режим доступа: для авториз. пользователей.

5. Петрова, А.В. Анализ и оценка кадровой безопасности предприятия / А. В. Петрова, В. А. Тераз // Менеджмент: теория и практика. — 2024. — № 1-2. — С. 135-138. — ISSN 2310-0613. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/363143. — Режим доступа: для авториз. пользователей.

6. Правовое обеспечение кадровой безопасности в системе информационной безопасности донецкой народной республики / Н. А. Тимошенко, N. Timoshenko, К. Е. Свиридова, K. Sviridova // Вестник Донецкого национального университета. Серия Е: Юридические науки. — 2020. — № 4. — С. 66-71. — ISSN 2664-374X. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/344570. — Режим доступа: для авториз. пользователей.

8.2. Дополнительная литература

1. Иванова С. В. Искусство подбора персонала: как оценить человека за час / С. В. Иванова. -Москва : Альпина Паблишер, 2021. -312 с. -ISBN 978-5-9614-3256-2.

2. Литвинюк А. А. Оценка персонала : учебник для вузов / А. А. Литвинюк. -Москва : Юрайт, 2023. -304 с. -(Высшее образование). -ISBN 978-5-534-09873-4.

3. Спенсер Л. М., Спенсер С. М. Компетенции на работе. Модели максимальной эффективности работы / пер. с англ. -М. : HIPPO, 2019. -384 с. - ISBN 978-5-00000-021-8.

4. Чуланова О. Л. Кадровый документооборот : учебное пособие / О. Л. Чуланова. -Москва : ИНФРА-М, 2024. -256 с. - (Среднее профессиональное образование). -ISBN 978-5-16-017845-7.

8.3. Нормативные правовые документы и иная правовая информация

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 22.04.2025). -Доступ из справ.-правовой системы «КонсультантПлюс».

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.02.2025). -Доступ из справ.-правовой системы «КонсультантПлюс».

3. Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» (ред. от 29.12.2024). -Доступ из справ.-правовой системы «Гарант».

4. Постановление Госкомстата России от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (ред. от 27.03.2023). -Доступ из справ.-правовой системы «КонсультантПлюс».

5. Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов…» (с изм. от 14.06.2024). -Доступ из справ.-правовой системы «КонсультантПлюс».

6. Профессиональные стандарты (по актуальному перечню Минтруда России). -Режим доступа: https://profstandart.rosmintrud.ru (официальный сайт).

8.4. Интернет-ресурсы

1. Электронно-библиотечная система «Юрайт» : https://urait.ru – доступ через личный кабинет РАНХиГС (по подписке)

2. Электронно-библиотечная система Znanium : https://znanium.com – доступ через университетскую сеть

3. Электронная библиотека IPRbooks : http://www.iprbookshop.ru/ – доступ по логину/паролю (справка в библиотеке)

4. Справочно-правовая система «КонсультантПлюс» : http://www.consultant.ru/ – свободный доступ к кодексам и текущему законодательству

5. Справочно-правовая система «Гарант» : http://www.garant.ru/ – свободный доступ к основным актам

6. Официальный интернет-портал правовой информации : http://pravo.gov.ru/ – бесплатно, официальные публикации законов

7. Российская государственная библиотека (РГБ) : https://www.rsl.ru/ – доступ к каталогам и электронным диссертациям

8. КиберЛенинка (научные статьи по HR и психологии труда) : https://cyberleninka.ru/ – свободный доступ

9. Профессиональный портал «HR-Лига» : https://www.hrliga.com/ – методические материалы и обзоры по подбору персонала

10. Портал «Работа в России» (аналитика рынка труда) : https://trudvsem.ru/ – государственная информационная система

11. Онлайн-библиотека по социологии и психологии труда (соционет) : http://www.socionet.ru/ – открытый доступ

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Требования к аудиториям

- Лекционные занятия: учебная аудитория для проведения лекций (вместимость не менее количества обучающихся в группе) с возможностью демонстрации презентаций и нормативных документов.
- Семинарские (практические) занятия: аудитория для практических занятий, оборудованная рабочими местами для обучающихся и преподавателя, с возможностью групповой работы (в том числе в малых группах).
- Помещения для самостоятельной работы: читальный зал или специализированная аудитория с доступом к сети Интернет и лицензионным электронно-библиотечным системам (ЭБС) для самостоятельной подготовки, выполнения расчётных заданий, написания докладов и рефератов.

Требования к оборудованию

- Доска (меловая или маркерная) – для схем, таблиц, разбора кейсов.
- Мультимедийный проектор – для демонстрации презентаций, видеоматериалов, нормативных документов.
- Персональный компьютер (стационарный) или ноутбук для преподавателя (или стационарный компьютер в аудитории) с характеристиками: операционная система не ниже Windows 7 (или аналогичная по функциям, например, macOS, Linux с графической оболочкой).
- При необходимости – ноутбук или планшет для студентов при выполнении групповых заданий (может быть предусмотрен мобильный класс).

Требования к программному обеспечению

- Пакет Microsoft Office (или его бесплатный аналог, например, LibreOffice) для подготовки документов, презентаций, таблиц (в том числе для построения матриц сравнения кандидатов, чек-листов, анализа воронки подбора).
- При наличии лицензий – специализированное ПО для HR-аналитики (необязательно, но рекомендуется для демонстрации):
  - *Профильное ПО* (например: «1С:Зарплата и управление персоналом», «БОСС-Кадровик», ATS-системы в ознакомительном режиме).
- Антивирусное программное обеспечение (например, Kaspersky, Dr.Web – по наличию).

Информационные справочные системы (доступ через сеть Интернет)

- Справочно-правовая система «КонсультантПлюс» – для доступа к ТК РФ, ФЗ-152, ФЗ-125, постановлениям Госкомстата, судебной практике по трудовым

спорам.
Режим доступа: http://www.consultant.ru – бесплатный доступ к основным актам; полные версии – по подписке образовательной организации.

- Справочно-правовая система «Гарант» – альтернативный источник правовой информации.

Режим доступа: http://www.garant.ru

- Официальный интернет-портал правовой информации (правовой портал) – официальное опубликование законов.

Режим доступа: http://pravo.gov.ru

- Профессиональные стандарты (официальный реестр Минтруда России) – для изучения требований к должностям.

Режим доступа: https://profstandart.rosmintrud.ru

- Электронно-библиотечные системы (ЭБС) – Юрайт, Znanium, IPRbooks (доступ через университетскую сеть или по логину/паролю).
- Поисковые системы общего назначения (Yandex, Google) – для отработки навыков X-Ray-поиска и Boolean-запросов (в рамках тем 1.5 и 2.1).

Доступ к сети Интернет

Для всех помещений, используемых при проведении лекционных, семинарских занятий и для самостоятельной работы, обеспечивается возможность подключения к информационно-телекоммуникационной сети Интернет (по проводной или беспроводной технологии, скорость – не менее 1 Мбит/с на одно рабочее место).