

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Костровец Лариса Борисовна
Должность: директор
Дата подписания: 17.05.2026 16:10:01
Уникальный программный ключ:
6882606104c36dbde41c4ab93a65382136a292d6

Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.01 Деловая коммуникация и защита персональных данных
(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.03 Управление персоналом
(код, наименование направления подготовки)

Управление персоналом организации и государственной службы
(наименование образовательной программы)

очная форма обучения
(форма обучения)

Год набора – 2026

Донецк

Автор(ы)-составитель(и) РПД:

Горун Валентина Викторовна, старший преподаватель кафедры управления персоналом и экономики труда

Заведующий кафедрой:

Стадник Алла Мироновна, канд.гос.упр., доцент, заведующий кафедрой управления персоналом и экономики труда

Рабочая программа дисциплины Б1.В.01.01 Деловая коммуникация и защита персональных данных одобрена на заседании кафедры управления персоналом и экономики труда факультета государственной службы и управления 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.01.01 Деловая коммуникация и защита персональных данных обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС (при наличии)	Код компетенции	Наименование компетенции	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Образовательный результат
В/01.6 Сбор информации о потребностях организации в персонале 07.003 Специалист по управлению персоналом, утв. Приказом Минтруда и социальной защиты РФ от 09.03.2022 №109н	ПК-1	Способен управлять процессами поиска, подбора и отбора персонала	ПК-1.4	Проводит отбор, оценку кандидатов и бюджетирование процесса подбора персонала	<i>ПК-1.4 3-5 Знает технологии, методы и методики проведения анализа, систематизации документов и информации;</i> <i>ПК-1.4 3-18 Знает законодательство Российской Федерации о персональных данных.</i>
В/01.6 Сбор информации о потребностях организации в персонале 07.003 Специалист по управлению персоналом, утв. Приказом Минтруда и социальной защиты РФ от 09.03.2022 №109н	ПК-1	Способен управлять процессами поиска, подбора и отбора персонала	ПК-1.5	Организовывает и контролирует процессы аттестации и оценки персонала	<i>ПК-1.5. 3-20 Знает правила ведения деловой переписки.</i>

F/01.6 Разработка корпоративной социальной политики 07.003 Специалист по управлению персоналом, утв. Приказом Минтруда и социальной защиты РФ от 09.03.2022 №109н	ПК-4	Способен разрабатывать корпоративную социальную политику с учетом стратегии развития организации	ПК-4.3	Организует взаимодействие с представителями органами работников, общественным и организациями и государственными органами	ПК-4.3 3-16 Знает нормативные правовые акты, регулирующие права и обязанности государственных органов, представительных органов работников; ПК-4.3 3-20 Знает правила ведения деловой переписки. ПК-4.3 У-10 Умеет обеспечивать соблюдение требований законодательства Российской Федерации и корпоративных политик работодателя в области обработки персональных данных и конфиденциальной информации ПК-4.3 У-11 Умеет вести деловую переписку.
--	------	--	--------	---	--

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

Общий объем дисциплины:

2,00 з.е., 72 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 40 ак. час на контактную работу с преподавателем, из них 18 ак.час на лекции и 18 ак.час на практические занятия. 32 ак. час на самостоятельную работу обучающихся.

Б1.В.01.01 Деловая коммуникация и защита персональных данных реализуется в 4-м семестре 2-го курса.

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	Кат.тэк	Контроль	СРкр	СРэк		СР
Л	ВЛ	ЛР	ПЗ												
Тема 1.	Правовой режим персональных данных в HR-процессах: от сбора до уничтожения	14	4	0	0	4	0	0	0	0	0	0	0	6	Доклады, Тестирование
Тема 2.	Конфиденциальность в цифровых коммуникациях: мессенджеры, e-mail и видеоконферен	14	4	0	0	4	0	0	0	0	0	0	0	6	Доклады, Тестирование

	ции													
Тема 3.	Этика и безопасность при сборе анкет, резюме и проведении интервью (включая видео-формат)	14	4	0	0	4	0	0	0	0	0	0	6	Доклады, Тестирование
Тама 4.	Управление инцидентами и претензиями: утечка ПДн как кризисная коммуникация	14	4	0	0	4	0	0	0	0	0	0	6	Опрос, Контрольное задание
Тема 5.	Обучение сотрудников и внутренний контроль: как внедрить культуру защиты ПДн через корпоративные коммуникации	12	2	0	0	2	0	0	0	0	0	0	8	Опрос, Контрольное задание
Промежуточная аттестация		4	0	0	0	0	0	0	0	4	0	0	0	Зачет
Итого		72	18	0	0	18	0	0	0	4	0	0	32	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

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

Тема 1. Правовой режим персональных данных в HR-процессах: от сбора до уничтожения. ПК-1.4; ПК-1.5; ПК-4.3.

Категории ПДн (обычные, специальные, биометрические), согласие на обработку, порядок работы с документами соискателей и сотрудников, сроки хранения личных дел, процедура уничтожения данных при увольнении.

Тема 2. Конфиденциальность в цифровых коммуникациях: мессенджеры, e-mail и видеоконференции. ПК-1.4; ПК-1.5; ПК-4.3.

Риски утечки данных в Teams, Zoom, Telegram, WhatsApp. Корпоративная переписка как объект защиты. Правила использования служебного e-mail (рассылки, «Reply All», передача данных третьим лицам). Защита от фишинга и социальной инженерии.

Тема 3. Этика и безопасность при сборе анкет, резюме и проведении интервью (включая видео-формат). ПК-1.4; ПК-1.5; ПК-4.3.

Что можно и нельзя спрашивать у кандидата (избегание дискриминационных и избыточных данных). Хранение и доступ к базе резюме. Запись видеособеседований и согласие на обработку данных. Особенности для государственной службы (проверки, допуски).

Тема 4. Управление инцидентами и претензиями: утечка ПДн как кризисная коммуникация. ПК-1.4; ПК-1.5; ПК-4.3.

Действия HR-службы и отдела персонала при компрометации данных (внутренняя или внешняя утечка). Алгоритм уведомления Роскомнадзора, работников и клиентов. Коммуникационные шаблоны для объяснения ситуации и сохранения репутации организации/госоргана.

Тема 5. Обучение сотрудников и внутренний контроль: как внедрить культуру защиты ПДн через корпоративные коммуникации. ПК-1.4; ПК-1.5; ПК-4.3.

Разработка памяток, чек-листов и e-learning курсов для персонала (особенно для линейных руководителей и секретариата). Роль HR в проведении внутренних аудитов и «фейковых фишинговых рассылок». Дисциплинарная ответственность за нарушение режима ПДн.

4. Типы оценочных материалов, показатели и критерии

оценивания

4.1. Оценочные материалы по дисциплине Б1.В.01.01 Деловая коммуникация и защита персональных данных 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	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, В). 	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 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	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 	Ответ считается верным, если правильно указана вся последовательность цифр

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

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	D
60-69	E			P/ Passed
35-59	Неудовлетворительно	Не зачтено	F	F/Failed
0-34			FX	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
60 баллов	40 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.01.01 Деловая коммуникация и защита персональных данных используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

доклад, опрос, тестирование.

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

Тема 1. Правовой режим персональных данных в HR-процессах: от сбора до уничтожения. ПК-1.4; ПК-1.5; ПК-4.3.

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.

Какое действие HR-специалиста соответствует требованиям законодательства о персональных данных (на примере РФ — ФЗ-152) при увольнении сотрудника?

Варианты ответов:

А) Передать личное дело сотрудника новому работодателю по устному запросу самого сотрудника.

Б) Хранить все личные дела уволенных сотрудников бессрочно в бумажном архиве.

В) Уничтожить или обезличить персональные данные сотрудника по истечении срока хранения, если иное не предусмотрено законом (например, по требованию налоговых органов).

Г) Отправить копии всех документов сотрудника по электронной почте его бывшему коллеге для «истории отдела».

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 действий HR-специалиста соответствуют требованиям законодательства о персональных данных (ФЗ-152)?

Варианты ответов:

А) Получение письменного согласия на обработку персональных данных сотрудника, если иное не предусмотрено трудовым договором.

Б) Передача копий паспортов всех сотрудников охранному предприятию

по устному распоряжению генерального директора.

В) Уничтожение личных дел кандидатов, не прошедших собеседование, после истечения установленного срока хранения (если нет иных законных оснований).

Г) Обезличивание персональных данных сотрудников перед передачей статистической отчетности в стороннюю организацию.

Д) Хранение сканов СНИЛС и ИНН сотрудников в общедоступной папке на файлообменнике без пароля.

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.

Расположите в правильной последовательности этапы работы HR-специалиста с персональными данными сотрудника от момента приема на работу до момента окончания обработки (согласно типовому документообороту).

Элементы:

1. Уничтожение или обезличивание ПДн после истечения срока хранения
2. Получение письменного согласия на обработку ПДн (или ознакомление с локальным актом)
3. Сбор и фиксация ПДн из документов, предоставленных сотрудником (паспорт, СНИЛС, ИНН, трудовая книжка)
4. Передача части ПДн в сторонние организации (налоговая, ПФР, банк для зарплатного проекта)
5. Хранение личного дела в архиве отдела кадров с разграничением доступа.

Тема 2. Конфиденциальность в цифровых коммуникациях: мессенджеры, e-mail и видеоконференции. ПК-1.4; ПК-1.5; ПК-4.3.

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.

Какой вариант действий минимизирует риск утечки персональных данных при использовании корпоративной электронной почты в работе HR-службы?

Варианты ответов:

А) Отправка незашифрованных сканов паспорта сотрудника на личный e-mail руководителя сторонней организации.

Б) Использование функции автоматического перевода всех входящих писем в общедоступную облачную папку.

В) Настройка автоматической блокировки отправки писем, содержащих ПДн (например, номера телефонов, СНИЛС), на внешние домены без шифрования или согласования.

Г) Копирование всех HR-рассылок («Всем сотрудникам») в мессенджер с уведомлением «для скорости».

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 меры считаются правильными для защиты персональных данных при ведении деловой переписки и использовании цифровых каналов?

Варианты ответов:

А) Использование корпоративной почты с шифрованием при отправке документов, содержащих паспортные данные.

Б) Отправка паролей от учетных записей сотрудников в личные сообщения Telegram для оперативности.

В) Запрет на пересылку служебной информации с ПДн на личную электронную почту или в мессенджеры.

Г) Настройка автоматического удаления писем с конфиденциальными вложениями из «Отправленных» через определенный срок.

Д) Копирование всех HR-рассылок в общий чат компании в WhatsApp для «повышения информированности».

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.

Расположите в правильной последовательности алгоритм действий HR-специалиста при необходимости направить внешнему контрагенту (аудиторской фирме) скан-копии паспортов двух сотрудников по электронной почте.

Элементы:

1. Отправка зашифрованного письма получателю с контролем доставки
2. Уточнение у руководителя службы безопасности или ответственного за ПДн, разрешена ли такая передача и на каком основании (договор, поручение)
3. Архивирование файлов с установкой пароля на архив
4. Запрос у получателя подтверждения готовности принять конфиденциальную информацию и обеспечить её защиту
5. Передача пароля от архива по иному каналу (телефон, SMS, отдельное сообщение в защищенном мессенджере)

Тема 3. Этика и безопасность при сборе анкет, резюме и проведении интервью (включая видео-формат). ПК-1.4; ПК-1.5; ПК-4.3.

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 ходе видеособеседования кандидат сообщил о своей религии и семейном положении. Какое действие HR-специалиста будет этичным и правомерным?

Варианты ответов:

А) Занести эту информацию в базу кандидата как дополнительное преимущество.

Б) Запросить письменное согласие на обработку специальных категорий ПДн прямо во время интервью.

В) Проигнорировать эту информацию, не фиксировать её в анкете и не учитывать при принятии решения о найме, так как она не относится к деловым качествам.

Г) Сообщить эту информацию будущему непосредственному руководителю кандидата для оценки совместимости в коллективе.

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 действия HR-специалиста являются этичными и правомерными при работе с кандидатами?

Варианты ответов:

А) Заранее (до собеседования) уведомить кандидата о том, что видеоконференция будет записываться, и получить его согласие.

Б) Требовать от всех кандидатов предоставления справки об отсутствии судимости, даже если должность этого не требует по закону.

В) Удалять резюме и анкеты кандидатов, которые не были допущены к следующему этапу, после истечения срока, необходимого для закрытия вакансии.

Г) Отказать в обработке биометрических данных (например, фото для пропуска) без отдельного письменного согласия кандидата.

Д) Запрашивать информацию о наличии беременности или планировании детей у всех женщин-соискательниц, чтобы «планировать отпуска».

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.

Расположите в правильной последовательности действия HR-специалиста при проведении видеособеседования с записью (согласно этико-правовым нормам).

Элементы:

1. Запуск записи видеоконференции
2. Объяснение целей записи (например: «для согласования с руководителем отдела», «для оценки качества собеседований»)
3. Устное предупреждение кандидата о том, что собеседование будет записываться
4. Получение явного согласия кандидата (словесное «да» или отметка в чате)
5. Размещение ссылки на видеоконференцию в приглашении с пометкой о возможной записи (предварительное информирование)

Тема 4. Управление инцидентами и претензиями: утечка ПДн как кризисная коммуникация. ПК-1.4; ПК-1.5; ПК-4.3.

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 HR-отделе произошла утечка: файл с зарплатами и паспортными данными 50 сотрудников случайно попал в открытый доступ на файловом сервере. Какое действие является первым шагом внутренней коммуникации согласно стандартам кризисного управления?

Варианты ответов:

А) Немедленно отправить объяснительную генеральному директору с

просьбой об увольнении виновного.

Б) Разослать всем сотрудникам компании уведомление «Извините, мы ошиблись, но ничего страшного не произошло».

В) Зафиксировать факт утечки (время, объём, характер данных) и запустить внутреннее расследование, после чего подготовить согласованное сообщение для пострадавших лиц и контролирующих органов.

Г) Удалить файл и сделать вид, что ничего не случилось, чтобы избежать паники.

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.

При обнаружении утечки персональных данных (например, файл с ПДн 100 сотрудников оказался в публичном доступе) какие коммуникационные шаги являются обязательными и корректными?

Варианты ответов:

А) Внутреннее уведомление руководителя службы безопасности или лица, ответственного за обработку ПДн в организации.

Б) Публикация новости об утечке в соцсетях компании до выяснения всех обстоятельств.

В) Уведомление Роскомнадзора (в РФ) в установленный законом срок после фиксации инцидента.

Г) Подготовка корректного сообщения для пострадавших сотрудников с описанием реальных рисков и рекомендаций (без паники и излишних деталей).

Д) Срочный массовый звонок всем сотрудникам компании для устных извинений без документального оформления.

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.

Расположите в правильной последовательности шаги кризисной коммуникации HR-службы и службы безопасности при обнаружении утечки

персональных данных сотрудников.

Элементы:

1. Подготовка и направление уведомления в Роскомнадзор (в установленный законом срок)
2. Фиксация факта утечки (время, объём данных, причина, круг лиц, получивших доступ)
3. Составление внутреннего отчета для руководства и запуск служебного расследования
4. Уведомление пострадавших сотрудников о факте утечки и рекомендации по снижению рисков (без паники)
5. Локализация инцидента (удаление доступа, отключение ресурса, изъятие носителя)

Тема 5. Обучение сотрудников и внутренний контроль: как внедрить культуру защиты ПДн через корпоративные коммуникации. ПК-1.4; ПК-1.5; ПК-4.3.

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

Какая практика обучения наиболее эффективна для проверки реальной готовности линейных руководителей (не HR) защищать персональные данные в повседневной работе?

Варианты ответов:

А) Ежегодное онлайн-тестирование «15 правил ФЗ-152» без обратной связи по ошибкам.

Б) Рассылка памятки «10 заповедей защиты ПДн» на корпоративную почту.

В) Проведение скрытого аудита — отправка сотрудникам (по инициативе отдела безопасности) фишингового письма с просьбой предоставить пароль или данные коллеги и последующий разбор результатов.

Г) Устное объявление на планерке: «Будьте осторожны с данными, а то оштрафуют».

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 методы обучения и контроля эффективно формируют культуру защиты персональных данных у сотрудников (включая линейных руководителей)?

Варианты ответов:

А) Регулярные (например, раз в полгода) внутренние рассылки с разбором реальных кейсов утечек и ошибок (без указания имен).

Б) Включение вопросов о работе с ПДн в программу онбординга (адаптации) новых сотрудников.

В) Проведение анонимных опросов сотрудников о том, соблюдают ли они правила защиты ПДн (с последующим анализом «слепых зон»).

Г) Штраф всех сотрудников, которые переписываются по рабочим вопросам в личных чатах, без разъяснения альтернатив.

Д) Организация «псевдофишинговых» рассылок (симуляция атаки) от имени IT-службы с последующим обучением тех, кто «попался».

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.

Расположите в правильной последовательности этапы внедрения системы внутреннего контроля и обучения сотрудников защите персональных данных через корпоративные коммуникации.

Элементы:

1. Разработка простых памяток и чек-листов «Что делать / чего не делать с ПДн» для разных категорий сотрудников

2. Оценка текущего уровня знаний и выявление «слепых зон» (анонимный опрос, базовое тестирование)

3. Проведение скрытых аудитов (симуляция фишинга, проверка оставленных документов)

4. Разбор с сотрудниками результатов скрытых аудитов и ошибок (без публичных наказаний)

5. Запуск регулярного обучения (вебинары, e-learning, кейсы в корпоративной рассылке) на основе выявленных проблем

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

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	0,2	20
КТ 3	100	0,3	30
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

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

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

КТ – 1.

Тема 1.

Доклад:

Подготовка докладов по теме: Конфиденциальность в цифровых коммуникациях: мессенджеры, e-mail и видеоконференции.

Тематика докладов:

1. Сравнительный анализ правовых режимов персональных данных в РФ, ЕС (GDPR) и США: последствия для транснациональных HR-процессов.

2. Особенности получения и оформления согласия на обработку специальных категорий персональных данных (биометрия, состояние здоровья, расовая принадлежность).

3. Правовые последствия обработки персональных данных без согласия работника: судебная практика и административные штрафы.

4. Сроки хранения личных дел сотрудников: пересечение требований трудового, архивного законодательства и ФЗ-152.

5. Порядок уничтожения персональных данных при ликвидации организации или увольнении сотрудника: документальное оформление.

6. Ответственность HR-службы за трансграничную передачу персональных данных (удаленные сотрудники, зарубежные командировки).

7. Обезличивание персональных данных как альтернатива уничтожению: методы, риски и примеры использования в HR-аналитике.

8. Особенности обработки персональных данных умерших сотрудников: правовой статус и доступ наследников.

9. Типичные нарушения законодательства о ПДн в работе отдела кадров малого и среднего бизнеса (по материалам судебных решений).

10. Разработка локального акта «Политика в отношении обработки персональных данных» для HR-службы: структура и обязательные элементы.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале

которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

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	

КТ – 2.

Тема 2.

Опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Почему использование WhatsApp, Telegram или Viber для передачи сканов паспортов сотрудников считается рискованным? Какие альтернативы предлагает законодательство?
2.	Что такое шифрование электронной почты? Какие виды шифрования существуют (TLS, PGP, S/MIME)?
3.	Какие данные можно считать «косвенными персональными данными» в подписи к электронному письму (на примере должности, телефона,

	фото)?
4.	Каковы правовые последствия случайной отправки файла с ПДн «не тому адресату» (опция «Reply All»)? Приведите пример из HR-практики.
5.	Перечислите обязательные элементы регламента использования корпоративной электронной почты для отдела кадров.
6.	Можно ли записывать видеособеседования и онлайн-совещания без явного предупреждения участников? Почему да или почему нет?
7.	Какие настройки доступа к облачным хранилищам (Google Drive, Яндекс.Диск) должен установить HR-отдел, чтобы не нарушать конфиденциальность?
8.	Что такое фишинговая атака на HR-отдел? Приведите два типичных сценария (письмо от «директора» с просьбой выслать зарплатные ведомости и т.п.).
9.	Какие технические средства помогают автоматически блокировать отправку писем, содержащих номера СНИЛС или паспортов, на внешние домены?
10.	Каков порядок действий HR-специалиста, если он случайно отправил конфиденциальный файл не тому внешнему контрагенту?

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
90-100	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.
75-89	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.
60-74	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.
0-59	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

КТ – 3.

Тема 3-4.

Тестовые задания с инструкцией по выполнению:

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 вариант действий минимизирует риск утечки персональных данных при использовании корпоративной электронной почты в работе HR-службы?

Варианты ответов:

А) Отправка незашифрованных сканов паспорта сотрудника на личный e-mail руководителя сторонней организации.

Б) Использование функции автоматического перевода всех входящих писем в общедоступную облачную папку.

В) Настройка автоматической блокировки отправки писем, содержащих ПДн (например, номера телефонов, СНИЛС), на внешние домены без шифрования или согласования.

Г) Копирование всех HR-рассылок («Всем сотрудникам») в мессенджер с уведомлением «для скорости».

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 меры считаются правильными для защиты персональных данных при ведении деловой переписки и использовании цифровых каналов?

Варианты ответов:

А) Использование корпоративной почты с шифрованием при отправке документов, содержащих паспортные данные.

Б) Отправка паролей от учетных записей сотрудников в личные сообщения Telegram для оперативности.

В) Запрет на пересылку служебной информации с ПДн на личную электронную почту или в мессенджеры.

Г) Настройка автоматического удаления писем с конфиденциальными вложениями из «Отправленных» через определенный срок.

Д) Копирование всех HR-рассылок в общий чат компании в WhatsApp для «повышения информированности».

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.

Расположите в правильной последовательности шаги кризисной коммуникации HR-службы и службы безопасности при обнаружении утечки персональных данных сотрудников.

Элементы:

1. Подготовка и направление уведомления в Роскомнадзор (в установленный законом срок)

2. Фиксация факта утечки (время, объём данных, причина, круг лиц, получивших доступ)

3. Составление внутреннего отчета для руководства и запуск служебного расследования

4. Уведомление пострадавших сотрудников о факте утечки и рекомендации по снижению рисков (без паники)

5. Локализация инцидента (удаление доступа, отключение ресурса, изъятие носителя).

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
90-100	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
75-89	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
60-74	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-59	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

КТ – 4.

Тема 5.

Контрольные задания:

Задание 1.

Вы — руководитель отдела персонала (HR-Director) крупной розничной компании (500+ сотрудников). В компании действует «Политика обработки персональных данных», все сотрудники под подпись ознакомлены с правилами. Однако за последние полгода зафиксировано 4 инцидента:

Секретарь отправила в общий чат WhatsApp сканы паспортов трёх новых сотрудников «для быстрого оформления пропусков».

Начальник склада оставил распечатанный список с ФИО, паспортными данными и зарплатами на видном месте стола; список сфотографировал уборщик.

Менеджер по продажам переслал на личную почту внешнего аудитора файл с данными (СНИЛС, ИНН) всего отдела продаж, так как «аудитор попросил срочно».

Бухгалтер скачала файл с зарплатной ведомостью на домашний компьютер без шифрования, компьютер заразился вирусом.

Все нарушители сказали примерно одно и то же: «Я не знал(а), что это нарушение. Думал(а), что раз делаю для работы, то можно. Нас предупреждали на подпись, но я не вникал(а), там много текста».

Ваше задание:

Вы решаете не ограничиваться только наказаниями (выговор -

депремирование), а внедрить инструмент корпоративной коммуникации и обучения, который системно повлияет на культуру обращения с ПДн.

Выберите ОДИН наиболее эффективный вариант действий (или предложите свой) и подробно обоснуйте, почему он лучше остальных.

Варианты действий:

А. Провести общее собрание всего коллектива, где публично объявить о штрафах за нарушение правил работы с ПДн, пригрозить увольнением за повторное нарушение и зачитать выдержки из ФЗ-152.

Б. Разработать обязательный 20-минутный электронный курс (e-learning) с видео-кейсами (анимированные ситуации, похожие на те, что произошли), коротким тестом после каждой главы и автоматическим напоминанием тем, кто не прошел. Курс должны пройти 100% сотрудников, результат засчитывается только при правильных ответах на вопросы по каждому кейсу.

В. Каждому нарушителю выдать индивидуальное задание: написать объяснительную и переписать от руки главу из «Политики обработки ПДн». Остальных сотрудников больше не беспокоить, чтобы не создавать «информационный шум».

Г. Раз в квартал проводить скрытый аудит («псевдофишинг»): отправлять сотрудникам от имени технического специалиста или руководителя письмо с просьбой прислать файл с персональными данными коллег. Тех, кто «попался», наказывать рублём, а лучшие результаты публиковать в топ-3 по отделам.

Критерии оценивания контрольных заданий:

Диапазон баллов	Описание критерия
90-100	Обучающимся задание выполнено без ошибок и в полном объеме.
75-89	Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
60-74	Обучающимся допущены отдельные ошибки при выполнении задания
0-59	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

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

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

6.1. Промежуточная аттестация (зачет) проводится в письменной форме. Обучающийся получает задание. Обучающийся получает чистые маркированные листы бумаги для записей, затем приступает к решению. Необходимо дать ответ в письменном виде, подробно изложив ход мышления, при необходимости завершить выводами.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Правовой режим персональных данных в HR-процессах: от сбора до уничтожения. УК-6.3; ОПК-1.2; ПК-5.1.

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Дайте определение персональных данных согласно ФЗ-152. Какие сведения о сотруднике НЕ относятся к персональным данным?
2.	Перечислите категории персональных данных (общедоступные, специальные, биометрические). Приведите примеры каждой категории применительно к HR-процессам.

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	HR-специалист получил письменное согласие сотрудника на обработку персональных данных. Через год сотрудник уволился. Какое действие является правомерным? Варианты:		

	<p>А) Хранить личное дело сотрудника бессрочно «на всякий случай».</p> <p>Б) Уничтожить все персональные данные сотрудника на следующий день после увольнения.</p> <p>В) Продолжать хранение личного дела в течение срока, установленного трудовым и архивным законодательством (например, 75 лет для приказов о приеме), а после его истечения уничтожить или обезличить данные.</p> <p>Г) Передать личное дело сотрудника ему лично под расписку.</p>		
2.	<p>Какие действия HR-специалиста требуют получения отдельного письменного согласия сотрудника (помимо базового согласия, включенного в трудовой договор)?</p> <p>Варианты:</p> <p>А. Передача персональных данных сотрудника аутсорсинговой компании для расчета зарплаты, если такая передача не предусмотрена трудовым договором.</p> <p>Б. Внесение в базу учета фамилии, имени, отчества и должности сотрудника для внутреннего телефонного справочника.</p> <p>В. Обработка биометрических данных сотрудника (отпечатки пальцев для пропускной системы).</p> <p>Г. Передача персональных данных сотрудника третьей стороне за пределами целей, заявленных при сборе.</p> <p>Д. Хранение копии паспорта в личном деле, если это прямо предусмотрено внутренними локальными актами и трудовым договором</p>		

3. Задания закрытого типа.

3.1. 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.

Какое действие HR-специалиста соответствует требованиям законодательства о персональных данных (на примере РФ — ФЗ-152) при увольнении сотрудника?

Варианты ответов:

А) Передать личное дело сотрудника новому работодателю по устному запросу самого сотрудника.

Б) Хранить все личные дела уволенных сотрудников бессрочно в бумажном архиве.

В) Уничтожить или обезличить персональные данные сотрудника по истечении срока хранения, если иное не предусмотрено законом (например, по требованию налоговых органов).

Г) Отправить копии всех документов сотрудника по электронной почте его бывшему коллеге для «истории отдела».

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 действий HR-специалиста соответствуют требованиям законодательства о персональных данных (ФЗ-152)?

Варианты ответов:

А) Получение письменного согласия на обработку персональных данных сотрудника, если иное не предусмотрено трудовым договором.

Б) Передача копий паспортов всех сотрудников охранному предприятию

по устному распоряжению генерального директора.

В) Уничтожение личных дел кандидатов, не прошедших собеседование, после истечения установленного срока хранения (если нет иных законных оснований).

Г) Обезличивание персональных данных сотрудников перед передачей статистической отчетности в стороннюю организацию.

Д) Хранение сканов СНИЛС и ИНН сотрудников в общедоступной папке на файлообменнике без пароля.

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.

Расположите в правильной последовательности этапы работы HR-специалиста с персональными данными сотрудника от момента приема на работу до момента окончания обработки (согласно типовому документообороту).

Элементы:

1. Уничтожение или обезличивание ПДн после истечения срока хранения
2. Получение письменного согласия на обработку ПДн (или ознакомление с локальным актом)
3. Сбор и фиксация ПДн из документов, предоставленных сотрудником (паспорт, СНИЛС, ИНН, трудовая книжка)
4. Передача части ПДн в сторонние организации (налоговая, ПФР, банк для зарплатного проекта)
5. Хранение личного дела в архиве отдела кадров с разграничением доступа.

Тема 2. Конфиденциальность в цифровых коммуникациях: мессенджеры, e-mail и видеоконференции. УК-6.3; ОПК-1.2; ПК-5.1.

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Почему использование WhatsApp, Telegram или Viber для передачи сканов паспортов сотрудников считается рискованным? Какие альтернативы предлагает законодательство?
2.	Что такое шифрование электронной почты? Какие виды шифрования существуют (TLS, PGP, S/MIME)?

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	<p>HR-специалисту нужно срочно направить внешнему аудитору скан-копии паспортов трех сотрудников. Какой способ будет наиболее безопасным с точки зрения защиты персональных данных?</p> <p>Варианты:</p> <p>А) Отправить файлы через WhatsApp, так как это быстро и удобно.</p> <p>Б) Вложить файлы в обычное письмо на корпоративную почту аудитора без пароля.</p> <p>В) Заархивировать файлы с паролем, отправить архив по корпоративной почте, а пароль передать аудитору по телефону или в защищенном мессенджере.</p> <p>Г) Выложить файлы в общую папку на Google Диске со ссылкой для всех желающих.</p>		
2.	<p>Расположите в правильной последовательности действия HR-специалиста после того, как он обнаружил, что отправил по электронной почте файл с персональными данными сотрудников совершенно постороннему адресату (ошибочная рассылка).</p>		

	<p>Элементы:</p> <ol style="list-style-type: none"> 1. Уведомить своего непосредственного руководителя и ответственного за обработку ПДн. 2. Попытаться отозвать письмо (функция Recall в Outlook или аналоги) или связаться с получателем с просьбой удалить письмо. 3. Зафиксировать факт инцидента (время, адресат, состав данных). 4. Подготовить внутреннюю служебную записку для возможного расследования 		
--	---	--	--

3. Задания закрытого типа.

3.1. 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.

Какой вариант действий минимизирует риск утечки персональных данных при использовании корпоративной электронной почты в работе HR-службы?

Варианты ответов:

А) Отправка незашифрованных сканов паспорта сотрудника на личный e-mail руководителя сторонней организации.

Б) Использование функции автоматического перевода всех входящих писем в общедоступную облачную папку.

В) Настройка автоматической блокировки отправки писем, содержащих ПДн (например, номера телефонов, СНИЛС), на внешние домены без шифрования или согласования.

Г) Копирование всех HR-рассылок («Всем сотрудникам») в мессенджер с уведомлением «для скорости».

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 меры считаются правильными для защиты персональных данных при ведении деловой переписки и использовании цифровых каналов?

Варианты ответов:

А) Использование корпоративной почты с шифрованием при отправке документов, содержащих паспортные данные.

Б) Отправка паролей от учетных записей сотрудников в личные сообщения Telegram для оперативности.

В) Запрет на пересылку служебной информации с ПДн на личную электронную почту или в мессенджеры.

Г) Настройка автоматического удаления писем с конфиденциальными вложениями из «Отправленных» через определенный срок.

Д) Копирование всех HR-рассылок в общий чат компании в WhatsApp для «повышения информированности».

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.

Расположите в правильной последовательности алгоритм действий HR-специалиста при необходимости направить внешнему контрагенту (аудиторской фирме) скан-копии паспортов двух сотрудников по электронной почте.

Элементы:

1. Отправка зашифрованного письма получателю с контролем доставки
2. Уточнение у руководителя службы безопасности или ответственного за ПДн, разрешена ли такая передача и на каком основании (договор, поручение)

3. Архивирование файлов с установкой пароля на архив
4. Запрос у получателя подтверждения готовности принять конфиденциальную информацию и обеспечить её защиту
5. Передача пароля от архива по иному каналу (телефон, SMS, отдельное сообщение в защищенном мессенджере)

Тема 3. Этика и безопасность при сборе анкет, резюме и проведении интервью (включая видео-формат). УК-6.3; ОПК-1.2; ПК-5.1.

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Какие вопросы НЕЛЬЗЯ задавать кандидату на собеседовании с точки зрения этики и законодательства о персональных данных (минимум 5 примеров)?
2.	Вправе ли HR-специалист потребовать у кандидата справку о несудимости для должности, не связанной с детьми или гостайной? Обоснуйте ответ.

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	<p>На собеседовании кандидат добровольно сообщил, что он состоит в религиозной организации и не может работать по субботам. HR-специалист отказал кандидату, сославшись на режим работы организации (суббота — рабочий день). В решении об отказе HR указал: «отказано в связи с религиозными убеждениями, не позволяющими работать по субботам». Нарушены ли этико-правовые нормы?</p> <p>Варианты: А) Нет, не нарушены, так как режим работы — объективное требование.</p>		

	<p>Б) Да, нарушены, поскольку религиозные убеждения относятся к специальным категориям ПДн, и ссылка на них в отказе незаконна.</p> <p>В) Да, нарушены, потому что в отказе некорректно зафиксирована причина: вместо объективного «не соответствует графику работы» указана дискриминационная формулировка.</p> <p>Г) Нет, не нарушены, так как кандидат сам сообщил эти данные.</p>		
2.	<p>Какие действия HR-специалиста соответствуют этическим нормам при работе с резюме кандидатов, полученных через сайт-агрегатор (hh.ru, SuperJob)?</p> <p>Варианты:</p> <p>А. Хранение резюме кандидатов в защищенной базе с разграничением доступа только для сотрудников, участвующих в найме.</p> <p>Б. Пересылка резюме кандидата другу из другой компании, «чтобы он посмотрел, вдруг ему подойдет».</p> <p>В. Удаление резюме кандидата из базы после того, как вакансия закрыта и истек разумный срок (например, 6 месяцев), если кандидат не дал согласие на хранение дольше.</p> <p>Г. Сохранение резюме всех кандидатов за 3 года в общей папке на Яндекс.Диске без пароля, «вдруг пригодится».</p> <p>Д. Уведомление кандидата о том, что его резюме будет храниться в кадровом резерве до 1 года, и получение на это отдельного согласия.</p>		

3. Задания закрытого типа.

3.1. 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 ходе видеособеседования кандидат сообщил о своей религии и семейном положении. Какое действие HR-специалиста будет этичным и правомерным?

Варианты ответов:

А) Занести эту информацию в базу кандидата как дополнительное преимущество.

Б) Запросить письменное согласие на обработку специальных категорий ПДн прямо во время интервью.

В) Проигнорировать эту информацию, не фиксировать её в анкете и не учитывать при принятии решения о найме, так как она не относится к деловым качествам.

Г) Сообщить эту информацию будущему непосредственному руководителю кандидата для оценки совместимости в коллективе.

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 действия HR-специалиста являются этичными и правомерными при работе с кандидатами?

Варианты ответов:

А) Заранее (до собеседования) уведомить кандидата о том, что видеоконференция будет записываться, и получить его согласие.

Б) Требовать от всех кандидатов предоставления справки об отсутствии судимости, даже если должность этого не требует по закону.

В) Удалять резюме и анкеты кандидатов, которые не были допущены к следующему этапу, после истечения срока, необходимого для закрытия

вакансии.

Г) Отказаться в обработке биометрических данных (например, фото для пропуска) без отдельного письменного согласия кандидата.

Д) Запрашивать информацию о наличии беременности или планировании детей у всех женщин-соискательниц, чтобы «планировать отпуска».

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.

Расположите в правильной последовательности действия HR-специалиста при проведении видеособеседования с записью (согласно этико-правовым нормам).

Элементы:

1. Запуск записи видеоконференции
2. Объяснение целей записи (например: «для согласования с руководителем отдела», «для оценки качества собеседований»)
3. Устное предупреждение кандидата о том, что собеседование будет записываться
4. Получение явного согласия кандидата (словесное «да» или отметка в чате)
5. Размещение ссылки на видеоконференцию в приглашении с пометкой о возможной записи (предварительное информирование).

Тема 4. Управление инцидентами и претензиями: утечка ПДн как кризисная коммуникация. УК-6.3; ОПК-1.2; ПК-5.1.

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Какое событие в HR-отделе признается «утечкой персональных данных» с юридической точки зрения?

2.	Перечислите обязательные шаги HR-службы в первые 15 минут после обнаружения утечки (локализация, фиксация, кто уведомляется первым).
----	--

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	<p>В отделе кадров произошла утечка: файл с персональными данными 200 сотрудников (паспорта, СНИЛС, зарплаты) случайно оказался в открытом доступе на 6 часов. Когда следует уведомить Роскомнадзор (в РФ)?</p> <p>Варианты:</p> <p>А) Не позднее 24 часов с момента обнаружения утечки.</p> <p>Б) Не позднее 24 часов с момента инцидента (факта утечки), а затем уточненное уведомление — в течение 72 часов.</p> <p>В) Только после завершения внутреннего расследования (независимо от сроков).</p> <p>Г) Уведомлять не нужно, если утечка не привела к материальному ущербу.</p>		
2.	<p>Расположите в правильной последовательности коммуникационные шаги HR-службы при крупной утечке персональных данных сотрудников.</p> <p>Элементы:</p> <p>А) Внутреннее уведомление сотрудников, чьи данные утекли (с рекомендациями).</p> <p>Б) Публичное заявление для СМИ (если утечка стала публичной).</p> <p>В) Локализация инцидента (устранение доступа).</p> <p>Г) Направление первого уведомления в Роскомнадзор.</p>		

3. Задания закрытого типа.

3.1. 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 HR-отделе произошла утечка: файл с зарплатами и паспортными данными 50 сотрудников случайно попал в открытый доступ на файловом сервере. Какое действие является первым шагом внутренней коммуникации согласно стандартам кризисного управления?

Варианты ответов:

А) Немедленно отправить объяснительную генеральному директору с просьбой об увольнении виновного.

Б) Разослать всем сотрудникам компании уведомление «Извините, мы ошиблись, но ничего страшного не произошло».

В) Зафиксировать факт утечки (время, объём, характер данных) и запустить внутреннее расследование, после чего подготовить согласованное сообщение для пострадавших лиц и контролирующих органов.

Г) Удалить файл и сделать вид, что ничего не случилось, чтобы избежать паники.

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.

При обнаружении утечки персональных данных (например, файл с ПДн 100 сотрудников оказался в публичном доступе) какие коммуникационные шаги являются обязательными и корректными?

Варианты ответов:

А) Внутреннее уведомление руководителя службы безопасности или лица, ответственного за обработку ПДн в организации.

Б) Публикация новости об утечке в соцсетях компании до выяснения всех обстоятельств.

В) Уведомление Роскомнадзора (в РФ) в установленный законом срок после фиксации инцидента.

Г) Подготовка корректного сообщения для пострадавших сотрудников с описанием реальных рисков и рекомендаций (без паники и излишних деталей).

Д) Срочный массовый звонок всем сотрудникам компании для устных извинений без документального оформления.

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.

Расположите в правильной последовательности шаги кризисной коммуникации HR-службы и службы безопасности при обнаружении утечки персональных данных сотрудников.

Элементы:

1. Подготовка и направление уведомления в Роскомнадзор (в установленный законом срок)

2. Фиксация факта утечки (время, объём данных, причина, круг лиц, получивших доступ)

3. Составление внутреннего отчета для руководства и запуск служебного расследования

4. Уведомление пострадавших сотрудников о факте утечки и рекомендации по снижению рисков (без паники)

5. Локализация инцидента (удаление доступа, отключение ресурса, изъятие носителя)

Тема 5. Обучение сотрудников и внутренний контроль: как внедрить культуру защиты ПДн через корпоративные коммуникации. УК-6.3; ОПК-1.2; ПК-5.1.

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Почему одного лишь подписания «Согласия на обработку ПДн» недостаточно для формирования культуры защиты данных?

2.	Какие форматы обучения защите ПДн наиболее эффективны для линейных руководителей (не для HR)? Почему лекция уступает тренажеру?
----	---

2. Задания комбинированного типа:

2.1. Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	<p>HR-служба провела скрытый аудит («псевдофишинговую» рассылку): сотрудникам от имени IT-отдела пришло письмо с просьбой прислать список логинов и паролей для «плановой проверки». Сотрудник склада Владимир переслал запрошенные данные. Какое действие руководства будет наиболее правильным для формирования культуры защиты ПДн?</p> <p>Варианты:</p> <p>А) Объявить Владимиру выговор и депремировать на месяц «чтобы другим неповадно было».</p> <p>Б) Уволить Владимира за разглашение конфиденциальной информации.</p> <p>В) Провести с Владимиром индивидуальную беседу, объяснить, почему это опасно, и включить его в группу обязательного обучения по информационной безопасности без формального наказания.</p> <p>Г) Игнорировать инцидент, так как это была всего лишь проверка.</p>		
2.	Какие методы внутреннего контроля и обучения наиболее эффективно в долгосрочной перспективе формируют культуру осознанной защиты персональных данных у		

<p>сотрудников (а не культуру страха)?</p> <p>Варианты:</p> <p>А. Регулярная рассылка коротких (2-3 минуты) видеокейсов «Как мы чуть не потеряли данные» с разбором реальных ситуаций (без указания имен нарушителей).</p> <p>Б. Установка системы тотального контроля за каждым действием сотрудника на рабочем компьютере с автоматическими штрафами за каждое отклонение.</p> <p>В. Проведение обязательного интерактивного тренинга для новых сотрудников с игровыми сценариями «Выбери правильное действие в опасной ситуации».</p> <p>Г. Создание анонимного канала для сообщения о случайных ошибках («я случайно...») без страха наказания, с публичным разбором решения (без указания автора).</p> <p>Д. Ежеквартальные публичные «расстрельные списки» нарушителей на общем собрании.</p>		
---	--	--

3. Задания закрытого типа.

3.1. 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

Какая практика обучения наиболее эффективна для проверки реальной готовности линейных руководителей (не HR) защищать персональные данные в повседневной работе?

Варианты ответов:

А) Ежегодное онлайн-тестирование «15 правил ФЗ-152» без обратной связи по ошибкам.

Б) Рассылка памятки «10 заповедей защиты ПДн» на корпоративную почту.

В) Проведение скрытого аудита — отправка сотрудникам (по инициативе отдела безопасности) фишингового письма с просьбой предоставить пароль или данные коллеги и последующий разбор результатов.

Г) Устное объявление на планерке: «Будьте осторожны с данными, а то оштрафуют».

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 методы обучения и контроля эффективно формируют культуру защиты персональных данных у сотрудников (включая линейных руководителей)?

Варианты ответов:

А) Регулярные (например, раз в полгода) внутренние рассылки с разбором реальных кейсов утечек и ошибок (без указания имен).

Б) Включение вопросов о работе с ПДн в программу онбординга (адаптации) новых сотрудников.

В) Проведение анонимных опросов сотрудников о том, соблюдают ли они правила защиты ПДн (с последующим анализом «слепых зон»).

Г) Штраф всех сотрудников, которые переписываются по рабочим вопросам в личных чатах, без разъяснения альтернатив.

Д) Организация «псевдофишинговых» рассылок (симуляция атаки) от имени ИТ-службы с последующим обучением тех, кто «попался».

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.

Расположите в правильной последовательности этапы внедрения системы внутреннего контроля и обучения сотрудников защите персональных данных через корпоративные коммуникации.

Элементы:

1. Разработка простых памяток и чек-листов «Что делать / чего не делать с ПДн» для разных категорий сотрудников
2. Оценка текущего уровня знаний и выявление «слепых зон» (анонимный опрос, базовое тестирование)
3. Проведение скрытых аудитов (симуляция фишинга, проверка оставленных документов)
4. Разбор с сотрудниками результатов скрытых аудитов и ошибок (без публичных наказаний)
5. Запуск регулярного обучения (вебинары, e-learning, кейсы в корпоративной рассылке) на основе выявленных проблем

6.3. Критерии и шкала оценивания на основе БРС.

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	40
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.	30-39
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.	20-29
Дан ответ, который содержит ряд серьезных неточностей,	0-19

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 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. 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 — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если 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 – 15-20 минут. Подведением итогов заканчивается практическое занятие. 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. Беляев, М. К. Деловая коммуникация и защита персональных данных : учебник для академического бакалавриата / М. К. Беляев, О. В. Максимова. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). —

ISBN 978-5-534-14568-9.

2. Кузнецова, И. В. Управление персоналом и защита персональных данных : учебное пособие для вузов / И. В. Кузнецова, А. П. Смирнов ; под общей редакцией И. В. Кузнецовой. — Санкт-Петербург : Питер, 2022. — 288 с. — (Учебник для вузов). — ISBN 978-5-4461-1892-6.

3. Сидорова, Е. Ю. Деловая коммуникация : учебник для студентов вузов / Е. Ю. Сидорова. — 4-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 384 с. — (Высшее образование: Бакалавриат). — ISBN 978-5-16-012345-7.

4. Чернышова, Л. И. Защита персональных данных в кадровой службе : учебно-практическое пособие / Л. И. Чернышова, Н. А. Петрова. — Москва : Дело, 2022. — 176 с. — (Библиотека HR-специалиста). — ISBN 978-5-7749-1587-9.

8.2. Дополнительная литература

1. Андреева, Т. В. Психология делового общения : учебное пособие / Т. В. Андреева. — 3-е изд., испр. и доп. — Москва : ФЛИНТА, 2021. — 248 с. — ISBN 978-5-9765-1254-8.

2. Волкова, Н. Н. Конфиденциальное делопроизводство и защита персональных данных : практикум / Н. Н. Волкова, С. А. Козлов. — Воронеж : Издательский дом ВГУ, 2023. — 144 с. — ISBN 978-5-9273-1987-9.

3. Глухов, В. В. Менеджмент и деловые коммуникации : учебник для вузов / В. В. Глухов, Е. В. Коноплева. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 256 с. — ISBN 978-5-8114-2456-8.

4. Иванов, Д. А. Этические аспекты сбора и обработки персональных данных в HR-практике : монография / Д. А. Иванов. — Екатеринбург : Издательство УрФУ, 2023. — 168 с. — ISBN 978-5-7996-1789-1.

5. Корнеев, И. Р. Управление инцидентами информационной безопасности в организации : практическое руководство / И. Р. Корнеев. — Москва : ДМК Пресс, 2022. — 208 с. — ISBN 978-5-97060-987-2.

6. Лебедева, О. В. Деловая переписка на государственной службе : учебно-методическое пособие / О. В. Лебедева. — 2-е изд., доп. — Москва : РУДН, 2021. — 132 с. — ISBN 978-5-209-08765-4.

7. Михайлов, С. Н. Цифровая безопасность и защита персональных данных в условиях удаленной работы : практическое пособие / С. Н. Михайлов. — Новосибирск : НГУЭУ, 2023. — 96 с. — ISBN 978-5-7016-2345-7.

8. Попова, Е. А. Профессиональная этика HR-специалиста : учебное пособие / Е. А. Попова. — 3-е изд., перераб. — Казань : Издательство КФУ, 2022. — 156 с. — ISBN 978-5-00130-456-2.

9. Рожкова, М. А. Юридическая ответственность за нарушения в сфере обработки персональных данных : учебное пособие / М. А. Рожкова. — Москва : Статут, 2023. — 184 с. — ISBN 978-5-8354-1789-2.

10. Шаталова, Н. И. Формирование корпоративной культуры

информационной безопасности : монография / Н. И. Шаталова, В. П. Кузнецов. — Нижний Новгород : Издательство ННГУ, 2022. — 204 с. — ISBN 978-5-91326-876-4.

8.3. Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Российская газета. — 1993. — 25 дек. ; Собрание законодательства РФ. — 2020. — № 31. — Ст. 4398.

2. Трудовой кодекс Российской Федерации : Федеральный закон от 30 декабря 2001 г. № 197-ФЗ (ред. от 25 февраля 2025 г.) // Собрание законодательства РФ. — 2002. — № 1 (ч. 1). — Ст. 3. — (с изм. и доп., вступ. в силу с 1 марта 2025 г.).

3. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 21 декабря 2024 г.) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3451.

4. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 25 февраля 2025 г.) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3448.

5. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ (ред. от 25 апреля 2025 г.) (ст. 13.11 – нарушение законодательства о персональных данных) // Собрание законодательства РФ. — 2002. — № 1 (ч. 1). — Ст. 1.

6. О государственной гражданской службе Российской Федерации : Федеральный закон от 27 июля 2004 г. № 79-ФЗ (ред. от 25 декабря 2024 г.) // Собрание законодательства РФ. — 2004. — № 31. — Ст. 3215.

7. О муниципальной службе в Российской Федерации : Федеральный закон от 2 марта 2007 г. № 25-ФЗ (ред. от 25 декабря 2024 г.) // Собрание законодательства РФ. — 2007. — № 10. — Ст. 1152.

8. Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 6 марта 1997 г. № 188 (ред. от 13 июля 2015 г.) // Собрание законодательства РФ. — 1997. — № 10. — Ст. 1127.

9. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Постановление Правительства РФ от 1 ноября 2012 г. № 1119 (ред. от 15 сентября 2023 г.) // Собрание законодательства РФ. — 2012. — № 45. — Ст. 6257.

10. О перечне персональных данных, подлежащих уничтожению при достижении целей их обработки или при отзыве согласия : Приказ

Роскомнадзора от 4 сентября 2023 г. № 128 // Официальный интернет-портал правовой информации. — URL: <https://www.pravo.gov.ru> (дата обращения: 24.04.2026).

11. ГОСТ Р 7.0.100-2018. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления : национальный стандарт Российской Федерации : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2018 г. № 1200-ст. — Москва : Стандартинформ, 2019. — 116 с.

12. Разъяснения по вопросам, связанным с применением Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» : письмо Роскомнадзора от 21 февраля 2024 г. № 08-13625 // Документ официально не опубликован. — СПС «КонсультантПлюс».

8.4. Интернет-ресурсы

<https://cyberleninka.ru/>

<https://e.lanbook.com>

<https://znanium.ru>

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

Требования к аудитории:

- Лекционные
- Семинарские
- Помещения для самостоятельной работы

Требования к оборудованию:

- доска
- проектор
- ПК (стационарный) или ноутбук: операционная система: не ниже Windows 7 (или аналогичная по функциям)

Требования к программному обеспечению:

- пакет Microsoft Office