Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»
(ИМПЭ им. А.С. Грибоедова)

ИНСТИТУТ МЕЖДУНАРОДНОЙ ЭКОНОМИКИ, ЛИДЕРСТВА И МЕНЕДЖМЕНТА

УТВЕРЖДАЮ
Директор института
международной экономики,
лидерства и менеджмента
_____ А.А. Панарин
«22» декабря 2023г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине:
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Специальность
38.05.02 Таможенное дело

Специализация:
Таможенные платежи и валютный контроль

Квалификация (степень):
специалист таможенного дела

Формы обучения:
очная, заочная

Москва

Фонд оценочных средств для дисциплины «Информационная безопасность и защита информации». Направление подготовки/специальность 38.05.02 Таможенное дело, направленность (профиль/специализация): Таможенные платежи и валютный контроль/ О.А. Левичев. – М.: ИМПЭ им. А.С. Грибоедова

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Разработчик: О.А. Левичев

Заведующий кафедрой. _____ Т.В. Новикова

1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Настоящий Фонд оценочных средств (ФОС) по дисциплине «Информационная безопасность и защита информации» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «Информационная безопасность и защита информации». На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Для определения качества освоения обучающимися учебного материала по дисциплине используются следующие оценочные средства:

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Тестирование	Вид контроля, позволяющий оценить изученный теоретический материал.	Вопросы для проведения тестирования
2	Практические задания	Вид контроля, позволяющий оценить умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач	Задания к практическому занятию
3	Контрольная работа	Вид контроля, позволяющий определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций	Задания контрольной работы
4	Самостоятельная работа	Вид контроля, позволяющий оценить проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборку нормативного и иного материала и выполнение других заданий	Задания самостоятельной работы
5	Курсовая работа	Вид контроля, позволяющий выявить степень владения базовыми знаниями, умениями и навыками, необходимыми для обучения, и определить уровень владения новым материалом	Индивидуальные задания (темы) для курсовой работы

6	Зачет/Зачет с оценкой/Экзамен	Вид контроля, позволяющий выявить степень овладения знаниями, умениями и навыками, необходимыми для дальнейшего освоения образовательной программы подготовки	Вопросы для подготовки к зачету/зачету с оценкой/экзамену

3. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЕ

3.1. Сопроводительная информация.

Разработчик	О.А. Левичев
Кафедра	Аудита, финансов и кредита
Наименование дисциплины	Информационная безопасность и защита информации
Факультет / институт	Института международной экономики, лидерства и менеджмента
Направление подготовки / специальность	38.05.02 Таможенное дело
Количество вопросов в оценочных заданиях (диапазон)	От 18 до 36
Общее время тестирования (мин)	90
Общее количество вопросов/заданий в ФОС	36
Размещенность на сайте Университета примерного перечня вопросов, заданий ФОС – для подготовки обучающихся к прохождению оценки (да / нет)	*Да*

3.2. Характеристика оцениваемых компетенций.

Код компетенции	**Формулировка компетенции**	**Индикаторы достижения компетенции**
УК- 10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	**ИУК-10.1** Знает способы профилактики коррупции и формирования нетерпимого отношения к ней. **ИУК-10.2** Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям

4. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

4.1. ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ.

Тесты содержат набор вопросов, в полном объеме охватывающие изученный теоретический материал по указанной теме (индикаторы ЗНАТЬ). Выполнение тестов позволяет определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций. Индивидуальный тестовый сеанс для каждого обучающегося формируется по специальному алгоритму, обеспечивающему заданную тематическую структуру и пропорциональное наличие вопросов разного типа и сложности.

При формировании тестов необходимо использовать задания следующих типов:

Тип задания 1. Задания закрытого типа на установление соответствия.

Тип задания 2. Задания закрытого типа на установление последовательности.

Тип задания 3. Задания комбинированного типа, предполагающие выбор одного правильного ответа из предложенных.

Тип задания 4. Задания комбинированного типа, предполагающие выбор нескольких ответов из предложенных.
Тип задания 5. Задания открытого типа с развернутым ответом.

<table>
<tr><th>Тема</th><th>Код и формулировка компетенции</th><th>Индикаторы достижения компетенции</th><th>Тест по теме</th></tr>
<tr><td>Тема 1. Борьба с угрозами несанкционированного доступа к информации</td><td>УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности</td><td>ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td><td>
Задания закрытого типа на установление соответствия
Вопрос 1. Установите соответствие между видами угроз информационной безопасности и их характеристиками.
<table>
<tr><td>Вид угрозы</td><td>Характеристика</td></tr>
<tr><td>1. Физическая угроза</td><td>А. Несанкционированный доступ к данным через уязвимости в ПО</td></tr>
<tr><td>2. Программная угроза</td><td>Б. Повреждение оборудования в результате стихийных бедствий</td></tr>
<tr><td>3. Организационная угроза</td><td>В. Ошибки персонала при работе с информацией</td></tr>
<tr><td>4. Правовая угроза</td><td>Г. Отсутствие необходимых нормативных документов по защите информации</td></tr>
</table>
Правильный ответ: 1 – Б, 2 – А, 3 – В, 4 – Г.
Вопрос 2. Соотнесите меры защиты информации с их типами.
<table>
<tr><td>Тип меры</td><td>Мера защиты</td></tr>
<tr><td>1. Законодательная</td><td>А. Использование антивирусного ПО</td></tr>
<tr><td>2. Организационная</td><td>Б. Принятие федеральных законов в области ИБ</td></tr>
<tr><td>3. Техническая</td><td>В. Разработка инструкций по работе с конфиденциальной информацией</td></tr>
<tr><td>4. Программно-математическая</td><td>Г. Применение криптографических методов защиты</td></tr>
</table>
Правильный ответ: 1 – Б, 2 – В, 3 – А, 4 – Г.
</td></tr>
</table>

<table>
<tr><th>Тема</th><th>Код и формулировка компетенции</th><th>Индикаторы достижения компетенции</th><th>Тест по теме</th></tr>
<tr><td></td><td></td><td></td><td>Вопрос 3. Установите соответствие между принципами защиты информации и их сутью.
<table>
<tr><td>Принцип</td><td>Суть принципа</td></tr>
<tr><td>1. Конфиденциальность</td><td>А. Обеспечение возможности получения информации в нужное время</td></tr>
<tr><td>2. Целостность</td><td>Б. Защита от несанкционированного изменения данных</td></tr>
<tr><td>3. Доступность</td><td>В. Защита от несанкционированного ознакомления с данными</td></tr>
</table>
Правильный ответ: 1 – В, 2 – Б, 3 – А.</td></tr>
<tr><td>Тема 1. Борьба с угрозами несанкционированного доступа к информации</td><td>УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности</td><td>ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td><td>2. Задания закрытого типа на установление последовательности
Вопрос 1. Установите правильную последовательность этапов реализации атаки на информационную систему:
1. Эксплуатация уязвимости.
2. Сбор информации о цели.
3. Закрепление в системе.
4. Получение доступа.
5. Планирование атаки.
Правильный ответ: 5 → 2 → 1 → 4 → 3.
Вопрос 2. Определите правильную последовательность действий при обнаружении атаки:
1. Локализация угрозы.
2. Фиксация доказательств.
3. Анализ инцидента.
4. Информирование ответственных лиц.
5. Восстановление работоспособности системы.
Правильный ответ: 4 → 1 → 2 → 3 → 5.
Вопрос 3. Расположите в правильной последовательности этапы построения системы защиты информации:
1. Разработка политики безопасности.
2. Анализ рисков.
3. Внедрение защитных механизмов.
4. Определение требований к защите.
5. Мониторинг и аудит.
Правильный ответ: 2 → 4 → 1 → 3 → 5.</td></tr>
</table>

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания комбинированного типа (выбор одного ответа)** **Вопрос 1.** Какой метод является наиболее эффективным для защиты от несанкционированного копирования программного обеспечения? А) Использование парольной защиты. Б) Применение электронных ключей (аппаратных донглов). В) Размещение предупреждающей надписи об авторских правах. Г) Ограничение доступа к файлам через права NTFS. **Правильный ответ:** Б) Применение электронных ключей (аппаратных донглов). **Объяснение:** Электронные ключи обеспечивают аппаратную защиту, которую сложно обойти программными методами. В отличие от парольной защиты (легко взламывается), предупреждающих надписей (не имеют технической силы) и прав доступа (могут быть изменены администратором), аппаратные донглы требуют физического наличия устройства для работы ПО, что существенно повышает уровень защиты. **Вопрос 2.** Что является первоочередной задачей при обнаружении факта несанкционированного доступа? А) Немедленное отключение системы от сети. Б) Фиксация всех доступных доказательств инцидента. В) Уведомление правоохранительных органов. Г) Восстановление резервных копий данных. **Правильный ответ:** Б) Фиксация всех доступных доказательств инцидента. **Объяснение:** Фиксация доказательств позволяет: 1) установить масштаб ущерба; 2) выявить методы атаки; 3) использовать данные для расследования и возможных судебных разбирательств. Отключение системы (А) может уничтожить важные улики в оперативной памяти. Уведомление органов (В) и восстановление данных (Г) — важные, но последующие шаги. **Вопрос 3.** Какой стандарт является основополагающим для построения системы менеджмента информационной безопасности? А) ISO/IEC 27001. Б) ГОСТ Р 57580.1-2017. В) PCI DSS. Г) NIST SP 800-53. **Правильный ответ:** А) ISO/IEC 27001. **Объяснение:** ISO/IEC 27001 — международный стандарт, определяющий требования к системе менеджмента информационной безопасности (СМИБ). Он универсален, признаётся во всём мире и служит основой для сертификации. ГОСТ Р 57580.1-2017 (Б) специфичен для финансового сектора РФ. PCI DSS (В) касается только обработки платёжных данных. NIST SP 800-53 (Г) применяется преимущественно в госучреждениях США.
Тема 1. Борьба с угрозами	УК-10. Способен формировать нетерпимое	ИУК-10.1 Знает способы профилактики	**Задания комбинированного типа (выбор нескольких ответов)** **Вопрос 1.** Какие из перечисленных мер относятся к организационным методам защиты информации? Выберите все верные варианты.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
несанкционированного доступа к информации	отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	коррупции и формирования нетерпимого отношения к ней.	А) Разработка регламентов работы с конфиденциальными данными. Б) Установка антивирусного ПО. В) Проведение тренингов по ИБ для сотрудников. Г) Использование межсетевых экранов. Д) Назначение ответственных за ИБ в подразделениях. **Правильные ответы:** А, В, Д. **Объяснение:** • А) Регламенты — ключевой организационный документ, нормирующий процессы. • В) Тренинги повышают осведомлённость персонала — важная часть организационной защиты. • Д) Распределение ответственности — основа организационной структуры ИБ. Б) и Г) относятся к техническим мерам, так как предполагают использование ПО/оборудования. **Вопрос 2.** Какие угрозы относятся к внутренним источникам рисков ИБ? Выберите все верные варианты. А) Ошибки пользователей при работе с данными. Б) Атаки хакеров через интернет. В) Злоумышленное действие сотрудника. Г) Сбои в работе серверного оборудования. Д) Фишинговые письма от мошенников. **Правильные ответы:** А, В, Г. **Объяснение:** • А) Ошибки персонала — классический внутренний риск (например, отправка конфиденциальных данных не тем адресатам). • В) Злоумышленники внутри организации (например, продажа данных конкурентам) — внутренняя угроза. • Г) Технические сбои оборудования — внутренний риск, так как источник находится в инфраструктуре организации. Б) и Д) — внешние угрозы, инициируемые посторонними лицами. **Вопрос 3.** Какие механизмы входят в систему идентификации и аутентификации? Выберите все верные варианты. А) Ввод логина и пароля. Б) Сканирование отпечатков пальцев. В) Проверка MAC-адреса устройства. Г) Анализ поведения пользователя (User Behavior Analytics). Д) Шифрование данных на диске. **Правильные ответы:** А, Б, В, Г. **Объяснение:** • А) Логин/пароль — базовый метод аутентификации. • Б) Биометрия (отпечатки) — современный метод аутентификации. • В) MAC-адрес может использоваться для идентификации устройства.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			• Г) Анализ поведения дополняет аутентификацию (например, обнаружение аномалий). Д) Шифрование — метод защиты данных, но не относится напрямую к идентификации/аутентификации.
Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания открытого типа с развёрнутым ответом** **Вопрос 1.** Опишите три ключевых принципа информационной безопасности (триада CIA) и приведите примеры их реализации в корпоративной среде. **Ответ:** 1. **Конфиденциальность** — защита информации от несанкционированного доступа. *Пример:* шифрование данных при передаче по сети, разграничение прав доступа к файлам, использование двухфакторной аутентификации для входа в систему. 2. **Целостность** — гарантия неизменности данных. *Пример:* применение хэш-сумм для проверки целостности файлов, ведение журналов изменений (audit trails), резервное копирование с контролем версий. 3. **Доступность** — обеспечение работоспособности систем и данных. *Пример:* резервирование серверов, использование систем бесперебойного питания (ИБП), организация георасределённых дата-центров для отказоустойчивости. **Вопрос 2.** Перечислите основные этапы анализа рисков информационной безопасности и кратко поясните каждый из них. **Ответ:** 1. **Идентификация активов** Определение информационных ресурсов, подлежащих защите: данные (персональные, финансовые, коммерческая тайна), аппаратное и программное обеспечение, каналы связи. *Пример:* составление реестра критически важных серверов и баз данных. 2. **Оценка угроз** Выявление потенциальных источников опасности: внешние (хакеры, вирусы) и внутренние (ошибки персонала, сбои оборудования). *Пример:* анализ статистики инцидентов за последний год для выявления типичных атак. 3. **Определение уязвимостей** Поиск «слабых мест» в системе защиты: незакрытые патчи ПО, слабые пароли, отсутствие шифрования. *Пример:* сканирование сети на наличие открытых портов. 4. **Анализ вероятности реализации угроз** Оценка шансов наступления инцидента с учётом существующих уязвимостей. *Пример:* расчёт вероятности фишинговой атаки при наличии не обученного персонала. 5. **Оценка последствий** Прогнозирование ущерба от реализации угрозы: финансовый, репутационный, юридический. *Пример:* расчёт потерь от простоя CRM-системы на 12 часов. 6. **Расчёт уровня риска** Комбинирование вероятности и последствий по формуле:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Риск=Вероятность×Ущерб. *Пример:* высокий риск при вероятности атаки 70 % и ущербе 5 млн руб. 7. **Разработка мер снижения риска** Выбор контрмер: технические (антивирусы), организационные (инструкции), правовые (договоры NDA). *Пример:* внедрение системы резервного копирования для снижения риска потери данных. 8. **Мониторинг и пересмотр** Регулярное обновление оценки рисков с учётом изменений в ИТ-инфраструктуре и угрозах. *Пример:* квартальный аудит безопасности после внедрения нового ПО. **Вопрос 3.** Объясните, почему комплексный подход к защите информации (сочетание законодательных, организационных, технических и других мер) эффективнее, чем использование только одного типа защиты. Приведите конкретные примеры. **Ответ:** Комплексный подход обеспечивает **многоуровневую защиту** («принцип эшелонирования»), где слабость одного слоя компенсируется надёжностью других. **Причины эффективности:** 1. **Перекрытие всех векторов атак** Один тип защиты не закрывает все угрозы. *Пример:* • Технические средства (файрволы) не предотвратят утечку данных через сотрудника. • Организационные меры (инструкции) бесполезны против вирусной атаки без антивируса. 2. **Снижение зависимости от человеческого фактора** Даже при ошибке сотрудника технические средства могут блокировать угрозу. *Пример:* DLP-система не позволит отправить конфиденциальный файл по email, даже если сотрудник случайно прикрепил его. 3. **Соответствие нормативным требованиям** Законодательные меры (ФЗ-152, GDPR) обязывают использовать комбинацию методов. *Пример:* для защиты персональных данных требуется: • юридическое оформление согласия (законодательная мера); • разграничение доступа (организационная); • шифрование (техническая). 4. **Экономическая целесообразность** Распределение бюджета между мерами даёт лучший ROI. *Пример:* затраты на обучение персонала (организационная мера) снижают риски фишинга, сокращая расходы на ликвидацию последствий атак. 5. **Адаптивность к новым угрозам** Комплекс мер позволяет оперативно реагировать на изменения. *Пример:* при появлении нового вируса технические средства (антивирус) блокируют его, а организационные (временный запрет USB-носителей) минимизируют распространение.
Тема 2.	УК-10. Способен	ИУК-10.1	**Задания закрытого типа на установление соответствия**

<table>
<tr><th>Тема</th><th>Код и формулировка компетенции</th><th>Индикаторы достижения компетенции</th><th>Тест по теме</th></tr>
<tr><td>Борьба с вирусным заражением информации</td><td>формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности</td><td>Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td><td>
Задание 1. Установите соответствие между типом антивирусной программы и её функцией.
<table>
<tr><td>Тип программы</td><td>Функция</td></tr>
<tr><td>1. Программы-детекторы</td><td>А. Отслеживают изменения в файлах и системных областях</td></tr>
<tr><td>2. Программы-доктора</td><td>Б. Блокируют подозрительные действия в реальном времени</td></tr>
<tr><td>3. Программы-ревизоры</td><td>В. Ищут известные вирусы по сигнатурам</td></tr>
<tr><td>4. Программы-фильтры</td><td>Г. Лечат заражённые файлы, удаляя вирус</td></tr>
</table>
Правильный ответ: 1 – В; 2 – Г; 3 – А; 4 – Б.
Задание 2. Соотнесите вид вредоносного ПО с его характеристикой.
<table>
<tr><td>Вид ПО</td><td>Характеристика</td></tr>
<tr><td>1. Компьютерный вирус</td><td>А. Собирает и передаёт конфиденциальные данные без ведома пользователя</td></tr>
<tr><td>2. Программа-шпион</td><td>Б. Самовоспроизводится и внедряется в другие программы</td></tr>
<tr><td>3. Программа-сканер</td><td>В. Ищет уязвимости в системе для последующего использования</td></tr>
</table>
Правильный ответ: 1 – Б; 2 – А; 3 – В.
Задание 3. Установите соответствие между деструктивным действием вируса и его проявлением.
<table>
<tr><td>Действие вируса</td><td>Проявление</td></tr>
<tr><td>1. Разрушение программы защиты</td><td>А. Система становится уязвимой для последующих атак</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Тема</th><th>Код и формулировка компетенции</th><th>Индикаторы достижения компетенции</th><th>Тест по теме</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>2. Изменение состояния программной среды</td><td>Б. Файлы становятся нечитаемыми или удаляются</td></tr>
<tr><td>3. Воздействие на программно-аппар атные средства</td><td>В. Программы работают некорректно или не запускаются</td></tr>
<tr><td></td><td>Г. Оборудование работает нестабильно или выходит из строя</td></tr>
</table>
Правильный ответ: 1 – А; 2 – В; 3 – Г.
</td></tr>
<tr><td>Тема 2. Борьба с вирусным заражением информации</td><td>УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности</td><td>ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td><td>Задания закрытого типа на установление последовательности
Задание 1. Расположите этапы распространения компьютерного вируса в правильной последовательности:
А. Активизация вируса при запуске заражённого файла.
Б. Поиск новых объектов для заражения.
В. Внедрение вируса в систему.
Г. Репликация (копирование) вируса.
Д. Выполнение деструктивных действий.
Правильный ответ: В → А → Г → Б → Д.
Задание 2. Установите правильную последовательность действий при обнаружении вирусного заражения:
А. Изолировать заражённый компьютер от сети.
Б. Провести полное сканирование системы антивирусной программой.
В. Сообщить об инциденте ответственному за ИБ.
Г. Восстановить данные из резервной копии.
Д. Обновить антивирусные базы и ПО.
Правильный ответ: В → А → Б → Д → Г.
Задание 3. Определите верную последовательность этапов профилактики вирусного заражения:
А. Регулярное обновление антивирусного ПО.
Б. Обучение пользователей основам ИБ.
В. Настройка брандмауэра и фильтров.
Г. Создание резервных копий данных.
Д. Контроль внешних носителей и электронной почты.
Правильный ответ: Б → В → А → Д → Г.</td></tr>
<tr><td>Тема 2.</td><td>УК-10. Способен</td><td>ИУК-10.1</td><td>Задания комбинированного типа (выбор одного ответа)</td></tr>
</table>

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
Борьба с вирусным заражением информации	формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задание 1.** Какой тип антивирусной программы наиболее эффективен для обнаружения новых, неизвестных вирусов? А. Программы-детекторы. Б. Программы-ревизоры. В. Программы-фильтры. Г. Программы-доктора. **Правильный ответ:** Б – программы-ревизоры. **Объяснение:** программы-ревизоры отслеживают изменения в файлах и системных областях, сравнивая их с эталонными значениями. Это позволяет обнаруживать новые вирусы, даже если их сигнатуры ещё не известны, поскольку любое несанкционированное изменение может указывать на заражение. **Задание 2.** Что является наиболее эффективным способом предотвращения взлома парольной системы? А. Использование простых, легко запоминаемых паролей. Б. Применение двухфакторной аутентификации. В. Хранение паролей в текстовом файле на рабочем столе. Г. Использование одного пароля для всех сервисов. **Правильный ответ:** Б – применение двухфакторной аутентификации. **Объяснение:** двухфакторная аутентификация требует не только ввода пароля, но и дополнительного подтверждения (например, кода из SMS или биометрических данных). Это существенно усложняет несанкционированный доступ, даже если пароль был скомпрометирован. **Задание 3.** Какой метод профилактики вирусного заражения является первоочередным для организации? А. Установка антивирусного ПО на все компьютеры. Б. Регулярное резервное копирование данных. В. Обучение сотрудников основам информационной безопасности. Г. Ограничение прав доступа пользователей. **Правильный ответ:** В – обучение сотрудников основам информационной безопасности. **Объяснение:** человеческий фактор – один из главных источников угроз. Обучение сотрудников позволяет снизить риск заражения через фишинг, подозрительные вложения и ненадёжные ссылки. Без осознанного отношения персонала к ИБ технические меры могут оказаться недостаточно эффективными.
Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания комбинированного типа (выбор нескольких ответов)** **Задание 1.** Выберите все эффективные меры профилактики вирусного заражения: А. Регулярное обновление ОС и ПО. Б. Использование нелицензионного антивирусного ПО. В. Ограничение доступа к подозрительным веб-сайтам. Г. Открытие вложений из писем от неизвестных отправителей. Д. Резервное копирование важных данных. **Правильные ответы:** А, В, Д.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	поведению и противодействовать им в профессиональной деятельности		**Объяснение:** • **А** – обновления закрывают уязвимости, которые могут использовать вирусы. • **В** – ограничение доступа к подозрительным ресурсам снижает риск загрузки вредоносного кода. • **Д** – резервные копии позволяют восстановить данные после атаки. Ответы **Б** и **Г** увеличивают риски: нелицензионное ПО может содержать вирусы, а подозрительные вложения – основной канал заражения. **Задание 2.** Какие действия вируса относятся к деструктивным? Выберите все верные варианты. А. Шифрование файлов пользователя без его согласия. Б. Сбор информации о посещённых веб-сайтах. В. Удаление системных файлов. Г. Медленная работа компьютера из-за фоновых процессов. Д. Блокировка доступа к важным данным. **Правильные ответы:** А, В, Д. **Объяснение:** • **А** – шифрование без согласия пользователя (например, ransomware) лишает доступа к данным. • **В** – удаление системных файлов нарушает работу ОС. • **Д** – блокировка данных препятствует их использованию. Ответ **Б** относится к шпионской деятельности, а **Г** – к косвенным последствиям, но не является прямым деструктивным действием. **Задание 3.** Какие программы помогают обнаружить уязвимости, которые могут быть использованы вирусами? Выберите все подходящие варианты. А. Программы-сканеры. Б. Антивирусные мониторы. В. Системы IDS/IPS. Г. Файерволы. Д. Программы-архиваторы. **Правильные ответы:** А, Б, В, Г. **Объяснение:** • **А** – программы-сканеры ищут уязвимости в ПО и настройках. • **Б** – антивирусные мониторы отслеживают подозрительные действия в реальном времени. • **В** – IDS/IPS выявляют попытки эксплуатации уязвимостей. • **Г** – файерволы контролируют сетевой трафик и блокируют подозрительные соединения. Ответ **Д** не относится к обнаружению уязвимостей – архиваторы служат для сжатия данных.
Тема 2. Борьба с	УК-10. Способен формировать	ИУК-10.1 Знает способы	**Задания открытого типа с развёрнутым ответом** **Задание 1.** Опишите структуру современного компьютерного вируса и объясните, как каждый компонент

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
вирусным заражением информации	нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	профилактики коррупции и формирования нетерпимого отношения к ней.	способствует его функционированию. **Ответ:** Современный компьютерный вирус обычно состоит из следующих компонентов: 1. **Механизм заражения (инъекции)** – обеспечивает внедрение вируса в систему (например, через уязвимости или социальную инженерию). 2. **Код репликации** – отвечает за копирование вируса в другие файлы или системы. 3. **Триггер (условие активации)** – определяет, когда вирус начнёт выполнять деструктивные действия (например, при определённой дате или действии пользователя). 4. **Полезная нагрузка (payload)** – выполняет вредоносные действия: удаление данных, шифрование, сбор информации и т. п. 5. **Механизм скрытности** – позволяет вирусу избегать обнаружения (например, маскировка под легитимное ПО или шифрование кода). Каждый компонент усиливает эффективность вируса: механизм заражения обеспечивает распространение, репликация – масштабирование угрозы, триггер – неожиданность атаки. **Задание 2.** Перечислите и кратко охарактеризуйте основные модели поведения современных компьютерных вирусов. Для каждой модели приведите пример реального вируса или типа вредоносного ПО, иллюстрирующего её. **Ответ:** Основные модели поведения вирусов: 1. **Резидентная модель** Характеристика: вирус загружается в оперативную память при запуске заражённого файла и остаётся активным до перезагрузки системы. Перехватывает системные вызовы, внедряясь в процессы. Пример: вирус **CIH** («Чернобыль», 1998 г.) — резидентно заражал исполняемые файлы Windows, мог повреждать BIOS и данные на жёстком диске. 2. **Нерезидентная модель** Характеристика: активируется только при запуске заражённого файла, не остаётся в памяти после его завершения. Распространяется через копирование. Пример: классические файловые вирусы типа **Win32.Perrun**, заражавшие исполняемые файлы при их открытии. 3. **Полиморфная модель** Характеристика: изменяет свой код при каждом копировании (например, через шифрование с разным ключом), затрудняя обнаружение по сигнатурам. Пример: вирус **Storm Worm** (2007 г.) использовал полиморфизм и рассылку по электронной почте для распространения. 4. **Стелс-модель (скрытная)** Характеристика: маскирует своё присутствие: скрывает файлы, перехватывает вызовы ОС, подменяет данные о размерах файлов. Пример: **Rootkit.Win32.Agent**, который скрывал процессы и файлы, затрудняя обнаружение антивирусами. 5. **Сетевая модель (черви)**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Характеристика: самостоятельно распространяется по сети, используя уязвимости ОС или сервисов. Не требует запуска файла пользователем. Пример: червь **WannaCry** (2017 г.), эксплуатировавший уязвимость SMB в Windows для массового заражения. 6. **Троянская модель** Характеристика: маскируется под легитимное ПО, выполняет скрытые вредоносные действия (сбор данных, открытие бэкдоров). Пример: **Emotet** — троян, распространявшийся через фишинговые письма и служивший загрузчиком другого вредоносного ПО. 7. **Руткит-модель** Характеристика: получает привилегированный доступ к системе, скрывает деятельность других вредоносных программ. Пример: **Sony BMG Rootkit** (2005 г.), устанавливавшийся с аудио-CD и скрывавший файлы для защиты от копирования. **Задание 3.** Опишите комплексный план действий организации по предотвращению вирусных заражений и реагированию на инциденты. Укажите не менее пяти ключевых мер профилактики и не менее трёх этапов реагирования. Обоснуйте, почему каждая мера важна. **Ответ:** **Меры профилактики:** 1. **Регулярное обновление ПО и ОС** Обоснование: закрывает уязвимости, которые могут быть использованы вирусами для проникновения. Автоматические обновления снижают риск эксплуатации известных брешей. 2. **Использование многоуровневой антивирусной защиты** Обоснование: сочетание антивирусов-детекторов, мониторов и файерволов обеспечивает обнаружение на разных стадиях — от загрузки файла до сетевых атак. 3. **Обучение персонала основам кибергигиены** Обоснование: фишинг и социальная инженерия — главные каналы заражения. Обучение снижает риск открытия подозрительных вложений и перехода по вредоносным ссылкам. 4. **Ограничение прав пользователей** Обоснование: минимизация административных прав препятствует запуску вредоносного кода с привилегиями системы. Пользователи работают в режиме «только необходимое». 5. **Резервное копирование данных** Обоснование: позволяет восстановить информацию после атаки (например, ransomware). Резервы должны храниться оффлайн или в защищённом облаке, чтобы избежать их шифрования. **Этапы реагирования на инцидент:** 1. **Изоляция заражённой системы** Действия: отключение от сети, блокировка учётных записей, перевод в карантин.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Обоснование: предотвращает распространение вируса на другие узлы сети и утечку данных. 2. **Анализ и идентификация угрозы** Действия: сбор логов, анализ подозрительных процессов, определение типа вируса (с помощью песочниц и антивирусных лабораторий). Обоснование: точная диагностика позволяет выбрать эффективные методы лечения и предотвратить повторные атаки. 3. **Ликвидация и восстановление** Действия: удаление вируса (с использованием специализированных утилит), восстановление системы из резервных копий, смена паролей. Обоснование: гарантирует полное устранение угрозы и возврат к штатной работе. Проверка целостности данных исключает скрытые бэкдоры. **Дополнительно:** после инцидента важно провести разбор причин (post-mortem analysis) и обновить политики безопасности, чтобы минимизировать риски в будущем.
Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания закрытого типа на установление соответствия** **Вопрос 1.** Установите соответствие между правовыми документами и их уровнем регулирования. А) Федеральный закон «Об информации, информационных технологиях и о защите информации» Б) Конвенция о киберпреступности (Будапештская конвенция) В) Приказ ФСТЭК России № 21 Г) Локальные акты организации по защите информации 1. Международный уровень 2. Федеральный уровень 3. Ведомственный уровень 4. Корпоративный уровень **Правильный ответ:** А – 2; Б – 1; В – 3; Г – 4. **Вопрос 2.** Соотнесите виды информации с режимами её защиты. А) Персональные данные Б) Государственная тайна В) Коммерческая тайна Г) Служебная информация ограниченного доступа 1. Режим государственной тайны 2. Режим конфиденциальной информации 3. Режим персональных данных 4. Режим служебной тайны **Правильный ответ:** А – 3; Б – 1; В – 2; Г – 4. **Вопрос 3.** Установите соответствие между статьями УК РФ и видами компьютерных преступлений. А) Ст. 272 УК РФ

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Б) Ст. 273 УК РФ В) Ст. 274 УК РФ Г) Ст. 274.1 УК РФ 1. Создание, использование и распространение вредоносных компьютерных программ 2. Неправомерный доступ к компьютерной информации 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации 4. Неправомерное воздействие на критическую информационную инфраструктуру РФ **Правильный ответ:** А – 2; Б – 1; В – 3; Г – 4.
Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания закрытого типа на установление последовательности** **Вопрос 1.** Установите правильную последовательность этапов разработки нормативно-правовой базы в сфере ИБ в РФ. 1. Принятие федеральных законов 2. Разработка ведомственных приказов и инструкций 3. Утверждение Концепции правового обеспечения ИБ РФ 4. Принятие международных обязательств (ратификация конвенций) **Правильный ответ:** 4 → 3 → 1 → 2. **Вопрос 2.** Определите последовательность действий при расследовании инцидента информационной безопасности. 1. Фиксация доказательств 2. Установление факта нарушения 3. Уведомление правоохранительных органов (при необходимости) 4. Анализ причин и последствий **Правильный ответ:** 2 → 1 → 4 → 3. **Вопрос 3.** Расположите в правильной последовательности уровни правовой защиты информации (от общего к частному). 1. Локальные акты организации 2. Международные договоры 3. Федеральные законы 4. Ведомственные нормативные акты **Правильный ответ:** 2 → 3 → 4 → 1.
Тема 3. Организационно-правовое обеспечение информационной	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма,	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого	**Задания комбинированного типа (выбор одного ответа)** **Вопрос 1.** Какой документ определяет основные направления государственной политики в области информационной безопасности РФ? А) Доктрина информационной безопасности РФ Б) Федеральный закон «О безопасности» В) Конституция РФ

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
безопасности	терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	отношения к ней.	Г) Указ Президента о стратегии развития ИКТ **Правильный ответ:** А) Доктрина информационной безопасности РФ. **Объяснение:** Доктрина информационной безопасности РФ (утверждена Указом Президента РФ) является ключевым документом, определяющим стратегические цели, задачи и направления государственной политики в сфере ИБ. Она служит основой для разработки законодательных и нормативных актов, а также межведомственного взаимодействия. **Вопрос 2.** Какой международный документ впервые закрепил правовые нормы борьбы с киберпреступностью? А) Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Совет Европы, 1981 г.) Б) Будапештская конвенция о киберпреступности (2001 г.) В) Резолюция ООН о международной информационной безопасности Г) Договор о сотрудничестве в области ИБ между странами СНГ **Правильный ответ:** Б) Будапештская конвенция о киберпреступности (2001 г.). **Объяснение:** Будапештская конвенция (Конвенция о преступности в сфере компьютерной информации) — первый международный договор, систематизировавший составы киберпреступлений, механизмы расследования и международное сотрудничество в этой сфере. Она стала основой для национального законодательства многих стран. **Вопрос 3.** Какой нормативный акт регулирует обработку персональных данных в РФ? А) Федеральный закон № 152-ФЗ «О персональных данных» Б) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» В) Постановление Правительства о защите ПДн Г) Приказ Минцифры о мерах защиты ПДн **Правильный ответ:** А) Федеральный закон № 15 Newton-ФЗ «О персональных данных». **Объяснение:** ФЗ № 152-ФЗ — основной закон, регулирующий сбор, хранение, обработку и защиту персональных данных на территории РФ. Он устанавливает требования к операторам ПДн, права субъектов данных и меры ответственности за нарушения.
Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессионально	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания комбинированного типа (выбор нескольких ответов)** **Вопрос 1.** Какие из перечисленных мер относятся к правовым способам профилактики коррупции в сфере ИБ? (Выберите 3 варианта.) А) Введение уголовной ответственности за неправомерный доступ к информации Б) Проведение антикоррупционной экспертизы нормативных актов В) Установка антивирусного ПО на рабочие станции Г) Разработка кодексов этики для ИТ-специалистов Д) Обязательное декларирование доходов госслужащих **Правильные ответы:** А, Б, Д. **Объяснение:** • **А** — правовая мера, так как устанавливает юридическую ответственность за противоправные действия. • **Б** — профилактическая правовая мера, направленная на выявление коррупциогенных факторов в нормативных

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	й деятельности		актах. • **Д** — правовая мера контроля за доходами госслужащих, предотвращающая конфликт интересов. *Варианты В и Г не являются правовыми мерами: В — техническая мера, Г — морально-этическая.* **Вопрос 2.** Какие международные документы регулируют защиту информации? (Выберите 3 варианта.) А) Будапештская конвенция о киберпреступности Б) Всеобщая декларация прав человека В) Конвенция о защите физических лиц при обработке ПДн (Совет Европы) Г) Женевские конвенции Д) Резолюции ООН по международной информационной безопасности **Правильные ответы:** А, В, Д. **Объяснение:** • **А** — регулирует борьбу с киберпреступностью. • **В** — устанавливает стандарты защиты персональных данных. • **Д** — закрепляет принципы международного сотрудничества в сфере ИБ. *Варианты Б и Г не относятся напрямую к регулированию ИБ.* **Вопрос 3.** Какие нормативные акты РФ содержат положения о защите государственной тайны? (Выберите 3 варианта.) А) Закон РФ «О государственной тайне» Б) Указ Президента о перечне сведений, отнесённых к гостайне В) Федеральный закон «О коммерческой тайне» Г) Постановление Правительства о порядке допуска к гостайне Д) Трудовой кодекс РФ **Правильные ответы:** А, Б, Г. **Объяснение:** • **А** — базовый закон, определяющий понятие, режимы и порядок защиты гостайны. • **Б** — устанавливает конкретный перечень сведений, составляющих гостайну. • **Г** — регламентирует процедуры допуска лиц к гостайне. *Варианты В и Д не регулируют защиту гостайны (В — о коммерческой тайне, Д — общие трудовые нормы).*
Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	**Задания открытого типа с развёрнутым ответом** **Вопрос 1.** Опишите основные элементы Концепции правового обеспечения информационной безопасности РФ. Приведите примеры нормативных актов, реализующих каждый элемент. **Примерный ответ:** Концепция правового обеспечения ИБ РФ включает: 1. **Нормативно-правовую базу** (ФЗ «Об информации…», ФЗ «О персональных данных», Доктрина ИБ). 2. **Механизмы регулирования** (лицензирование, сертификация, контроль за соблюдением требований). 3. **Международное сотрудничество** (ратификация Будапештской конвенции, участие в ООН-группах по ИБ).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	поведению и противодействовать им в профессиональной деятельности		4. **Ответственность за нарушения** (ст. 272–274.1 УК РФ, административные штрафы). 5. **Просветительские меры** (обучение специалистов, информирование граждан о рисках). **Примеры актов:** • ФЗ № 149-ФЗ — базовые принципы ИБ. • Указ Президента РФ от 05.12.2016 № 646 (Доктрина информационной безопасности РФ) — стратегические цели и задачи; • Постановление Правительства от 01.11.2012 № 1119 — требования к защите персональных данных при их обработке; • Приказы ФСТЭК, ФСБ, Минцифры — ведомственные регламенты по технической и организационной защите информации. **Вопрос 2.** Проанализируйте, как законодательство РФ противодействует коррупционным рискам в сфере закупок ИТ-решений для государственных нужд. Укажите конкретные правовые механизмы и нормативные акты. **Примерный ответ:** Законодательство РФ использует комплекс правовых механизмов для профилактики коррупции в ИТ-закупках: 1. **Обязательная прозрачность процедур** (Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе…»): o публикация извещений и документации в ЕИС (Единая информационная система); o открытые аукционы и конкурсы; o обязательное общественное обсуждение крупных закупок. 2. **Антикоррупционные ограничения** (ст. 31 № 4 Newton-ФЗ): o запрет на участие лиц с конфликтом интересов; o проверка наличия судимости за экономические преступления; o требование отсутствия в реестре недобросовестных поставщиков. 3. **Контроль и аудит** (ст. 99 № 44-ФЗ): o мониторинг со стороны ФАС, казначейства, прокуратуры; o обязательные отчёты о исполнении контрактов; o внеплановые проверки при сигналах о нарушениях. 4. **Ответственность за нарушения** (УК РФ, КоАП РФ): o ст. 200.4 УК РФ — злоупотребления в сфере закупок; o административные штрафы за нарушение процедур (гл. 7 КоАП РФ); o дисквалификация должностных лиц. 5. **Стандартизация требований** (приказы Минцифры, ГОСТы): o типовые технические задания; o единые критерии оценки предложений; o обязательная экспертиза ИТ-решений. **Вопрос 3.** Охарактеризуйте роль международных стандартов (ISO/IEC) в правовом обеспечении информационной безопасности РФ. Приведите 3–4 примера конкретных стандартов и объясните, как они интегрированы в российское

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			законодательство и практику. **Примерный ответ:** Международные стандарты ISO/IEC служат основой для гармонизации российского законодательства с мировыми практиками ИБ. Их интеграция происходит через: • прямое применение (в виде национальных стандартов ГОСТ Р); • учёт требований в федеральных законах и подзаконных актах; • использование как базы для отраслевых регламентов. **Примеры стандартов и их реализация в РФ:** 1. **ISO/IEC 27001:2013** («Системы менеджмента ИБ — Требования»): o адаптирован как ГОСТ Р ИСО/МЭК 27001-2022; o обязателен для операторов критической информационной инфраструктуры (КИИ) по ФЗ № 187-ФЗ; o используется при сертификации СЗИ (средств защиты информации). 2. **ISO/IEC 27002:2022** («Свод правил по управлению ИБ»): o положения включены в приказы ФСТЭК № 21, № 17 (требования к организационным мерам защиты); o применяется при разработке внутренних регламентов организаций. 3. **ISO/IEC 27701:2019** («Расширение для управления персональными данными»): o учтён в ФЗ № 152-ФЗ («О персональных данных»); o служит основой для политик конфиденциальности и процедур обработки ПДн. 4. **ISO/IEC 15408** («Критерии оценки безопасности ИТ», «Общие критерии»): o реализован через систему сертификации ФСТЭК и ФСБ; o обязателен для СЗИ, используемых в госсекторе и на объектах КИИ; o лежит в основе требований к криптографической защите. **Значение интеграции:** • повышение доверия к российским ИТ-решениям на международном рынке; • унификация требований для трансграничной передачи данных; • снижение рисков за счёт применения проверенных практик.

Критерии оценивания тестового задания:

Оценка	Критерии оценивания
отлично	от 90 до 100 % правильно выполненных заданий
хорошо	от 70 до 89 % правильно выполненных заданий
удовлетворительно	от 50 до 69 % правильно выполненных заданий
неудовлетворительно	менее 50 % правильно выполненных заданий

4.2 ТИПОВЫЕ ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Практические задания должны отражать умение обучающегося применять осваиваемую компетенцию в практических ситуациях и при решении производственных задач (индикаторы УМЕТЬ).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Задание 1** Вы работаете специалистом по информационной безопасности в государственном учреждении. Вам поступает предложение от представителя коммерческой компании: за денежное вознаграждение вы должны «закрыть глаза» на выявленные в ходе аудита уязвимости в системе защиты информации, чтобы компания получила выгодный контракт. *Задание:* 1. Опишите, какие коррупционные риски возникают в данной ситуации. 2. Перечислите действия, которые вы обязаны предпринять согласно антикоррупционному законодательству и внутренним регламентам. 3. Укажите, к каким последствиям для вас и организации может привести согласие на предложение. *Решение:* 1. Коррупционный риск — конфликт интересов, подкуп должностного лица, нарушение принципов информационной безопасности ради личной выгоды. 2. Необходимо: ○ отказаться от предложения; ○ уведомить руководство и службу безопасности организации; ○ зафиксировать факт предложения (переписку, аудио-, видеоматериалы, если возможно); ○ подать уведомление в антикоррупционную комиссию или правоохранительные органы. 3. Последствия: ○ уголовная ответственность (ст. 290 УК РФ — получение взятки); ○ утрата доверия, увольнение, дисквалификация; ○ компрометация системы защиты информации, утечка данных, репутационные и финансовые потери организации. **Задание 2** Вам как сотруднику отдела информационной безопасности поручено выбрать поставщика средств защиты информации. Один из кандидатов — фирма, где работает ваш близкий родственник. *Задание:* 1. Определите, есть ли в этой ситуации конфликт интересов. 2. Какие меры вы должны предпринять, чтобы исключить коррупционные риски? 3. Как оформить уведомление о конфликте интересов? *Решение:*

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			1. Да, ситуация создаёт потенциальный конфликт интересов: личная связь может повлиять на объективность выбора. 2. Необходимо: ○ заявить о конфликте интересов руководству; ○ воздержаться от участия в принятии решения по выбору поставщика; ○ передать полномочия другому сотруднику; ○ обеспечить прозрачность процедуры отбора (публичные критерии, конкурсный отбор). 3. Уведомление оформляется в письменной форме с указанием: ○ сути конфликта (родственная связь); ○ должности и ФИО родственника; ○ мер, предложенных для устранения конфликта; ○ даты и подписи. **Задание 3** Вы обнаружили, что ваш коллега регулярно передаёт конфиденциальные данные сторонним лицам за вознаграждение. *Задание:* 1. Какие признаки указывают на коррупционное правонарушение? 2. Каковы ваши действия в соответствии с антикоррупционной политикой организации? 3. Какие нормативные акты регулируют данную ситуацию? *Решение:* 1. Признаки: ○ несанкционированный доступ и передача информации; ○ получение материального вознаграждения; ○ скрытность действий, обход контрольных процедур. 2. Действия: ○ зафиксировать факты (логи, переписки, свидетельства); ○ сообщить руководству и службе безопасности; ○ не вступать в контакт с нарушителем, не пытаться разрешить ситуацию самостоятельно; ○ сотрудничать с внутренней проверкой и правоохранительными органами. 3. Нормативные акты: ○ Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»; ○ ст. 272 УК РФ (неправомерный доступ к компьютерной информации); ○ внутренние антикоррупционные регламенты организации.
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает	**Задание 1** Вам необходимо разработать краткую памятку для сотрудников отдела информационной безопасности о действиях при предложении взятки. *Задание:*

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
		вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	1. Перечислите ключевые правовые нормы, которые следует упомянуть в памятке. 2. Укажите пошаговый алгоритм действий сотрудника. 3. Приведите примеры формулировок отказа от предложения. *Решение:* 1. Правовые нормы: o ст. 290 УК РФ (получение взятки); o ст. 291 УК РФ (дача взятки); o ФЗ № 273-ФЗ «О противодействии коррупции» (обязанность сообщать о фактах коррупции). 2. Алгоритм: o отказаться от предложения; o зафиксировать детали (кто, когда, как предложил, сумма, способ передачи); o немедленно уведомить руководство и службу безопасности; o при необходимости обратиться в правоохранительные органы. 3. Примеры формулировок: o «Я не могу принять это предложение, так как оно противоречит закону и моим должностным обязанностям»; o «Я обязан сообщить о данном предложении руководству»; o «Такие действия незаконны, я не буду в них участвовать». **Задание 2** В организации планируется обучение сотрудников по профилактике коррупции в сфере информационной безопасности. *Задание:* 1. Составьте план короткого тренинга (3–4 темы). 2. Для каждой темы укажите ключевой правовой акт или норму. 3. Предложите одно практическое упражнение для закрепления материала. *Решение:* 1. План тренинга: o Тема 1. Понятие коррупции и её проявления в сфере ИБ (примеры: подкуп, конфликт интересов, утечка данных за вознаграждение). o Тема 2. Правовые основы противодействия коррупции (ФЗ № 273-ФЗ, УК РФ). o Тема 3. Внутренние антикоррупционные процедуры организации (порядок уведомления, ответственность). o Тема 4. Этические аспекты профессиональной деятельности в ИБ. 2. Правовые акты: o Тема 1: ФЗ № 273-ФЗ, ст. 1 (определение коррупции). o Тема 2: ст. 290, 291 УК РФ; ФЗ № 273-ФЗ, ст. 9 (обязанность уведомлять). o Тема 3: локальные акты организации (положение о конфликте интересов, кодекс этики).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			○ Тема 4: профессиональные стандарты ИБ, этический кодекс. 3. Упражнение: разбор кейса — сотрудник получает предложение скрыть уязвимость за вознаграждение. Участники должны: ○ определить коррупционный риск; ○ выбрать правильные действия; ○ сослаться на нормы закона. **Задание 3** Вам поручено проверить соответствие внутренних документов организации антикоррупционному законодательству в части ИБ. *Задание:* 1. Перечислите, какие документы нужно проанализировать. 2. Укажите, какие положения должны быть в них закреплены. 3. Приведите пример формулировки антикоррупционной оговорки для договора с подрядчиком. *Решение:* 1. Документы для анализа: ○ положение о конфликте интересов; ○ кодекс этики и служебного поведения; ○ регламент проведения аудитов ИБ; ○ договоры с подрядчиками (в т. ч. на оказание услуг ИБ); ○ порядок уведомления о фактах коррупции. 2. Обязательные положения: ○ определение конфликта интересов и порядок его урегулирования; ○ обязанность сообщать о предложениях взятки; ○ ответственность за коррупционные правонарушения; ○ процедуры проверки контрагентов и поставщиков ИБ-решений; ○ правила доступа к конфиденциальной информации. 3. Пример оговорки: «Стороны обязуются не предлагать, не давать, не требовать и не принимать взятки, подарки или иные преимущества, которые могут повлиять на исполнение обязательств по настоящему договору. В случае выявления фактов коррупции, стороны обязаны незамедлительно уведомить друг друга и соответствующие органы. Нарушение данного положения является основанием для расторжения договора».
Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает	**Задание 1** **Условие** Вы — системный администратор компании. Вам поступило электронное письмо от неизвестного отправителя с вложением «Акт_проверки_СИБ.doc.exe». В тексте письма указано, что это

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
	проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	срочный документ от регулятора, требующий немедленного ознакомления. Перечислите **не менее 5 признаков**, указывающих на потенциальную угрозу, и опишите **последовательность ваших действий** для предотвращения заражения. **Решение** **Признаки угрозы:** 1. Расширение файла .exe (исполняемый файл) при заявленном формате документа .doc. 2. Неизвестный отправитель. 3. Фраза «срочный документ от регулятора» как метод психологического давления. 4. Отсутствие официальной подписи или контактов регулятора. 5. Подозрительное имя файла (смешение форматов). **Действия:** 1. Не открывать вложение. 2. Проверить адрес отправителя на подозрительные домены. 3. Сообщить в службу ИБ компании о письме. 4. Заблокировать отправителя в почтовой системе. 5. Провести сканирование рабочей станции антивирусом. **Задание 2** **Условие** Ваш коллега просит передать ему через флеш-накопитель «важный файл», но предупреждает, что антивирус на его компьютере «часто ругается на этот файл». Он утверждает, что это «ложное срабатывание». Объясните, **почему нельзя выполнять эту просьбу**, и предложите **альтернативный безопасный способ** передачи данных. **Решение** **Причины отказа:** • Антивирус реагирует на потенциально вредоносный код. • Передача файла может заразить вашу систему и корпоративную сеть. • Действие коллеги нарушает политику ИБ компании. **Альтернативный способ:** 1. Попросить коллегу загрузить файл в корпоративный облачный диск с антивирусной проверкой. 2. Если файл критически важен — обратиться в службу ИБ для анализа файла в изолированной среде. 3. Использовать зашифрованный канал передачи (например, S/MIME для почты). **Задание 3**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			Условие Вам предложили «ускорить» установку лицензионного ПО, предоставив «специальный активатор» в виде исполняемого файла. Укажите **не менее 3 рисков** такого действия и опишите, как **официально** получить лицензию без нарушения ИБ. **Решение** **Риски:** 1. Активатор может содержать троянскую программу. 2. Нарушение лицензионного соглашения ведёт к юридическим последствиям. 3. Заражение сети компании, утечка данных. **Официальный порядок:** 1. Обратиться в отдел закупок/ИТ для оформления заявки на лицензию. 2. Использовать корпоративный портал поставщика ПО для скачивания официального дистрибутива. 3. Применять только ключи, предоставленные лицензирующим отделом.
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Задание 1** **Условие** Вы обнаружили, что ваш подчинённый регулярно использует нелицензионное ПО для выполнения рабочих задач. Он объясняет это «экономией бюджета». Укажите **не менее 3 нормативных актов РФ**, регулирующих использование ПО, и опишите **ваши действия** как руководителя. **Решение** **Нормативные акты:** 1. **ГК РФ, часть IV** (ст. 1261 – 1302) — охрана программ для ЭВМ как объектов авторского права. 2. **ФЗ от 27.07.2006 № 149-ФЗ** «Об информации, информационных технологиях…» — требования к использованию лицензированного ПО. 3. **КоАП РФ, ст. 7.12** — административная ответственность за нарушение авторских прав. **Действия руководителя:** 1. Зафиксировать факт использования нелицензионного ПО (скриншоты, логи). 2. Провести беседу с сотрудником о последствиях нарушений. 3. Направить запрос в ИТ-отдел на предоставление лицензионного аналога. 4. При повторении — применить дисциплинарное взыскание. **Задание 2** **Условие**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			Вам поступило предложение от поставщика ИБ-решений «предоставить скидку 50 %» при условии, что вы «закроете глаза» на отсутствие сертификатов соответствия у продукта. Перечислите **правовые последствия** такого соглашения и опишите **порядок отказа** от предложения. **Решение** **Правовые последствия:** • **Уголовная ответственность** по ст. 290 УК РФ (получение взятки) или ст. 291 УК РФ (дача взятки). • **Административная ответственность** по ст. 19.28 КоАП РФ (незаконное вознаграждение). • **Аннулирование контрактов** и репутационные риски для компании. **Порядок отказа:** 1. Отклонить предложение в письменной форме, указав на недопустимость коррупции. 2. Сообщить о попытке склонения к правонарушению в службу безопасности компании. 3. Зафиксировать переписку/аудиозапись (при наличии) как доказательство. 4. Продолжить работу только с сертифицированными продуктами. **Задание 3** **Условие** Вы выявили, что сотрудник передаёт третьим лицам доступ к корпоративной системе ИБ под предлогом «консультации». Назовите **не менее 3 статей УК РФ**, которые могут быть применены, и опишите **алгоритм действий** для пресечения нарушения. **Решение** **Статьи УК РФ:** 1. **Ст. 272** — неправомерный доступ к компьютерной информации. 2. **Ст. 183** — незаконное получение и разглашение сведений, составляющих коммерческую тайну. 3. **Ст. 292** — служебный подлог (если изменены логи доступа). **Алгоритм действий:** 1. Немедленно заблокировать учётную запись сотрудника. 2. Собрать доказательства (логи систем, переписки). 3. Сообщить в службу безопасности и юридический отдел. 4. Провести внутреннее расследование. 5. При наличии состава преступления — направить материалы в правоохранительные органы.
Тема 3. Организационно-	УК-10. Способен формировать	ИУК-10.2 Предупреждает коррупционные риски в	**Задание 1** Вы — специалист по информационной безопасности в госучреждении. Вам предлагают

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
правовое обеспечение информационной безопасности	нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	«ускорить» согласование технического решения по защите данных за денежное вознаграждение. **Задача:** 1. Определите, какие нормы законодательства РФ запрещают подобные действия. 2. Составьте краткий (5–7 предложений) письменный отказ, ссылаясь на конкретные статьи законов. 3. Укажите, в какой орган следует сообщить о попытке склонения к коррупции. **Решение:** 1. Действия запрещены: o ст. 9 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции» (запрет на принятие вознаграждений); o ст. 290 УК РФ (получение взятки). 2. Пример отказа: «В соответствии со ст. 9 ФЗ № 273-ФЗ я не вправе принимать денежные вознаграждения за выполнение должностных обязанностей. Предложение о выплате вознаграждения расценивается как попытка склонения к коррупционному правонарушению. Прошу прекратить подобные обсуждения. В случае повторения я буду вынужден уведомить компетентные органы». 3. Сообщить в подразделение по профилактике коррупционных правонарушений госоргана или в прокуратуру (ст. 11 ФЗ № 273-ФЗ). **Задание 2** Вам как ИТ-специалисту поручено выбрать поставщика ПО для защиты информации. Один из кандидатов намекает, что «личное вознаграждение» повысит шансы его компании. **Задача:** 1. Перечислите шаги, которые вы предпримете для предотвращения конфликта интересов. 2. Укажите, какие документы нужно оформить, чтобы зафиксировать попытку склонения к коррупции. 3. Назовите сроки подачи уведомления о конфликте интересов. **Решение:** 1. Шаги: o отказаться от переговоров с намекающим представителем; o уведомить руководство и комиссию по этике; o провести закупку через конкурентные процедуры (44-ФЗ или 223-ФЗ). 2. Документы: o служебная записка на имя руководителя с описанием ситуации; o акт о факте склонения к коррупции (с свидетелями, если возможно). 3. Срок уведомления — не позднее следующего рабочего дня (п. 1 ч. 2 ст. 11 ФЗ № 273-ФЗ). **Задание 3** Вы обнаружили, что ваш коллега принимает подарки от подрядчика, обслуживающего системы

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			защиты информации. **Задача:** 1. Определите, какие статьи законов нарушаются. 2. Составьте план действий для пресечения нарушения. 3. Укажите, какие меры дисциплинарной ответственности могут быть применены. **Решение:** 1. Нарушения: o ст. 575 ГК РФ (запрет подарков стоимостью свыше 3 000 руб. служащим); o ст. 19.28 КоАП РФ (незаконное вознаграждение от юрлица). 2. План: o зафиксировать факт (фото, свидетели); o сообщить руководителю и в комиссию по противодействию коррупции; o инициировать служебную проверку. 3. Меры: o замечание, выговор (ст. 192 ТК РФ); o увольнение по п. 7.1 ст. 81 ТК РФ (утрата доверия).
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Задание 1** Составьте памятку для сотрудников ИТ-подразделения (5–7 пунктов) о действиях при попытке склонения к коррупции. Включите: • ссылки на законы; • порядок уведомления руководства; • контакты органов, куда можно обратиться анонимно. **Решение:** Памятка: 1. Откажитесь от принятия любых вознаграждений за выполнение должностных обязанностей (ст. 9 ФЗ № 273-ФЗ). 2. Зафиксируйте детали предложения (дата, время, суть, свидетели). 3. Незамедлительно уведомите руководителя и комиссию по этике. 4. Подайте письменное уведомление о факте склонения к коррупции (срок — следующий рабочий день). 5. При угрозе или давлении обратитесь в прокуратуру или МВД. 6. Используйте телефон горячей линии госоргана или Антикоррупционного центра. 7. Сохраняйте конфиденциальность информации о расследовании. **Задание 2** Разработайте чек-лист для самооценки коррупционных рисков при закупках ПО и оборудования для информационной безопасности. Включите не менее 5 критериев. **Решение:**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			Чек-лист: 1. Есть ли конфликт интересов у членов закупочной комиссии? (ст. 10 ФЗ № 273-ФЗ). 2. Обоснованы ли требования к поставщику в документации? (ст. 33 44-ФЗ). 3. Проведён ли анализ рыночных цен перед определением НМЦК? 4. Есть ли ограничения на участие аффилированных лиц? (ст. 31 44-ФЗ). 5. Ведётся ли аудио- или видеозапись процедур вскрытия заявок? 6. Опубликованы ли протоколы закупок в ЕИС в установленные сроки? 7. Есть ли механизм обжалования решений комиссии? **Задание 3** Подготовьте краткий (1–2 абзаца) текст выступления на собрании сотрудников о важности антикоррупционного поведения в ИТ-сфере. Включите: • 2–3 примера коррупционных рисков в ИТ; • ссылки на последствия (штрафы, увольнение, уголовная ответственность); • призыв к формированию культуры нетерпимости к коррупции. **Решение:** «Коллеги, в сфере информационной безопасности коррупционные риски особенно опасны: это может быть выбор ненадёжного ПО за вознаграждение, сокрытие уязвимостей или несанкционированный доступ к данным. Такие действия ведут к серьёзным последствиям: штрафам по ст. 19.28 КоАП РФ, увольнению по п. 7.1 ст. 81 ТК РФ или уголовной ответственности по ст. 290 УК РФ. Мы должны формировать культуру нетерпимости к коррупции: отказывать от незаконных предложений, сообщать о подозрительных ситуациях и строго следовать регламентам. Только так мы обеспечим безопасность данных и доверие клиентов».

Критерии оценивания практических занятий:

Оценка	Критерии оценивания
отлично	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи, формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, обосновывает свои суждения и даёт правильные ответы на вопросы преподавателя
хорошо	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи и формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, но содержание ответов имеют некоторые неточности и требуют уточнения и комментария со стороны преподавателя
удовлетворительно	Выставляется, если обучающийся знает и понимает материал по заданной теме, но изложение неполное, непоследовательное, допускаются неточности в определении понятий, студент не может обосновать свои ответы на уточняющие вопросы преподавателя
неудовлетворительно	Выставляется, если обучающийся допускает ошибки в определении понятий, искажающие их смысл, беспорядочно и неуверенно излагает материал. Делает ошибки в ответах на уточняющие вопросы преподавателя

4.3. ТИПОВЫЕ ЗАДАНИЯ ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Контрольные работы содержат несколько практических заданий по индивидуальным вариантам, в полном объеме охватывающих изученный материал по указанной теме (индикаторы УМЕТЬ). Выполнение контрольных работ позволяет определить результат освоения компетенций по дисциплине в рамках рассматриваемой темы, оцениваемый с помощью соответствующих индикаторов достижения компетенций

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Вариант 1** **Задание.** В организации планируется закупка системы защиты информации. Руководитель отдела ИТ получил от одного из поставщиков конфиденциальное предложение: скидка 30 % при условии, что решение будет принято в пользу этого поставщика без проведения открытого тендера. **Вопросы:** 1. Какие коррупционные риски возникают в данной ситуации? 2. Какие действия должен предпринять сотрудник, чтобы исключить вмешательство в профессиональную деятельность и предотвратить коррупционное правонарушение? 3. Какие нормативные акты регулируют процедуру закупок в данной ситуации? **Вариант 2** **Задание.** Сотрудник службы ИБ обнаружил уязвимость в корпоративной системе, которая позволяет получать доступ к конфиденциальным данным. Он решает не сообщать о ней руководству, а предложить сторонней компании «устранить проблему за вознаграждение» без оформления официального договора. **Вопросы:** 1. В чём заключается коррупционный риск в данном случае? 2. Какие последствия могут наступить для сотрудника и организации? 3. Каков правильный порядок действий сотрудника при обнаружении уязвимости? **Вариант 3** **Задание.** Руководитель подразделения требует от подчинённого передать ему логин и пароль от системы контроля доступа, мотивируя это «необходимостью оперативного реагирования». **Вопросы:** 1. Почему такое требование несёт коррупционный риск? 2. Как должен поступить сотрудник, чтобы не нарушить профессиональную этику и законодательство? 3. Какие меры защиты информации нарушаются в данной ситуации?
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Вариант 1** **Задание.** Вы — специалист по ИБ в госучреждении. Вам предложили вознаграждение за предоставление доступа к закрытой базе данных. **Вопросы и задания:** 1. Перечислите статьи УК РФ, которые регулируют данную ситуацию. 2. Составьте краткий алгоритм действий при получении подобного предложения. 3. Укажите, в какие органы следует обратиться для фиксации факта склонения к коррупции. **Решение:** 1. Ст. 290 УК РФ (получение взятки), ст. 291 УК РФ (дача взятки), ст. 291.1 УК РФ (посредничество во взяточничестве).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			2. Алгоритм: o отказать в предложении; o зафиксировать детали (время, место, суть предложения, данные предложившего); o уведомить руководство и службу безопасности; o подать заявление в правоохранительные органы. 3. Органы: МВД (отдел по борьбе с коррупцией), ФСБ, прокуратура. **Вариант 2** **Задание.** В компании выявлен факт систематического копирования конфиденциальных данных сотрудником для передачи конкурентам за вознаграждение. **Вопросы и задания:** 1. Какие статьи УК РФ и ФЗ применяются в данном случае? 2. Разработайте 3–4 профилактические меры для предотвращения подобных ситуаций. 3. Опишите, как должна быть организована система контроля доступа, чтобы минимизировать риски. **Решение:** 1. Ст. 183 УК РФ (незаконное получение и разглашение коммерческой тайны), ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ФЗ «О коммерческой тайне» № 98-ФЗ. 2. Профилактические меры: o регулярный аудит прав доступа; o DLP-система для контроля утечек; o подписание соглашений о неразглашении (NDA); o обучение персонала по ИБ. 3. Система контроля: ролевая модель доступа, журнал событий, двухфакторная аутентификация, ограничение внешних носителей. **Вариант 3** **Задание.** Вам как руководителю ИТ-подразделения поручили «закрыть глаза» на нарушения в обработке персональных данных ради ускорения проекта. **Вопросы и задания:** 1. Какие законы РФ нарушаются в этой ситуации? 2. Приведите 3 аргумента, обосновывающие недопустимость такого решения. 3. Предложите альтернативный вариант действий, соответствующий закону. **Решение:** 1. ФЗ «О персональных данных» № 152-ФЗ, КоАП ст. 13.11, УК ст. 137. 2. Аргументы: o риск штрафов и уголовной ответственности; o утрата доверия клиентов и репутации; o возможность судебных исков со стороны субъектов ПДн.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			3. Альтернатива: провести аудит соответствия ПДн, внедрить необходимые меры защиты, согласовать сроки с учётом требований закона.
Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Вариант 1** Вы — специалист по ИБ в госучреждении. Вам предлагают «за определённое вознаграждение» не фиксировать обнаруженный вирус в отчётности, чтобы избежать проверки вышестоящей инстанции. **Задание:** 1. Опишите 3–4 аргумента, почему нельзя соглашаться. 2. Укажите, какие нормативные акты регулируют подобные ситуации. 3. Предложите алгоритм действий в этой ситуации. **Вариант 2** В компании выявлен факт использования нелицензионного антивирусного ПО. Руководитель просит «не афишировать» проблему, чтобы не платить штрафы. **Задание:** 1. Перечислите риски для организации при сокрытии факта. 2. Назовите статьи КоАП/УК РФ, которые могут быть применены. 3. Составьте краткий план легализации ПО. **Вариант 3** Вам как ИТ-специалисту предлагают за вознаграждение установить «особый» антивирус, который будет передавать данные третьей стороне. **Задание:** 1. Определите признаки коррупционного предложения. 2. Укажите, какие законы запрещают подобные действия. 3. Опишите порядок уведомления руководства и правоохранительных органов.
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	**Вариант 1** **Ситуация:** В ходе аудита обнаружено, что сотрудник ИТ-отдела регулярно получает «бонусы» от поставщика антивирусного ПО за продление контрактов. **Задание:** 1. Назовите статьи ФЗ «О противодействии коррупции», нарушенные сотрудником. 2. Перечислите меры дисциплинарной и уголовной ответственности. 3. Разработайте 3–4 профилактические меры для предотвращения подобных случаев. **Решение:** 1. Нарушены ст. 10 (конфликт интересов), ст. 12 (ограничения для госслужащих) ФЗ № 273-ФЗ. 2. Дисциплинарная ответственность (выговор, увольнение), уголовная по ст. 290 УК РФ (взятка). 3. Профилактические меры: ○ ежегодное декларирование интересов;

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			○ ротация поставщиков; ○ аудит закупок; ○ горячая линия для сообщений о коррупции. **Вариант 2** **Ситуация:** Руководитель ИТ-подразделения настаивает на закупке дорогого ПО у компании, принадлежащей его родственнику, несмотря на наличие более дешёвых аналогов. **Задание:** 1. Укажите нормы, регулирующие конфликт интересов в госзакупках. 2. Опишите порядок действий сотрудника, заметившего нарушение. 3. Приведите 3 примера документов, подтверждающих злоупотребление. **Решение:** 1. ФЗ № 44-ФЗ (ст. 31 — требования к участникам), ФЗ № 273-ФЗ (ст. 10). 2. Порядок действий: ○ зафиксировать факт предложения; ○ уведомить комиссию по этике; ○ подать заявление в ФАС/прокуратуру. 3. Документы-доказательства: ○ протоколы закупок; ○ договоры с аффилированной фирмой; ○ переписка с руководителем. **Вариант 3** **Ситуация:** Вам как аудитору предлагают «закрыть глаза» на уязвимости в системе ИБ за вознаграждение. **Задание:** 1. Перечислите статьи УК РФ, касающиеся коммерческого подкупа. 2. Составьте шаблон уведомления о коррупционном предложении (5–7 пунктов). 3. Укажите органы, куда можно направить жалобу. **Решение:** 1. Ст. 204 УК РФ (коммерческий подкуп), ст. 304 УК РФ (провокация взятки). 2. Шаблон уведомления: ○ ФИО заявителя; ○ описание предложения; ○ дата и место инцидента; ○ данные предложившего; ○ свидетели (если есть); ○ прилагаемые доказательства; ○ подпись и дата.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			3. Органы: o комиссия по этике организации; o прокуратура; o МВД (отдел по борьбе с экономическими преступлениями); ФАС (если связаны с госзакупками).

Критерии оценивания контрольной работы:

Оценка	Критерии оценивания
отлично	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи, формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, обосновывает свои суждения и даёт правильные ответы на вопросы преподавателя
хорошо	Выставляется, если обучающийся умеет увязывать теорию с практикой (решает задачи и формулирует выводы, умеет пояснить полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом по заданной теме, но содержание ответов имеют некоторые неточности и требуют уточнения и комментария со стороны преподавателя.
удовлетворительно	Выставляется, если обучающийся знает и понимает материал по заданной теме, но изложение неполное, непоследовательное, допускаются неточности в определении понятий, студент не может обосновать свои ответы на уточняющие вопросы преподавателя
неудовлетворительно	Выставляется, если обучающийся допускает ошибки в определении понятий, искажающие их смысл, беспорядочно и неуверенно излагает материал. Делает ошибки в ответах на уточняющие вопросы преподавателя

4.4. ТИПОВЫЕ ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа (индикаторы ЗНАТЬ, УМЕТЬ – на выбор) включает в себя проработку теоретического материала, изучение рекомендуемой литературы, выполнение практико-ориентированных заданий (заполнение таблиц, проведение сравнительного анализа, составление схем и др.), решение практических задач, создание презентаций, написание рефератов, подборка нормативного и иного материала и выполнение других заданий.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
Тема 1. Борьба с угрозами	УК-10. Способен формировать	ИУК-10.1 Знает способы профилактики коррупции и	**Задание 1.** Составьте глоссарий (10–12 терминов) по теме «Коррупционные риски в сфере информационной безопасности». Для каждого термина:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
несанкционированного доступа к информации	нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	формирования нетерпимого отношения к ней.	• дайте определение (с опорой на нормативные акты); • приведите пример проявления в ИТ-среде (например, «продажа доступов к конфиденциальным данным»); • укажите способ профилактики. **Формат:** таблица с колонками: «Термин», «Определение», «Пример», «Профилактика». **Задание 2.** Проанализируйте 3 реальных кейса (из открытых источников) о коррупционных нарушениях в сфере ИБ (например, инсайдерские утечки, подкуп сотрудников ИТ-отделов). Для каждого кейса: 1. Опишите схему правонарушения. 2. Укажите уязвимости в системе ИБ, которые были использованы. 3. Предложите меры профилактики, которые могли бы предотвратить инцидент. **Формат:** краткий отчёт (1–2 стр. на кейс) с выводами. **Задание 3.** Разработайте памятку для сотрудников «Как распознать и предотвратить коррупционное предложение в сфере ИБ». Включите: • типичные сценарии склонения к нарушению (не менее 5); • алгоритм действий при получении подозрительного предложения; • контакты для сообщения о нарушениях. **Формат:** инфографика или буклет (5–7 слайдов/страниц). **Задание 4.** Подготовьте доклад (5–7 мин.) на тему: «Роль корпоративной культуры в профилактике коррупции в ИТ-компаниях». Осветите: • принципы формирования «антикоррупционного климата»; • примеры кодексов этики ИТ-специалистов; • методы обучения сотрудников распознаванию рисков. **Задание 5.** Создайте тест (10 вопросов) для самопроверки знаний по теме «Профилактика коррупции в ИБ». Включайте: • вопросы на знание нормативных актов; • ситуационные задачи (например, «Как поступить, если коллега предлагает продать базу данных?»); • варианты ответов с обоснованием правильного решения.
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную	**Задание 1.** Разработайте регламент «Проверка контрагентов на коррупционные риски при закупках ИТ-решений». Включите: • этапы проверки (анализ репутации, аудит документов, мониторинг конфликтов интересов); • критерии отбора надёжных поставщиков; • форму отчёта о результатах проверки. **Формат:** документ в виде инструкции (2–3 стр.) с чек-листом.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
		деятельность в случаях склонения к коррупционным правонарушениям	**Задание 2.** Решите кейс: В компании планируется внедрение новой системы защиты данных. Один из поставщиков предлагает «ускорить» процесс за неофициальное вознаграждение, обещая при этом скидку на ПО. **Задачи:** 1. Определите коррупционные риски в данной ситуации. 2. Составьте письмо-отказ поставщику с обоснованием (ссылаясь на нормы закона). 3. Предложите альтернативный механизм выбора поставщика (например, тендер с прозрачными критериями). **Формат:** письмо (0,5 стр.) + краткий анализ (1 стр.). **Задание 3.** Постройте схему «Система внутреннего контроля за коррупционными рисками в ИТ-отделе». Отразите: • роли ответственных лиц (руководитель, служба безопасности, аудиторы); • периодичность проверок; • инструменты мониторинга (журналы доступа, аудит прав, анализ аномалий); • порядок реагирования на инциденты. **Формат:** графическая схема + пояснительная записка (1 стр.). **Задание 4.** Подготовьте презентацию (8–10 слайдов) для тренинга «Защита профессиональной независимости: как отказать в коррупционном предложении». Включите: • юридические основания для отказа (ссылки на УК РФ, ФЗ «О противодействии коррупции»); • психологические техники уверенного отказа; • сценарии ролевых игр (например, диалог с «предлагающим» коллегой). **Задание 5.** Разработайте план аудита ИТ-инфраструктуры на предмет коррупционных уязвимостей. Укажите: • объекты проверки (серверы, базы данных, системы доступа); • методы выявления злоупотреблений (анализ логов, проверка прав пользователей, тестирование на проникновение); • критерии оценки рисков (шкала от низкого до критического); • форму итогового отчёта. **Формат:** план-график (таблица) + описание методологии (2 стр.).
Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	1. **Анализ кейса: «Теневые схемы в закупках ПО»** *Задание.* Изучите реальный кейс (например, дело о завышении стоимости лицензий на антивирусное ПО в госучреждении). Выпишите: ○ признаки коррупционной схемы (откаты, аффилированность); ○ способы её маскировки (фиктивные тендеры, дробление закупок);

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
	экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности		○ меры профилактики (публичность закупок, аудит). *Формат:* таблица из 3 колонок с краткими тезисами (не более 5 пунктов в каждой). *Критерии оценки:* ○ точность выявления коррупционных признаков; ○ обоснованность предложенных мер профилактики; ○ ссылки на антикоррупционные нормы (ФЗ № 273). 2. **Разработка памятки «Этичные правила ИТ-специалиста»** *Задание.* Составьте памятку для сотрудников ИТ-отдела (5–7 пунктов), включающую: ○ запрет на принятие подарков от поставщиков ПО; ○ порядок уведомления о конфликте интересов; ○ правила выбора антивирусных решений без личной выгоды. *Формат:* текстовый документ с маркированными списками. *Критерии оценки:* ○ соответствие принципам антикоррупционной политики; ○ практичность рекомендаций; ○ ясность формулировок. 3. **Дискуссия «Моральный выбор в ИТ»** *Задание.* Подготовьте 3 аргумента «за» и 3 «против» следующей ситуации: *«Сотрудник ИТ-отдела знает, что его начальник получает откат от поставщика антивирусов, но молчит, опасаясь увольнения».* *Формат:* эссе объёмом 300–400 слов с выводами. *Критерии оценки:* ○ глубина анализа этических аспектов; ○ опора на антикоррупционные принципы; ○ логичность аргументации. 4. **Кейс-задача «Проверка поставщика»** *Задание.* Вам как члену закупочной комиссии нужно проверить компанию-поставщика антивирусов. Составьте список из 5 вопросов, которые помогут выявить признаки коррупции (например, связь с чиновниками, офшорные счета). *Формат:* нумерованный список вопросов с пояснениями (1–2 предложения на вопрос). *Критерии оценки:* ○ релевантность вопросов коррупционным рискам; ○ конкретика формулировок; ○ учёт требований ФЗ № 44. 5. **Мини-исследование «Общественное мнение о коррупции в ИТ»** *Задание.* Проведите опрос 5–7 человек (студенты, преподаватели, ИТ-специалисты) на тему: *«Считаете ли вы, что закупки антивирусного ПО часто сопровождаются коррупцией?*

<table>
<tr><th>Тема</th><th>Код и формулировка компетенции</th><th>Индикаторы достижения компетенции</th><th>Типовое задание для самостоятельной работы</th></tr>
<tr><td></td><td></td><td></td><td>Почему?»
Обобщите результаты в виде диаграммы и краткого анализа (1 страница).
Формат: PDF-документ с диаграммой и выводами.
Критерии оценки:
o репрезентативность выборки;
o корректность визуализации данных;
o выводы о путях профилактики коррупции</td></tr>
<tr><td></td><td></td><td>ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям</td><td>1. Сравнительный анализ правовых норм
Задание. Заполните таблицу, сопоставив статьи УК РФ и ФЗ, регулирующие борьбу с коррупцией в ИТ-сфере:
<table>
<tr><td>Нормативный акт</td><td>Статья</td><td>Содержание</td><td>Применение к ИТ-сфере</td></tr>
<tr><td>УК РФ № 290</td><td>ст. 290</td><td>Получение взятки</td><td>Закупки ПО</td></tr>
<tr><td>ФЗ № 273</td><td>ст. 13.3</td><td>Обязанность организаций принимать антикоррупционные меры</td><td>Политика ИТ-компаний</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
2. Критерии оценки:
o точность цитирования норм;
o корректность примеров из ИТ-сферы;
o полнота охвата (не менее 4 норм).
3. Разбор судебной практики
Задание. Найдите 2 судебных решения по делам о коррупции в сфере ИТ (например, завышение цен на антивирусы). Выпишите:
o фабулу дела;
o применённые статьи УК РФ/ФЗ;
o наказание;
o уроки для профилактики.
Формат: краткий отчёт (2 страницы) с ссылками на источники.
Критерии оценки:
o актуальность кейсов (не старше 5 лет);</td></tr>
</table>

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
			○ точность правовых ссылок; ○ практическая значимость выводов. 4. **Разработка локального акта «Антикоррупционная политика ИТ-отдела»** *Задание.* Создайте проект документа (3–4 раздела), включающего: ○ цели и задачи политики; ○ перечень коррупционно-опасных должностей (например, менеджер по закупкам ПО); ○ порядок проверки контрагентов; ○ санкции за нарушения. *Формат:* документ в стиле корпоративного регламента. *Критерии оценки:* ○ соответствие ФЗ № 273; ○ детализация процедур; ○ реалистичность санкций. 5. **Правовая экспертиза договора на поставку антивирусов** *Задание.* Проанализируйте типовой договор (предоставляется преподавателем) на наличие коррупционных рисков. Выпишите: ○ подозрительные условия (например, отсутствие штрафных санкций); ○ пробелы в описании обязательств поставщика; ○ рекомендации по доработке. *Формат:* таблица с колонками «Риск», «Обоснование», «Решение». *Критерии оценки:* ○ глубина правового анализа; ○ конкретные предложения по исправлению; ○ ссылки на ГК РФ и ФЗ № 44. 6. **Ситуационная задача «Уведомление о коррупции»** *Задание.* Вы обнаружили, что ваш коллега получает вознаграждение от поставщика антивирусов. Составьте: ○ служебную записку на имя руководителя (с описанием фактов); ○ образец заявления в прокуратуру (по форме ФЗ № 273). *Формат:* 2 документа в деловом стиле (по 1 странице каждый). *Критерии оценки:* ○ соблюдение процессуальных требований; ○ чёткость формулировок; ○ указание на правовые основания (ст. 9 ФЗ № 273).

Критерии оценивания самостоятельной работы:

Оценка	Критерии оценивания
отлично	выставляется если работа носит научно-исследовательский характер, проанализирован и сделан сравнительный анализ нескольких литературных источников, приведены примеры
хорошо	выставляется если проанализирован и сделан сравнительный анализ нескольких литературных источников, приведены примеры
удовлетворительно	выставляется если проведен сравнительный анализ научно-методической литературы, приведены примеры
неудовлетворительно	выставляется если работа прошла проверку на антиплагиат и соответствует требованиям оформления

5. МАТЕРИАЛЫ ДЛЯ ДИАГНОСТИЧЕСКОЙ РАБОТЫ

Задания для диагностической работы должны обеспечивать оценку полностью или частично сформированных компетенций. Каждое задание должно быть привязано к тому или иному индикатору сформированности компетенций.

При формировании заданий для диагностической работы необходимо использовать тестовые задания следующих типов:

Тип задания 1. Задания закрытого типа на установление соответствия.

Тип задания 2. Задания закрытого типа на установление последовательности.

Тип задания 3. Задания комбинированного типа, предполагающие выбор одного правильного ответа из предложенных.

Тип задания 4. Задания комбинированного типа, предполагающие выбор нескольких ответов из предложенных.

Тип задания 5. Задания открытого типа с развернутым ответом.

Все типы заданий должны быть представлены не менее одного раза.

<table>
<tr><th rowspan="2">№ п/п</th><th rowspan="2">Тема занятия</th><th rowspan="2">Код компетенции</th><th rowspan="2">Индикатор</th><th rowspan="2">Тип задания</th><th colspan="2">Задание</th><th rowspan="2">Уровень освоения компетенции</th></tr>
<tr><th>Вариант 1</th><th>Вариант 2</th></tr>
<tr><td>1</td><td>Тема 1. Борьба с угрозами несанкционированного доступа к информации</td><td>УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционном</td><td>ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td><td>1</td><td>Задания закрытого типа на установление соответствия
1. Установите соответствие между видами угроз информационной безопасности и их характеристиками.<table><tr><td>Вид угрозы</td><td>Характеристика</td></tr></table></td><td>1. Установите соответствие между принципами защиты информации и их сутью.<table><tr><td>Принцип</td><td>Суть принципа</td></tr><tr><td>1. Конфиденциальн</td><td>А. Обеспечение возможности</td></tr></table></td><td>Базовый (1-3 минуты)</td></tr>
</table>

		у поведению и противодействовать им в профессиональной деятельности			1. Физическая угроза — А. Несанкционированный доступ к данным через уязвимости в ПО 2. Программная угроза — Б. Повреждение оборудования в результате стихийных бедствий 3. Организационная угроза — В. Ошибки персонала при работе с информацией 4. Правовая угроза — Г. Отсутствие необходимых нормативных документов по защите информации **Правильный ответ:** 1 – Б, 2 – А, 3 – В, 4 – Г.	ость — получения информации в нужное время 2. Целостность — Б. Защита от несанкционированного изменения данных 3. Доступность — В. Защита от несанкционированного ознакомления с данными **Правильный ответ:** 1 – В, 2 – Б, 3 – А.	
2	Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	2	**Задания закрытого типа на установление последовательности** **2.** Установите правильную последовательность этапов реализации атаки на информационную систему: 1. Эксплуатация уязвимости. 2. Сбор информации о цели. 3. Закрепление в системе. 4. Получение доступа. 5. Планирование атаки. **Правильный ответ:** 5 → 2 → 1 → 4 → 3.	**2.** Расположите в правильной последовательности этапы построения системы защиты информации: 1. Разработка политики безопасности. 2. Анализ рисков. 3. Внедрение защитных механизмов. 4. Определение требований к защите. 5. Мониторинг и аудит. **Правильный ответ:** 2 → 4 → 1 → 3 → 5.	Базовый (1-3 минуты)

3	Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	3	**Задания комбинированного типа (выбор одного ответа)** **3.** Какой метод является наиболее эффективным для защиты от несанкционированного копирования программного обеспечения? А) Использование парольной защиты. Б) Применение электронных ключей (аппаратных донглов). В) Размещение предупреждающей надписи об авторских правах. Г) Ограничение доступа к файлам через права NTFS. **Правильный ответ:** Б) Применение электронных ключей (аппаратных донглов). **Объяснение:** Электронные ключи обеспечивают аппаратную защиту, которую сложно обойти программными методами. В отличие от парольной защиты (легко взламывается), предупреждающих надписей (не имеют технической силы) и прав доступа (могут быть изменены администратором), аппаратные донглы требуют физического наличия устройства для работы ПО, что существенно повышает уровень защиты.	**3.** Какой стандарт является основополагающим для построения системы менеджмента информационной безопасности? А) ISO/IEC 27001. Б) ГОСТ Р 57580.1-2017. В) PCI DSS. Г) NIST SP 800-53. **Правильный ответ:** А) ISO/IEC 27001. **Объяснение:** ISO/IEC 27001 — международный стандарт, определяющий требования к системе менеджмента информационной безопасности (СМИБ). Он универсален, признаётся во всём мире и служит основой для сертификации. ГОСТ Р 57580.1-2017 (Б) специфичен для финансового сектора РФ. PCI DSS (В) касается только обработки платёжных данных. NIST SP 800-53 (Г) применяется преимущественно в госучреждениях США.	Повышенный (3-5 минут)
4	Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	4	**Задания комбинированного типа (выбор нескольких ответов)** **4.** Какие из перечисленных мер относятся к организационным методам защиты информации? Выберите все верные варианты. А) Разработка регламентов работы с конфиденциальными данными. Б) Установка антивирусного ПО. В) Проведение тренингов по ИБ для сотрудников. Г) Использование межсетевых экранов.	**4.** Какие механизмы входят в систему идентификации и аутентификации? Выберите все верные варианты. А) Ввод логина и пароля. Б) Сканирование отпечатков пальцев. В) Проверка MAC-адреса устройства. Г) Анализ поведения пользователя (User Behavior Analytics). Д) Шифрование данных на диске. **Правильные ответы:** А, Б, В, Г. **Объяснение:** • А) Логин/пароль — базовый метод	Повышенный (3-5 минут)

		профессиональной деятельности			Д) Назначение ответственных за ИБ в подразделениях. **Правильные ответы:** А, В, Д. **Объяснение:** • А) Регламенты — ключевой организационный документ, нормирующий процессы. • В) Тренинги повышают осведомлённость персонала — важная часть организационной защиты. • Д) Распределение ответственности — основа организационной структуры ИБ. Б) и Г) относятся к техническим мерам, так как предполагают использование ПО/оборудования.	аутентификации. • Б) Биометрия (отпечатки) — современный метод аутентификации. • В) MAC-адрес может использоваться для идентификации устройства. • Г) Анализ поведения дополняет аутентификацию (например, обнаружение аномалий). Д) Шифрование — метод защиты данных, но не относится напрямую к идентификации/аутентификации.	
5	Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	5	**Задания открытого типа с развёрнутым ответом** **5.** Опишите три ключевых принципа информационной безопасности (триада CIA) и приведите примеры их реализации в корпоративной среде. **Ответ:** 1. **Конфиденциальность** — защита информации от несанкционированного доступа. *Пример:* шифрование данных при передаче по сети, разграничение прав доступа к файлам, использование двухфакторной аутентификации для входа в систему. 2. **Целостность** — гарантия неизменности данных. *Пример:* применение хэш-сумм для проверки целостности файлов, ведение журналов изменений (audit trails), резервное копирование с контролем версий. 3. **Доступность** — обеспечение работоспособности систем и данных. *Пример:* резервирование серверов,	**5.** Объясните, почему комплексный подход к защите информации (сочетание законодательных, организационных, технических и других мер) эффективнее, чем использование только одного типа защиты. Приведите конкретные примеры. **Ответ:** Комплексный подход обеспечивает **многоуровневую защиту** («принцип эшелонирования»), где слабость одного слоя компенсируется надёжностью других. **Причины эффективности:** 1. **Перекрытие всех векторов атак** Один тип защиты не закрывает все угрозы. *Пример:* • Технические средства (файрволы) не предотвратят утечку данных через сотрудника. • Организационные меры (инструкции) бесполезны против вирусной атаки без антивируса. 2. **Снижение зависимости от человеческого фактора** Даже при ошибке сотрудника	Высокий (5-10 минут)

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>использование систем бесперебойного питания (ИБП), организация георазпределённых дата-центров для отказоустойчивости.</td>
<td>технические средства могут блокировать угрозу. Пример: DLP-система не позволит отправить конфиденциальный файл по email, даже если сотрудник случайно прикрепил его.
3. Соответствие нормативным требованиям
Законодательные меры (ФЗ-152, GDPR) обязывают использовать комбинацию методов. Пример: для защиты персональных данных требуется:
• юридическое оформление согласия (законодательная мера);
• разграничение доступа (организационная);
• шифрование (техническая).
4. Экономическая целесообразность
Распределение бюджета между мерами даёт лучший ROI. Пример: затраты на обучение персонала (организационная мера) снижают риски фишинга, сокращая расходы на ликвидацию последствий атак.
5. Адаптивность к новым угрозам
Комплекс мер позволяет оперативно реагировать на изменения. Пример: при появлении нового вируса технические средства (антивирус) блокируют его, а организационные (временный запрет USB-носителей) минимизируют распространение.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Тема 2. Борьба с вирусным заражением информации</td>
<td>УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционном</td>
<td>ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.</td>
<td>1</td>
<td>Задания закрытого типа на установление соответствия
6. Установите соответствие между типом антивирусной программы и её функцией.
<table><tr><td>Тип программы</td><td>Функция</td></tr><tr><td>1. Програм</td><td>А. Отслеживают</td></tr></table></td>
<td>6. Соотнесите вид вредоносного ПО с его характеристикой.
<table><tr><td>Вид ПО</td><td>Характеристика</td></tr><tr><td>1. Компьютерный вирус</td><td>А. Собирает и передаёт конфиденциальные данные без ведома</td></tr></table></td>
<td>Базовый (1-3 минуты)</td>
</tr>
</table>

		у поведению и противодействовать им в профессиональной деятельности			мы-детекторы — изменения в файлах и системных областях 2. Программы-доктора — Б. Блокируют подозрительные действия в реальном времени 3. Программы-ревизоры — В. Ищут известные вирусы по сигнатурам 4. Программы-фильтры — Г. Лечат заражённые файлы, удаляя вирус **Правильный ответ:** 1 – В; 2 – Г; 3 – А; 4 – Б.	пользователя 2. Программа-шпион — Б. Самовоспроизводится и внедряется в другие программы 3. Программа-сканер — В. Ищет уязвимости в системе для последующего использования **Правильный ответ:** 1 – Б; 2 – А; 3 – В.	
7	Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	2	**Задания закрытого типа на установление последовательности** **7.** Расположите этапы распространения компьютерного вируса в правильной последовательности: А. Активизация вируса при запуске заражённого файла. Б. Поиск новых объектов для заражения. В. Внедрение вируса в систему. Г. Репликация (копирование) вируса. Д. Выполнение деструктивных действий. **Правильный ответ:** В → А → Г → Б → Д.	**7.** Определите верную последовательность этапов профилактики вирусного заражения: А. Регулярное обновление антивирусного ПО. Б. Обучение пользователей основам ИБ. В. Настройка брандмауэра и фильтров. Г. Создание резервных копий данных. Д. Контроль внешних носителей и электронной почты. **Правильный ответ:** Б → В → А → Д → Г.	Базовый (1-3 минуты)
8	Тема 2. Борьба с вирусным заражением	УК-10. Способен формировать	ИУК-10.1 Знает способы профилактики	3	**Задания комбинированного типа (выбор одного ответа)** **8.** Какой тип антивирусной программы	**8.** Какой метод профилактики вирусного заражения является первоочередным для организации?	Повышенный (3-5

	информации	нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	коррупции и формирования нетерпимого отношения к ней.		наиболее эффективен для обнаружения новых, неизвестных вирусов? А. Программы-детекторы. Б. Программы-ревизоры. В. Программы-фильтры. Г. Программы-доктора. **Правильный ответ:** Б – программы-ревизоры. **Объяснение:** программы-ревизоры отслеживают изменения в файлах и системных областях, сравнивая их с эталонными значениями. Это позволяет обнаруживать новые вирусы, даже если их сигнатуры ещё не известны, поскольку любое несанкционированное изменение может указывать на заражение.	А. Установка антивирусного ПО на все компьютеры. Б. Регулярное резервное копирование данных. В. Обучение сотрудников основам информационной безопасности. Г. Ограничение прав доступа пользователей. **Правильный ответ:** В – обучение сотрудников основам информационной безопасности. **Объяснение:** человеческий фактор – один из главных источников угроз. Обучение сотрудников позволяет снизить риск заражения через фишинг, подозрительные вложения и ненадёжные ссылки. Без осознанного отношения персонала к ИБ технические меры могут оказаться недостаточно эффективными	минут)
9	Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	4	**Задания комбинированного типа (выбор нескольких ответов)** **9.** Выберите все эффективные меры профилактики вирусного заражения: А. Регулярное обновление ОС и ПО. Б. Использование нелицензионного антивирусного ПО. В. Ограничение доступа к подозрительным веб-сайтам. Г. Открытие вложений из писем от неизвестных отправителей. Д. Резервное копирование важных данных. **Правильные ответы:** А, В, Д. **Объяснение:** • **А** – обновления закрывают уязвимости, которые могут использовать вирусы. • **В** – ограничение доступа к подозрительным ресурсам снижает риск загрузки вредоносного кода. • **Д** – резервные копии позволяют восстановить данные после атаки.	**9.** Какие действия вируса относятся к деструктивным? Выберите все верные варианты. А. Шифрование файлов пользователя без его согласия. Б. Сбор информации о посещённых веб-сайтах. В. Удаление системных файлов. Г. Медленная работа компьютера из-за фоновых процессов. Д. Блокировка доступа к важным данным. **Правильные ответы:** А, В, Д. **Объяснение:** • **А** – шифрование без согласия пользователя (например, ransomware) лишает доступа к данным. • **В** – удаление системных файлов нарушает работу ОС. • **Д** – блокировка данных препятствует их использованию. Ответ **Б** относится к шпионской	Повышенный (3-5 минут)

					Ответы **Б** и **Г** увеличивают риски: нелицензионное ПО может содержать вирусы, а подозрительные вложения – основной канал заражения.	деятельности, а **Г** – к косвенным последствиям, но не является прямым деструктивным действием.	
10	Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	5	**Задания открытого типа с развёрнутым ответом** **10.** Опишите структуру современного компьютерного вируса и объясните, как каждый компонент способствует его функционированию. **Ответ:** Современный компьютерный вирус обычно состоит из следующих компонентов: 1. **Механизм заражения (инъекции)** – обеспечивает внедрение вируса в систему (например, через уязвимости или социальную инженерию). 2. **Код репликации** – отвечает за копирование вируса в другие файлы или системы. 3. **Триггер (условие активации)** – определяет, когда вирус начнёт выполнять деструктивные действия (например, при определённой дате или действии пользователя). 4. **Полезная нагрузка (payload)** – выполняет вредоносные действия: удаление данных, шифрование, сбор информации и т. п. 5. **Механизм скрытности** – позволяет вирусу избегать обнаружения (например, маскировка под легитимное ПО или шифрование кода). Каждый компонент усиливает эффективность вируса: механизм заражения обеспечивает распространение, репликация – масштабирование угрозы, триггер – неожиданность атаки.	**10.** Опишите комплексный план действий организации по предотвращению вирусных заражений и реагированию на инциденты. Укажите не менее пяти ключевых мер профилактики и не менее трёх этапов реагирования. Обоснуйте, почему каждая мера важна. **Ответ:** **Меры профилактики:** 1. **Регулярное обновление ПО и ОС** Обоснование: закрывает уязвимости, которые могут быть использованы вирусами для проникновения. Автоматические обновления снижают риск эксплуатации известных брешей. 2. **Использование многоуровневой антивирусной защиты** Обоснование: сочетание антивирусов-детекторов, мониторов и файерволов обеспечивает обнаружение на разных стадиях — от загрузки файла до сетевых атак. 3. **Обучение персонала основам кибергигиены** Обоснование: фишинг и социальная инженерия — главные каналы заражения. Обучение снижает риск открытия подозрительных вложений и перехода по вредоносным ссылкам. 4. **Ограничение прав пользователей** Обоснование: минимизация административных прав препятствует запуску вредоносного кода с привилегиями системы. Пользователи работают в режиме «только	Высокий (5-10 минут)

						необходимое». 5. **Резервное копирование данных** Обоснование: позволяет восстановить информацию после атаки (например, ransomware). Резервы должны храниться оффлайн или в защищённом облаке, чтобы избежать их шифрования. **Этапы реагирования на инцидент:** 1. **Изоляция заражённой системы** Действия: отключение от сети, блокировка учётных записей, перевод в карантин. Обоснование: предотвращает распространение вируса на другие узлы сети и утечку данных. 2. **Анализ и идентификация угрозы** Действия: сбор логов, анализ подозрительных процессов, определение типа вируса (с помощью песочниц и антивирусных лабораторий). Обоснование: точная диагностика позволяет выбрать эффективные методы лечения и предотвратить повторные атаки. 3. **Ликвидация и восстановление** Действия: удаление вируса (с использованием специализированных утилит), восстановление системы из резервных копий, смена паролей. Обоснование: гарантирует полное устранение угрозы и возврат к штатной работе. Проверка целостности данных исключает скрытые бэкдоры. **Дополнительно:** после инцидента важно провести разбор причин (post-mortem analysis) и обновить политики безопасности, чтобы минимизировать риски в будущем.	
11	Тема 3.	УК-10.	ИУК-10.1 Знает	1	**Задания закрытого типа на**	**11.** Соотнесите виды информации с	Базовы

	Организационно-правовое обеспечение информационной безопасности	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	способы профилактики коррупции и формирования нетерпимого отношения к ней.		**установление соответствия** **11.** Установите соответствие между правовыми документами и их уровнем регулирования. А) Федеральный закон «Об информации, информационных технологиях и о защите информации» Б) Конвенция о киберпреступности (Будапештская конвенция) В) Приказ ФСТЭК России № 21 Г) Локальные акты организации по защите информации 1. Международный уровень 2. Федеральный уровень 3. Ведомственный уровень 4. Корпоративный уровень **Правильный ответ:** А – 2; Б – 1; В – 3; Г – 4.	режимами её защиты. А) Персональные данные Б) Государственная тайна В) Коммерческая тайна Г) Служебная информация ограниченного доступа 1. Режим государственной тайны 2. Режим конфиденциальной информации 3. Режим персональных данных 4. Режим служебной тайны **Правильный ответ:** А – 3; Б – 1; В – 2; Г – 4.	й (1-3 минуты)
12	Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	2	**Задания закрытого типа на установление последовательности** **12.** Установите правильную последовательность этапов разработки нормативно-правовой базы в сфере ИБ в РФ. 1. Принятие федеральных законов 2. Разработка ведомственных приказов и инструкций 3. Утверждение Концепции правового обеспечения ИБ РФ 4. Принятие международных обязательств (ратификация конвенций) **Правильный ответ:** 4 → 3 → 1 → 2.	**12.** Определите последовательность действий при расследовании инцидента информационной безопасности. 1. Фиксация доказательств 2. Установление факта нарушения 3. Уведомление правоохранительных органов (при необходимости) 4. Анализ причин и последствий **Правильный ответ:** 2 → 1 → 4 → 3.	Базовый (1-3 минуты)
13	Тема 3. Организационно-правовое обеспечение информационной	УК-10. Способен формировать нетерпимое отношение к	ИУК-10.1 Знает способы профилактики коррупции и формирования	3	**Задания комбинированного типа (выбор одного ответа)** **13.** Какой документ определяет основные направления государственной политики в области информационной безопасности	**13.** Какой международный документ впервые закрепил правовые нормы борьбы с киберпреступностью? А) Конвенция о защите физических лиц при автоматизированной обработке	Повышенный (3-5 минут)

	безопасности	проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	нетерпимого отношения к ней.		РФ? А) Доктрина информационной безопасности РФ Б) Федеральный закон «О безопасности» В) Конституция РФ Г) Указ Президента о стратегии развития ИКТ **Правильный ответ:** А) Доктрина информационной безопасности РФ. **Объяснение:** Доктрина информационной безопасности РФ (утверждена Указом Президента РФ) является ключевым документом, определяющим стратегические цели, задачи и направления государственной политики в сфере ИБ. Она служит основой для разработки законодательных и нормативных актов, а также межведомственного взаимодействия.	персональных данных (Совет Европы, 1981 г.) Б) Будапештская конвенция о киберпреступности (2001 г.) В) Резолюция ООН о международной информационной безопасности Г) Договор о сотрудничестве в области ИБ между странами СНГ **Правильный ответ:** Б) Будапештская конвенция о киберпреступности (2001 г.). **Объяснение:** Будапештская конвенция (Конвенция о преступности в сфере компьютерной информации) — первый международный договор, систематизировавший составы киберпреступлений, механизмы расследования и международное сотрудничество в этой сфере. Она стала основой для национального законодательства многих стран.	
14	Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	4	**Задания комбинированного типа (выбор нескольких ответов)** **14.** Какие международные документы регулируют защиту информации? (Выберите 3 варианта.) А) Будапештская конвенция о киберпреступности Б) Всеобщая декларация прав человека В) Конвенция о защите физических лиц при обработке ПДн (Совет Европы) Г) Женевские конвенции Д) Резолюции ООН по международной информационной безопасности **Правильные ответы:** А, В, Д. **Объяснение:** • **А** — регулирует борьбу с киберпреступностью. • **В** — устанавливает стандарты защиты персональных данных.	**14.** Какие нормативные акты РФ содержат положения о защите государственной тайны? (Выберите 3 варианта.) А) Закон РФ «О государственной тайне» Б) Указ Президента о перечне сведений, отнесённых к гостайне В) Федеральный закон «О коммерческой тайне» Г) Постановление Правительства о порядке допуска к гостайне Д) Трудовой кодекс РФ **Правильные ответы:** А, Б, Г. **Объяснение:** • **А** — базовый закон, определяющий понятие, режимы и порядок защиты гостайны. • **Б** — устанавливает конкретный перечень сведений, составляющих гостайну.	Повышенный (3-5 минут)

					• **Д** — закрепляет принципы международного сотрудничества в сфере ИБ. *Варианты Б и Г не относятся напрямую к регулированию ИБ.*	• **Г** — регламентирует процедуры допуска лиц к гостайне. *Варианты В и Д не регулируют защиту гостайны (В — о коммерческой тайне, Д — общие трудовые нормы).*	
15	Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.1 Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.	5	**Задания открытого типа с развёрнутым ответом** **15.** Опишите основные элементы Концепции правового обеспечения информационной безопасности РФ. Приведите примеры нормативных актов, реализующих каждый элемент. **Примерный ответ:** Концепция правового обеспечения ИБ РФ включает: **Нормативно-правовую базу** (ФЗ «Об информации…», ФЗ «О персональных данных», Доктрина ИБ). **Механизмы регулирования** (лицензирование, сертификация, контроль за соблюдением требований). **Международное сотрудничество** (ратификация Будапештской конвенции, участие в ООН-группах по ИБ). **Ответственность за нарушения** (ст. 272–274.1 УК РФ, административные штрафы). **Просветительские меры** (обучение специалистов, информирование граждан о рисках). **Примеры актов:** • ФЗ № 149-ФЗ — базовые принципы ИБ. • Указ Президента РФ от 05.12.2016 № 646 (Доктрина информационной безопасности РФ) — стратегические цели и задачи; • Постановление Правительства от	**15.** Проанализируйте, как законодательство РФ противодействует коррупционным рискам в сфере закупок ИТ-решений для государственных нужд. Укажите конкретные правовые механизмы и нормативные акты. **Примерный ответ:** Законодательство РФ использует комплекс правовых механизмов для профилактики коррупции в ИТ-закупках: **Обязательная прозрачность процедур** (Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе…»): ○ публикация извещений и документации в ЕИС (Единая информационная система); ○ открытые аукционы и конкурсы; ○ обязательное общественное обсуждение крупных закупок. **Антикоррупционные ограничения** (ст. 31 № 4 Newton-ФЗ): ○ запрет на участие лиц с конфликтом интересов; ○ проверка наличия судимости за экономические преступления; ○ требование отсутствия в реестре недобросовестных поставщиков. **Контроль и аудит** (ст. 99 № 44-ФЗ): ○ мониторинг со стороны ФАС, казначейства, прокуратуры; ○ обязательные отчёты о исполнении контрактов; ○ внеплановые проверки при сигналах о	Высокий (5-10 минут)

					01.11.2012 № 1119 — требования к защите персональных данных при их обработке; • Приказы ФСТЭК, ФСБ, Минцифры — ведомственные регламенты по технической и организационной защите информации.	нарушениях. **Ответственность за нарушения** (УК РФ, КоАП РФ): o ст. 200.4 УК РФ — злоупотребления в сфере закупок; o административные штрафы за нарушение процедур (гл. 7 КоАП РФ); o дисквалификация должностных лиц. **Стандартизация требований** (приказы Минцифры, ГОСТы): o типовые технические задания; o единые критерии оценки предложений; обязательная экспертиза ИТ-решений.	
16	Тема 1. Борьба с угрозами несанкционированного доступа к информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	Решение задач	16. Вы работаете специалистом по информационной безопасности в государственном учреждении. Вам поступает предложение от представителя коммерческой компании: за денежное вознаграждение вы должны «закрыть глаза» на выявленные в ходе аудита уязвимости в системе защиты информации, чтобы компания получила выгодный контракт. Задание: 1. Опишите, какие коррупционные риски возникают в данной ситуации. 2. Перечислите действия, которые вы обязаны предпринять согласно антикоррупционному законодательству и внутренним регламентам. 3. Укажите, к каким последствиям для вас и организации может привести согласие на предложение. Решение: 1. Коррупционный риск — конфликт интересов, подкуп должностного лица, нарушение принципов информационной	16. Вам как сотруднику отдела информационной безопасности поручено выбрать поставщика средств защиты информации. Один из кандидатов — фирма, где работает ваш близкий родственник. Задание: 1. Определите, есть ли в этой ситуации конфликт интересов. 2. Какие меры вы должны предпринять, чтобы исключить коррупционные риски? 3. Как оформить уведомление о конфликте интересов? Решение: 1. Да, ситуация создаёт потенциальный конфликт интересов: личная связь может повлиять на объективность выбора. 2. Необходимо: o заявить о конфликте интересов руководству; o воздержаться от участия в принятии решения по выбору поставщика; o передать полномочия другому сотруднику;	Высокий (5-10 минут)

					безопасности ради личной выгоды. 2. Необходимо: o отказаться от предложения; o уведомить руководство и службу безопасности организации; o зафиксировать факт предложения (переписку, аудио-, видеоматериалы, если возможно); o подать уведомление в антикоррупционную комиссию или правоохранительные органы. 3. Последствия: o уголовная ответственность (ст. 290 УК РФ — получение взятки); o утрата доверия, увольнение, дисквалификация; o компрометация системы защиты информации, утечка данных, репутационные и финансовые потери организации	o обеспечить прозрачность процедуры отбора (публичные критерии, конкурсный отбор). 3. Уведомление оформляется в письменной форме с указанием: o сути конфликта (родственная связь); o должности и ФИО родственника; o мер, предложенных для устранения конфликта; o даты и подписи.	
17	Тема 2. Борьба с вирусным заражением информации	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	Решение задач	17. Условие Вы — системный администратор компании. Вам поступило электронное письмо от неизвестного отправителя с вложением «Акт_проверки_СИБ.doc.exe». В тексте письма указано, что это срочный документ от регулятора, требующий немедленного ознакомления. Перечислите не менее 5 признаков, указывающих на потенциальную угрозу, и опишите последовательность ваших действий для предотвращения заражения. Решение Признаки угрозы: 1. Расширение файла .exe (исполняемый файл) при заявленном формате документа .doc. 2. Неизвестный отправитель.	17. Условие Ваш коллега просит передать ему через флеш накопитель «важный файл», но предупреждает, что антивирус на его компьютере «часто ругается на этот файл». Он утверждает, что это «ложное срабатывание». Объясните, почему нельзя выполнять эту просьбу, и предложите альтернативный безопасный способ передачи данных. Решение Причины отказа: • Антивирус реагирует на потенциально вредоносный код. • Передача файла может заразить вашу систему и корпоративную сеть. • Действие коллеги нарушает политику ИБ компании.	Высокий (5-10 минут)

					3. Фраза «срочный документ от регулятора» как метод психологического давления. 4. Отсутствие официальной подписи или контактов регулятора. 5. Подозрительное имя файла (смешение форматов). Действия: 1. Не открывать вложение. 2. Проверить адрес отправителя на подозрительные домены. 3. Сообщить в службу ИБ компании о письме. 4. Заблокировать отправителя в почтовой системе. 5. Провести сканирование рабочей станции антивирусом.	Альтернативный способ: 1. Попросить коллегу загрузить файл в корпоративный облачный диск с антивирусной проверкой. 2. Если файл критически важен — обратиться в службу ИБ для анализа файла в изолированной среде. 3. Использовать зашифрованный канал передачи (например, S/MIME для почты).	
18	Тема 3. Организационно-правовое обеспечение информационной безопасности	УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям	Решение задач	18. Вы — специалист по информационной безопасности в госучреждении. Вам предлагают «ускорить» согласование технического решения по защите данных за денежное вознаграждение. Задача: 1. Определите, какие нормы законодательства РФ запрещают подобные действия. 2. Составьте краткий (5–7 предложений) письменный отказ, ссылаясь на конкретные статьи законов. 3. Укажите, в какой орган следует сообщить о попытке склонения к коррупции. Решение: 1. Действия запрещены: o ст. 9 Федерального закона от 25.12.2008 № 273 ФЗ «О противодействии коррупции» (запрет на принятие вознаграждений);	18. Вам как ИТ специалисту поручено выбрать поставщика ПО для защиты информации. Один из кандидатов намекает, что «личное вознаграждение» повысит шансы его компании. Задача: 1. Перечислите шаги, которые вы предпримете для предотвращения конфликта интересов. 2. Укажите, какие документы нужно оформить, чтобы зафиксировать попытку склонения к коррупции. 3. Назовите сроки подачи уведомления о конфликте интересов. Решение: 1. Шаги: o отказаться от переговоров с намекающим представителем; o уведомить руководство и комиссию по этике; o провести закупку через конкурентные	Высокий (5-10 минут)

					o ст. 290 УК РФ (получение взятки). 2. Пример отказа: «В соответствии со ст. 9 ФЗ № 273 ФЗ я не вправе принимать денежные вознаграждения за выполнение должностных обязанностей. Предложение о выплате вознаграждения расценивается как попытка склонения к коррупционному правонарушению. Прошу прекратить подобные обсуждения. В случае повторения я буду вынужден уведомить компетентные органы». 3. Сообщить в подразделение по профилактике коррупционных правонарушений госоргана или в прокуратуру (ст. 11 ФЗ № 273 ФЗ).	процедуры (44 ФЗ или 223 ФЗ). 2. Документы: o служебная записка на имя руководителя с описанием ситуации; o акт о факте склонения к коррупции (с свидетелями, если возможно). 3. Срок уведомления — не позднее следующего рабочего дня (п. 1 ч. 2 ст. 11 ФЗ № 273 ФЗ).	

Критерии оценивания диагностической работы:

Оценка	Критерии оценивания
отлично	от 90 до 100 % правильно выполненных заданий
хорошо	от 70 до 89 % правильно выполненных заданий
удовлетворительно	от 50 до 69 % правильно выполненных заданий
неудовлетворительно	менее 50 % правильно выполненных заданий