Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 23.09.2026 19:10:45
Уникальный программный ключ:
637517d24e103c3db032acf37e839d98ec1c5bb2f5eb89c29abfcd7f63985447

Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

МЕЖДУНАРОДНЫЙ ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БИЗНЕС-ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор Международного института информационных технологий и бизнес-информатики
_____ Т.В. Новикова
«17» декабря 2025г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
09.03.03 Прикладная информатика
(уровень бакалавриат)

Направленность (профиль):
«Анализ данных»

Форма обучения: **очная, заочная**

Москва

Фонд оценочных средств для дисциплины «Информационная безопасность». Направление подготовки/специальность 09.03.03 Прикладная информатика, направленность (профиль/специализация): «Анализ Данных» / О.А. Левичев – М.: ИМПЭ им. А.С. Грибоедова.

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины.

Разработчик: О.А. Левичев

Заведующий кафедрой: _____/ Н. Н. Загускин

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

Настоящий Фонд оценочных средств (ФОС) по дисциплине «Информационная безопасность» является неотъемлемым приложением к рабочей программе дисциплины (РПД) «Информационная безопасность». 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	Прикладной информатики и информационных технологий
Наименование дисциплины	Информационная безопасность
Факультет / институт	Институт международной экономики, лидерства и менеджмента
Направление подготовки / специальность	09.03.03 Прикладная информатика
Количество вопросов в оценочных заданиях (диапазон)	11-22
Общее время тестирования (мин)	90 мин
Общее количество вопросов/заданий в ФОС	22
Размещенность на сайте Университета примерного перечня вопросов, заданий ФОС – для подготовки обучающихся к прохождению оценки (да / нет)	Да

3.1. Модели контролируемых 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.** Знать природу экстремизма, терроризма, коррупционного поведения как социально- правового явления. Понимать общественную опасность экстремизма, терроризма, коррупционного поведения во всех их проявлениях, последствия и необходимость противодействия им **ИУК-10.2.** Уметь реализовывать средства обеспечения законности и правопорядка в сфере противодействия экстремизма, терроризма, коррупционному поведению
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне

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. 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.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
Тема 1 Введение в информационную безопасность	**УК-10** Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	**И У К - 1 0 . 1 .** Знать природу экстремизма, терроризма, коррупционного поведения как социально-правового явления. Понимать общественную опасность экстремизма, терроризма,	**Задание 1.1** Какие из перечисленных мер напрямую способствуют обеспечению конфиденциальности информации в автоматизированной информационной системе (АИС)? Варианты ответов: а) Шифрование данных на сервере. б) Регулярное создание резервных копий. в) Внедрение системы разграничения доступа (RBAC). г) Установка системы бесперебойного питания (ИБП). Ответ: а, в. Пояснение: ответ "а" (Шифрование данных) делает информацию недоступной для прочтения лицам, не обладающим ключом дешифрования, что является прямой мерой обеспечения конфиденциальности. Ответ "в" (Система разграничения доступа (RBAC)) гарантирует, что доступ к информации будут иметь только авторизованные пользователи,

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	коррупционного поведения во всех их проявлениях, последствия и необходимость противодействия им ИОПК-3.1. Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникаци	что также обеспечивает конфиденциальность. **Задание 1.2** Какие из следующих утверждений точно характеризуют угрозы целостности информации? Варианты ответов: а) Умышленное внесение некорректных данных в систему. б) Случайное удаление файла пользователем. в) Перехват трафика с целью его прослушивания. г) Проведение атаки типа "Отказ в обслуживании" (DDoS). Ответ: а, б. Пояснение: ответы "а" (Внесение некорректных данных) и "б" (Случайное удаление файла) — это действия, которые нарушают точность и полноту информации, то есть ее целостность. **Задание 1.3** Установите правильную последовательность этапов при первоначальном построении системы защиты информации на предприятии. Этапы: 1. Разработка и внедрение организационных и технических мер защиты. 2. Идентификация и оценка всех информационных активов. 3. Разработка политики информационной безопасности. 4. Выявление угроз и уязвимостей для активов, оценка рисков. Ответ: 2431 Пояснение: Логика построения системы защиты следует классическому циклу управления рисками: сначала нужно понять, что защищать (2 - идентификация активов), затем понять, от чего защищать (4 - анализ угроз и рисков). На основе этого формируются общие

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
		онных технологий и с учётом основных требований информационной безопасности на базовом уровне	правила и подходы (3 - политика ИБ), и только потом выбираются и внедряются конкретные меры и инструменты (1). **Задание 1.4** Расположите основные составляющие информационной безопасности (триада CIA) в порядке приоритета для системы онлайн-банкинга с точки зрения рядового клиента. Составляющие ИБ: 1. Доступность 2. Целостность 3. Конфиденциальность Ответ: 231 Пояснение: Для клиента банка первостепенна Целостность (2) — уверенность в том, что сумма перевода не изменилась, а транзакция прошла точно. Затем Конфиденциальность (3) — сохранность его финансовых данных. Доступность (1) важна, но кратковременная недоступность сервиса менее критична, чем ошибка в операции или утечка данных. **Задание 1.5** Установите соответствие между основным принципом построения систем защиты АИС и его содержанием. Список 1 (Принцип): 1. Принцип "простота контроля" 2. Принцип минимальных привилегий 3. Принцип неотвратимости наказания 4. Принцип комплексности защиты Список 2 (Содержание):

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			А. Каждый пользователь должен иметь доступ только к тем ресурсам, которые необходимы для его прямых обязанностей. Б. Защита должна охватывать все компоненты АИС и все этапы информационного процесса. В. Механизмы безопасности должны быть максимально простыми для анализа и тестирования. Г. Любое нарушение политики безопасности должно фиксироваться и влечь за собой адекватные меры ответственности. Ответ: 1В, 2А, 3Г, 4Б **Задание 1.6** Установите соответствие между задачей системы информационной безопасности и мерой по ее реализации. Список 1 (Задача): 1. Защита от несанкционированного доступа (НСД) 2. Обнаружение инцидентов безопасности 3. Обеспечение аутентификации 4. Противодействие вредоносному программному обеспечению Список 2 (Мера): А. Внедрение системы двухфакторной аутентификации. Б. Установка и настройка антивирусного ПО и средств защиты от эксплойтов. В. Развертывание системы обнаружения вторжений (IDS/SIEM). Г. Настройка правил маршрутизации на межсетевом экране и использование механизмов контроля доступа. Ответ: 1Г, 2В, 3А, 4Б

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Что из перечисленного является ПРЯМОЙ задачей системы информационной безопасности? Варианты ответов: а) Повышение производительности вычислительной системы. б) Управление жизненным циклом программного обеспечения. в) Обеспечение своевременного и надежного доступа пользователей к информации. г) Автоматизация бизнес-процессов предприятия. Правильный ответ: в) Пояснение: ответ "в" - Это прямая формулировка задачи по обеспечению доступности — одного из ключевых свойств ИБ. **Задание 1.8** Какое понятие является наиболее точным и полным определением "информационной безопасности"? Варианты ответов: а) Состояние защищенности информации от хищения. б) Защита информации от кибератак. в) Состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие. г) Процесс установки антивируса и межсетевого экрана. Правильный ответ: в) Пояснение: ответ "в" - это наиболее полное и системное определение, охватывающее все аспекты (защищенность, среду, все процессы — формирование, использование, развитие). **Задание 1.9** Как называется принцип построения систем защиты, который предполагает, что для доступа к защищенному ресурсу необходимо одновременное наличие нескольких условий

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			(например, разрешение от двух разных лиц)? Ответ: Принцип разделения секрета / Принцип разделения полномочий Пояснение: Этот принцип является фундаментальным для организации надежного контроля доступа, особенно к критическим операциям. Он предотвращает ситуации, когда одно лицо может единолично совершить неавторизованное или вредоносное действие. **Задание 1.10** Как называется свойство информации, нарушаемое в случае, если злоумышленник смог тайно отправить от чужого имени сообщение, например, фишинговое письмо? Ответ: Аутентичность (или Подлинность). Пояснение: Нарушение аутентичности (часто рассматривается как аспект целостности) означает, что получатель не может быть уверен в истинном источнике информации. В данном случае источник (отправитель письма) был подделан, что является прямой атакой на аутентичность.
Тема 2 Законодательный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографичес	И О П К - 3 . 1 . Знать принципы, методы и средства решения стандартных задач профессиональной деятельности	**Задание 2.1** Какие из перечисленных правовых актов являются в Российской Федерации специальными законами, непосредственно регулирующими отношения в сфере информационной безопасности? Варианты ответов: а) Гражданский кодекс РФ (часть 4). б) Федеральный закон «О персональных данных». в) Федеральный закон «Об информации, информационных технологиях и о защите информации». г) Трудовой кодекс РФ.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	кой культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	Ответ: б, в. Пояснение: ответы "б" (ФЗ «О персональных данных») и "в" (ФЗ «Об информации, информационных технологиях и о защите информации») — это профильные («специальные») законы, целиком посвященные регулированию вопросов обработки информации и ее защиты.
	УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и	**И У К - 1 0 . 1 .** Знать природу экстремизма, терроризма, коррупционного поведения как социально-правового	**Задание 2.2** В соответствии с Федеральным законом «О персональных данных», какие из перечисленных действий оператор обязан совершить до начала обработки персональных данных? Варианты ответов: а) Получить письменное согласие субъекта персональных данных на их обработку (за исключением случаев, предусмотренных законом). б) Уведомить уполномоченный орган (Роскомнадзор) о своем намерении осуществлять

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	противодействовать им в профессиональной деятельности	явления. Понимать общественную опасность экстремизма, терроризма, коррупционного поведения во всех их проявлениях, последствия и необходимость противодействия им	обработку персональных данных. в) Назначить лицо, ответственное за организацию обработки персональных данных. г) Провести классификацию информационной системы персональных данных. Ответ: а, б. Пояснение: ответ "а" (Получение согласия) — это одно из ключевых оснований для правомерной обработки ПДн, прямо предусмотренное законом. Ответ "б" (Уведомление Роскомнадзора) — обязательная процедура для большинства операторов перед началом обработки, за некоторыми исключениями (например, обработка данных сотрудников). **Задание 2.3** Установите логическую последовательность действий компании-оператора при организации легитимной обработки персональных данных сотрудников. Действия: 1. Определить цели и объем обрабатываемых персональных данных. 2. Опубликовать документ, определяющий политику компании в отношении обработки персональных данных (например, Положение). 3. Получить от сотрудника письменное согласие на обработку его персональных данных (если того требует закон). 4. Направить уведомление в Роскомнадзор об обработке персональных данных. Ответ: 1324 Пояснение: Сначала компания должна понять, что и зачем она обрабатывает (1). Затем, на основе этих целей, она получает от субъекта (сотрудника) согласие, если оно необходимо (3). Далее она formalizes свою политику (2), и лишь после этого уведомляет регулятора (4), так как в уведомлении указываются в т.ч. цели обработки и категории данных. **Задание 2.4**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Расположите виды электронных подписей, предусмотренные Федеральным законом «Об электронной подписи», в порядке убывания их юридической значимости (от самой сильной к наименее сильной). Виды подписей: 1. Простая электронная подпись (ПЭП) 2. Неквалифицированная усиленная электронная подпись (НЭП) 3. Квалифицированная усиленная электронная подпись (КЭП) Ответ: 321 Пояснение: КЭП (3) является самой сильной, так как соответствует всем признакам НЭП и дополнительно создана с использованием средств, сертифицированных ФСБ России, и ключ проверки которой содержится в квалифицированном сертификате. НЭП (2) обеспечивает большую защиту, чем простая, так как позволяет определить лицо, подписавшее документ, и факт внесения в него изменений. ПЭП (1) имеет наименьшую юридическую силу, которая должна быть специально оговариваться в соглашении между сторонами. **Задание 2.5** Установите соответствие между российским законом и его ключевым предметом регулирования. Список 1 (Закон): 1. Федеральный закон «Об информации, информационных технологиях и о защите информации» 2. Федеральный закон «О персональных данных» 3. Федеральный закон «Об электронной подписи» 4. Гражданский кодекс РФ (Часть 4) Список 2 (Предмет регулирования):

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			А. Правовые условия использования электронной подписи при совершении юридически значимых действий. Б. Основные принципы и правила обращения с информацией, понятие общедоступной и ограниченного доступа информации. В. Права на результаты интеллектуальной деятельности, в том числе на программы для ЭВМ и базы данных. Г. Порядок обработки специальных, биометрических и иных категорий персональных данных, права субъектов ПДн. Ответ: 1Б, 2Г, 3А, 4В **Задание 2.6** Установите соответствие между понятием и законодательным актом, в котором оно определяется. Список 1 (Понятие): 1. Информация 2. Персональные данные 3. Простая электронная подпись 4. Программа для ЭВМ Список 2 (Закон): А. Федеральный закон «Об электронной подписи» Б. Федеральный закон «Об информации, информационных технологиях и о защите информации» В. Гражданский кодекс РФ Г. Федеральный закон «О персональных данных» Ответ: 1Б, 2Г, 3А, 4В **Задание 2.7**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Какой федеральный закон является базовым (рамочным) в законодательстве РФ, непосредственно регулирующем информационные отношения? Варианты ответов: а) Федеральный закон «О безопасности». б) Федеральный закон «Об информации, информационных технологиях и о защите информации». в) Уголовный кодекс РФ. г) Федеральный закон «О коммерческой тайне». Ответ: б) Пояснение: ответ "б" (ФЗ «Об информации...») закладывает фундаментальные понятия (информация, информационные системы, обладатель информации, доступ к информации), принципы и основы правового режима информации в России, являясь рамочным для других специальных законов. **Задание 2.8** Какое условие является обязательным для того, чтобы простая электронная подпись (ПЭП) была приравнена к собственноручной подписи? Варианты ответов: а) Наличие сертификата ключа проверки электронной подписи, выданного аккредитованным удостоверяющим центром. б) Соблюдение всех признаков усиленной электронной подписи. в) Прямое указание на это в федеральном законе. г) Соглашение между участниками электронного взаимодействия, предусматривающее правило ее использования. Ответ: г)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: ответ "г", юридическая сила простой электронной подписи напрямую зависит от выполнения условий, заранее оговоренных и принятых всеми сторонами в соглашении (договоре, оферте и т.д.). Это прямо следует из ст. 9 ФЗ «Об электронной подписи». **Задание 2.9** Как называется основной федеральный орган исполнительной власти в России, осуществляющий контроль и надзор за соответствием обработки персональных данных требованиям законодательства? Ответ: Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций). Пояснение: Именно Роскомнадзор уполномочен проводить проверки операторов персональных данных, принимать уведомления об их обработке и выносить предписания об устранении нарушений Закона «О персональных данных». **Задание 2.10** Каким термином из Федерального закона «Об информации, информационных технологиях и о защите информации» обозначается лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам? Ответ: Обладатель информации. Пояснение: Это базовое понятие, введенное в ст. 2 указанного закона. Именно обладатель информации устанавливает ее правовой режим (например, общедоступная, ограниченного доступа) и правила обработки
Тема 3 Стандарты и спецификаци	ОПК-3 Способен решать	**И О П К - 3 . 1 .** Знать принципы,	**Задание 3.1** Какие из следующих утверждений точно характеризуют стандарт ГОСТ Р ИСО/МЭК 27001?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
и в области информационной безопасности	стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	Варианты ответов: а) Он содержит подробный каталог мер и средств контроля информационной безопасности. б) Он описывает требования к системе менеджмента информационной безопасности (СМИБ). в) Он предназначен для сертификации продуктов и программного обеспечения на соответствие требованиям безопасности. г) Он построен на основе цикла PDCA (Plan-Do-Check-Act). Ответ: б, г. Пояснение: Ответ "б" - это прямое определение стандарта ГОСТ Р ИСО/МЭК 27001: он задает требования к созданию, внедрению, мониторингу и улучшению СМИБ. Ответ "г" - Цикл PDCA является фундаментальной моделью для непрерывного улучшения СМИБ, что заложено в структуре стандарта. **Задание 3.2** Какие из перечисленных документов относятся к семейству стандартов управленческой информационной безопасности? Варианты ответов: а) ГОСТ Р ИСО/МЭК 15408 «Общие критерии». б) ISO/IEC 27002 «Кодекс практики для средств управления информационной безопасностью». в) Protection Profile (Профиль защиты). г) ГОСТ Р ИСО/МЭК 27001 «Требования к СМИБ». Ответ: б, г.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: Ответ "б", ISO/IEC 27002 — это стандарт-руководство, содержащий лучшие практики по внедрению мер управления ИБ в рамках СМИБ. Ответ "г", ГОСТ Р ИСО/МЭК 27001 — это основной стандарт требований к самой системе менеджмента. **Задание 3.3** Установите последовательность основных этапов цикла PDCA (Деминга) в контексте построения СМИБ согласно ГОСТ Р ИСО/МЭК 27001. Этапы: 1. Act (Воздействие) — предпринимать корректирующие и предупреждающие действия для постоянного улучшения СМИБ. 2. Plan (Планирование) — создавать политики, цели, процессы и меры управления, относящиеся к управлению рисками. 3. Do (Внедрение) — реализовывать процессы и меры управления ИБ. 4. Check (Проверка) — контролировать и анализировать performance процессов ИБ. Ответ: 2,3,4,1 Пояснение: Классический цикл непрерывного улучшения начинается с Планирования (Plan), затем следует Внедрение (Do), далее Проверка (Check) эффективности внедренного, и завершается цикл Воздействием (Act) для корректировки и улучшения. **Задание 3.4** Расположите в логической последовательности этапы работы с «Общими критериями» (ГОСТ Р ИСО/МЭК 15408). Этапы: 1. Выбор компонентов доверия к безопасности (например, уровень тестирования AVA_VAN). 2. Определение целевых показателей безопасности (Security Target) для конкретного

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			продукта. 3. Выбор функциональных компонентов безопасности из каталога стандарта (например, FIA_UAU – аутентификация пользователя). 4. Формулирование целей безопасности для продукта и предположений о среде. Ответ: 4,3,1,2 Пояснение: Сначала определяются общие цели безопасности и предположения (4). На их основе выбираются конкретные функциональные требования (3) и требования доверия (1) из каталогов стандарта. Весь этот комплект требований оформляется в Заявлении о безопасности (Security Target) (2), который является основным документом для оценки. **Задание 3.5** Вопрос: Установите соответствие между стандартом и его основной целью или содержанием. Список 1 (Стандарт/Документ): 1. ГОСТ Р ИСО/МЭК 27001 2. ГОСТ Р ИСО/МЭК 15408 («Общие критерии») 3. Protection Profile (Профиль защиты) 4. ГОСТ Р ИСО/МЭК 17799 / ISO/IEC 27002 Список 2 (Цель/Содержание): А. Независимая оценка и сертификация безопасности ИТ-продукта. Б. Свод лучших практик и рекомендаций по мерам управления ИБ. В. Сертификация системы управления безопасностью информации организации. Г. Независимый от реализации набор требований безопасности для一类 продуктов (напр., межсетевых экранов). Ответ: 1В, 2А, 3Г, 4Б

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 3.6 Установите соответствие между понятием из «Общих критериев» и его определением. Список 1 (Понятие): 1. Функциональные требования безопасности (SFR) 2. Уровень доверия к безопасности (EAL) 3. Цель безопасности (Security Objective) 4. Целевой объект оценки (TOE) Список 2 (Определение): А. Заранее определенный пакет требований доверия, который представляет уровень уверенности в безопасности продукта. Б. ИТ-продукт или система, подлежащие оценке. В. Конкретное требование к поведению продукта, выбранное из каталога стандарта. Г. Краткое заявление о намерении противостоять определенным угрозам. Ответ: 1В, 2А, 3Г, 4Б **Задание 3.7** Какой стандарт из семейства ISO/IEC 2700x является основополагающим для проведения сертификации системы менеджмента информационной безопасности организации? Варианты ответов: а) ISO/IEC 27002 б) ISO/IEC 27005 в) ISO/IEC 27001 г) ISO/IEC 15408 Ответ: в)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: ответ "в", ISO/IEC 27001 — это единственный стандарт в данном списке, который содержит именно требования, по которым аккредитованный орган может провести аудит и выдать сертификат соответствия. **Задание 4.8** Что из перечисленного является преимуществом использования «Общих критериев» (ГОСТ Р ИСО/МЭК 15408)? Варианты ответов: а) Гарантирует полное отсутствие уязвимостей в сертифицированном продукте. б) Позволяет проводить сравнительный анализ безопасности различных продуктов на основе их сертификатов. в) Определяет конкретный перечень технических средств защиты, которые должны быть использованы в продукте. г) Заменяет собой процесс управления рисками в организации. Ответ: б) Пояснение: ответ "б" является верным, потому что одной из ключевых целей «Общих критериев» является создание единой основы для оценки, позволяющей сравнивать результаты оценки безопасности разных продуктов. Уровень EAL и содержание Security Target позволяют это делать. **Задание 4.9** Как называется документ в рамках «Общих критериев», который содержит набор требований безопасности, специфичный для конкретного продукта или системы и является основным документом, предоставляемым для оценки? Ответ: Заявление о безопасности / Security Target (ST).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: Именно Security Target является центральным документом при оценке по «Общим критериям». В нем разработчик (спонсор оценки) формулирует, что именно и как будет оцениваться в целевом объекте оценки (TOE). Задание 4.10 Какой стандарт из семейства ISO/IEC 2700x был изначально основан на британском стандарте BS 7799-1 и представляет собой кодекс практик (свод руководящих принципов) по мерам управления информационной безопасностью? Ответ: ISO/IEC 27002 Пояснение: Историческая преемственность является важным аспектом для понимания эволюции стандартов. ISO/IEC 27002 ведет свою прямую lineage от BS 7799 (часть 1) и содержит детализированные рекомендации по внедрению мер контроля из Приложения А стандарта ISO/IEC 27001.
Тема 4 Административный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникацион	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографич	**Задание 4.1** Какие из перечисленных документов относятся к обязательным элементам Политики информационной безопасности организации верхнего уровня? Варианты ответов: а) Инструкция по настройке межсетевого экрана. б) Положение об обработке персональных данных. в) Регламент резервного копирования. г) Концепция информационной безопасности. Ответ: б, г. Пояснение: ответ "б", положение об обработке персональных данных — это документ уровня политики, устанавливающий основные принципы, цели и правила обработки ПДн в организации. ответ "г", концепция информационной безопасности — это

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	ных технологий и с учетом основных требований информационной безопасности	еской культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	основополагающий документ, определяющий стратегию, принципы и подходы к защите информации в организации. Является ядром политики безопасности. **Задание 4.2** Какие из следующих действий являются ключевыми элементами программы безопасности (Security Program)? Варианты ответов: а) Установка последних обновлений безопасности на серверы. б) Регулярное проведение аудитов и оценок рисков ИБ. в) Назначение ответственных за реализацию политик безопасности. г) Проведение тренингов по повышению осведомленности в области ИБ для сотрудников. Ответ: б, в, г. Пояснение: ответ "б", аудиты и оценка рисков — это управленческие процессы, являющиеся стержнем программы безопасности для контроля ее эффективности и выявления новых угроз. Ответ "в", назначение ответственных — это организационная мера, без которой невозможно выполнение программы (принцип персональной ответственности). Ответ "г", тренинги для сотрудников — это критически важный элемент программы, направленный на управление "человеческим фактором". **Задание 4.3** Установите правильную последовательность этапов разработки и внедрения системы управления информационной безопасностью на административном уровне. Этапы: 1. Принятие и официальное утверждение высшим руководством Политики информационной безопасности. 2. Разработка и реализация конкретных мер контроля, стандартов и процедур. 3. Проведение анализа рисков информационной безопасности.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			4. Создание организационной структуры и распределение ролей и ответственности в области ИБ. Ответ: 3,1,4,2 Пояснение: Классический подход следует логике управления рисками: сначала проводится анализ рисков (3), чтобы понять, от чего защищаться. На его основе формируется верховный документ — Политика (1), которую утверждает руководство. Далее создается организационная структура (4) для реализации политики. И только затем разрабатываются конкретные меры и процедуры (2). **Задание 4.4** Расположите этапы интеграции программы безопасности в жизненный цикл информационной системы (ЖЦ ИС) в хронологическом порядке. Этапы: 1. Формальный ввод системы в эксплуатацию при условии выполнения всех требований безопасности. 2. Разработка архитектуры системы с учетом требований безопасности и анализом угроз. 3. Вывод системы из эксплуатации с обеспечением сохранности и безопасного уничтожения архивных данных. 4. Составление и утверждение технического задания, включающего раздел с требованиями по информационной безопасности. Ответ: 4 → 2 → 1 → 3 Пояснение: Безопасность должна закладываться на ранних стадиях. Сначала требования фиксируются в ТЗ (4). Затем на их основе проектируется безопасная архитектура (2). После реализации и тестирования система вводится в эксплуатацию (1). Завершающий этап ЖЦ — безопасный вывод из эксплуатации (3).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 4.5 Установите соответствие между понятием административного уровня ИБ и его определением. Список 1 (Понятие): 1. Политика безопасности 2. Программа безопасности 3. Мера контроля (Control) 4. Аудит информационной безопасности Список 2 (Определение): А. Непрерывный управленческий процесс, направленный на реализацию политики, управление рисками и достижение целей в области ИБ. Б. Формальная проверка и оценка соответствия системы защиты установленным требованиям и политикам. В. Конкретное правило, процедура или практика, предназначенная для снижения риска. Г. Совокупность формализованных правил и подходов, определяющих цели и основные направления деятельности организации в области ИБ. Ответ: 1Г, 2А, 3В, 4Б **Задание 4.6** Установите соответствие между этапом жизненного цикла системы и административной мерой безопасности, которая должна быть на нем применена. Список 1 (Этап ЖЦ): 1. Проектирование 2. Реализация (кодирование) 3. Эксплуатация 4. Утилизация

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Список 2 (Мера безопасности): А. Проведение регулярного обучения пользователей правилам безопасной работы. Б. Проведение модерирования кода (code review) на предмет наличия уязвимостей. В. Разработка модели угроз и требований к безопасности. Г. Составление регламента уничтожения/очистки носителей информации. Ответ: 1В, 2Б, 3А, 4Г **Задание 4.7** Что из перечисленного является основной целью Политики информационной безопасности верхнего уровня? Варианты ответов: а) Детально описать настройки всех сетевых устройств. б) Продемонстрировать клиентам использование передовых технологий шифрования. в) Формально определить ответственность руководства и общие направления обеспечения ИБ в организации. г) Заложить основы для последующей сертификации по международным стандартам. Ответ: в) Пояснение: ответ "в" - это прямая и первичная цель политики верхнего уровня: закрепить приверженность руководства, распределить ответственность и задать стратегический курс. **Задание 4.8** Какой принцип является наиболее важным для успешной синхронизации программы безопасности с жизненным циклом систем? Варианты ответов: а) Принцип «безопасность как неотъемлемая часть процесса» (Security by Design).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			б) Принцип простоты контроля. в) Принцип минимальных привилегий. г) Принцип разделения обязанностей. Ответ: а) Пояснение: ответ "а", Security by Design — это краеугольный камень интеграции ИБ в ЖЦ. Он означает, что вопросы безопасности рассматриваются не постфактум, а на самых ранних этапах (проектирование, разработка), что значительно эффективнее и дешевле. **Задание 4.9** Как называется основной документ, который формально декларирует приверженность высшего руководства организации целям в области информационной безопасности, устанавливает общие рамки и определяет ответственность? Ответ: Политика информационной безопасности (Information Security Policy). Пояснение: Именно этот документ, утвержденный на уровне топ-менеджмента, является точкой отсчета для всей дальнейшей деятельности в области ИБ. Он задает тон и определяет значимость безопасности для всей организации. **Задание 4.10** На какой стадии жизненного цикла информационной системы мероприятия по безопасности являются наиболее затратными и менее эффективными для исправления фундаментальных недостатков? Ответ: Стадия эксплуатации (или сопровождения). Пояснение: Исправление архитектурных или системных недоработок в области безопасности на стадии эксплуатации требует значительных переделок, остановки работающей системы и сопряжено с наибольшими затратами и рисками. Это

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			подтверждает важность закладки безопасности на ранних стадиях (Projection и Development).
Тема 5 Процедурный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информацион	**Задание 5.1** Какие из перечисленных мер относятся к процедурному уровню обеспечения информационной безопасности? Варианты ответов: а) Настройка правил фильтрации на межсетевом экране. б) Проведение вводного инструктажа по безопасности для нового сотрудника. в) Установка системы видеонаблюдения по периметру здания. г) Разработка регламента резервного копирования. Ответ: б, г. Пояснение: ответ "б", инструктаж сотрудника — это классическая процедурная мера, направленная на управление персоналом. Ответ "г", разработка регламента резервного копирования — это создание формальной процедуры, определяющей порядок действий для обеспечения поддержки работоспособности. **Задание 5.2** Какие действия входят в типовой план реагирования на инциденты информационной безопасности на процедурном уровне? Варианты ответов: а) Немедленное отключение всех серверов для предотвращения распространения угрозы. б) Сбор и сохранение доказательств (логов, дампов памяти). в) Установка последних сигнатур антивирусной программы. г) Уведомление руководителя и службы ИБ о факте инцидента.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
		ной безопасности на базовом уровне	Ответ: б, г. Пояснение: ответ "б", сбор доказательств — это ключевая процедура для последующего анализа инцидента и, возможно, правовых действий. Ответ "г", уведомление ответственных лиц — это первоочередная процедурная action, без которой невозможно запустить процесс реагирования. **Задание 5.3** Установите правильную последовательность этапов управления персоналом в контексте ИБ при увольнении сотрудника. Этапы: 1. Проведение выходного интервью с напоминанием о действующих обязательствах по соблюдению конфиденциальности. 2. Получение заявления об увольнении и уведомление службы ИБ. 3. Немедленное аннулирование всех учетных записей, пропусков и токенов доступа. 4. Инвентаризация и возврат всех информационных активов (ноутбуков, документов, ключей). Ответ: 2,3,4,1 Пояснение: Процедура должна минимизировать период, когда увольняемый сотрудник имеет доступ, но уже мотивирован его использовать в ущерб. Сначала служба ИБ получает уведомление (2), чтобы немедленно аннулировать доступы (3). Затем обеспечивается возврат активов (4), и в завершение проводится финальное интервью (1) для юридического закрепления обязательств. **Задание 5.4** Расположите в логической последовательности ключевые шаги процедуры реагирования на инцидент безопасности.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Шаги: 1. Локализация инцидента и предотвращение его расширения. 2. Подготовка отчета и реализация мер по предотвращению повторения инцидента. 3. Обнаружение и идентификация инцидента. 4. Ликвидация последствий инцидента и восстановление работоспособности. Ответ: 3,1,4,2 Пояснение: Стандартный цикл реагирования начинается с обнаружения (3). После подтверждения инцидента следует его локализация (1), чтобы остановить распространение ущерба. Далее происходит восстановление (4) систем и услуг. Завершает цикл постинцидентный анализ (2), направленный на улучшение системы защиты. **Задание 5.5** Установите соответствие между классом мер процедурного уровня и конкретным примером его реализации. Список 1 (Класс мер): 1. Управление персоналом 2. Физическая защита 3. Поддержка работоспособности 4. Реагирование на нарушения Список 2 (Пример реализации): А. Регламент проведения ежедневного резервного копирования критичных данных. Б. Процедура сопровождения посетителей на территории центра обработки данных. В. Обязательство сотрудника о неразглашении коммерческой тайны (NDA). Г. Чек-лист первоочередных действий при обнаружении заражения вирусом. Ответ: 1В, 2Б, 3А, 4Г

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 5.6 Установите соответствие между элементом плана восстановительных работ и его описанием. Список 1 (Элемент плана): 1. Цель восстановления (RTO - Recovery Time Objective) 2. Приоритетность систем 3. Ответственные лица 4. Точка восстановления (RPO - Recovery Point Objective) Список 2 (Описание): А. Максимально допустимое время простоя системы после инцидента. Б. Распределение ролей и контактной информации команды для выполнения плана. В. Определение порядка восстановления информационных систем и сервисов. Г. Максимально допустимый объем потери данных за период между последней резервной копией и сбоем. Ответ: 1А, 2В, 3Б, 4Г **Задание 5.7** Какой из перечисленных документов является наиболее важным с точки зрения процедурного управления персоналом для нового сотрудника, имеющего доступ к конфиденциальной информации? Варианты ответов: а) Поздравительная открытка от коллектива. б) Ознакомительный тур по офису. в) Подписанное соглашение о конфиденциальности (NDA). г) График работы и перерывов. Ответ: в)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: ответ "в", NDA — это юридически значимая процедурная мера, которая формально закрепляет обязанности сотрудника по защите информации и устанавливает ответственность за их нарушение. Это краеугольный камень управления рисками, связанными с персоналом. **Задание 5.8** Какая из перечисленных мер в наибольшей степени способствует поддержанию работоспособности информационной системы на процедурном уровне? Варианты ответов: а) Ежеквартальная смена паролей учетных записей пользователей. б) Регламентированное ежедневное резервное копирование данных. в) Установка решёток на окна серверной комнаты. г) Проведение ежегодной проверки знаний по ИБ. Ответ: б) Пояснение: ответ "б", регламент резервного копирования — это прямая процедурная мера, предназначенная specifically для обеспечения возможности восстановления работоспособности после сбоя, потери данных или иного инцидента **Задание 5.9** Как называется ключевой количественный показатель плана восстановления, который определяет максимально допустимое время простоя информационной системы или бизнес-процесса после сбоя? Ответ: Цель по времени восстановления Пояснение: RTO — это фундаментальный параметр для планирования восстановительных работ. Он диктует, насколько быстро процедуры восстановления должны быть

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			выполнены, и определяет выбор соответствующих технологий и решений (например, «холодное» или «горячее» резервирование). **Задание 5.10** Какой процедурный документ, подписываемый сотрудником, юридически закрепляет его обязанность не разглашать конфиденциальную информацию компании как во время работы, так и после увольнения? Ответ: Соглашение о конфиденциальности Пояснение: NDA является основной процедурно-правовой мерой управления персоналом в области ИБ. Он создает правовые основания для привлечения сотрудника к ответственности в случае разглашения им информации, что служит сдерживающим фактором и инструментом защиты интересов организации.
Тема 6 Идентификация и аутентификация	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической	**Задание 6.1** Какие из перечисленных мер напрямую повышают стойкость парольной аутентификации к перебору (brute-force)? Варианты ответов: а) Реализация политики блокировки учетной записи после нескольких неудачных попыток входа. б) Обязательное использование букв в разных регистрах, цифр и специальных символов. в) Хранение паролей в открытом виде для упрощения восстановления. г) Использование хеширования паролей с "солью" (salt) на стороне сервера. Правильные ответы: а, б, г. Пояснение: ответ "а" верный, потому что блокировка учетной записи резко снижает скорость и эффективность онлайн-перебора. Ответ "б" верный, так как усложнение пароля увеличивает пространство возможных вариантов, что делает полный перебор

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	и с учетом основных требований информационной безопасности	культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	computationally expensive. Ответ "г" правильный, потому что предотвращает использование предварительно вычисленных радужных таблиц (rainbow tables) для взлома хешей, что критически важно для защиты от офлайн-перебора в случае утечки базы паролей. **Задание 6.2** Установите правильную последовательность этапов процесса аутентификации пользователя в протоколе Kerberos. Этапы: 1. Сервер предоставления услуг (TGS) проверяет TGT и выдает билет на сервис (Service Ticket). 2. Клиент предъявляет TGT серверу предоставления услуг для получения доступа к конкретному сервису. 3. Клиент отправляет запрос на аутентификацию в Центр распределения ключей (KDC). 4. KDC проверяет учетные данные клиента и выдает билет на получение билетов (TGT - Ticket Granting Ticket). Ответ: 3,4,2,1 Пояснение: Классический сценарий Kerberos: клиент сначала аутентифицируется перед KDC (3), получая долгоживущий TGT (4). При необходимости доступа к сервису, клиент использует этот TGT для запроса к TGS (2), который выдает одноразовый билет на сервис (1). **Задание 6.3** Расположите методы аутентификации в порядке увеличения их устойчивости к компрометации учетных данных (от наименее устойчивого к наиболее устойчивому). Методы: 1. Статический пароль, не менявшийся 2 года.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			2. Одноразовый пароль (OTP), доставляемый по SMS. 3. Многофакторная аутентификация (пароль + биометрия). 4. Одноразовый пароль (OTP) на основе времени (TOTP) через мобильное приложение. Ответ: 1,2,4,3 Пояснение: Старый статический пароль — самый слабый метод. OTP по SMS уязвим к атакам на SS7 и перехвату SMS. TOTP через приложение безопаснее, так как не зависит от уязвимостей мобильной сети. Многофакторная аутентификация является самой устойчивой, так как для компрометации требуется взломать несколько независимых факторов. **Задание 6.4** Установите соответствие между понятием в области аутентификации и его определением. Список 1 (Понятие): 1. Идентификация 2. Аутентификация 3. OTP (One-Time Password) 4. FAR (False Acceptance Rate) Список 2 (Определение): А. Процесс проверки подлинности предъявленного идентификатора (подтверждение того, что субъект — это тот, за кого себя выдает). Б. Пароль, действительный для единственной сессии аутентификации или транзакции. В. Статистическая вероятность того, что система биометрической аутентификации incorrectly верифицирует несанкционированного пользователя. Г. Процесс распознавания субъекта системы по его идентификатору (заявление о том, кем субъект является). Ответ: 1Г, 2А, 3Б, 4В

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 6.5 Установите соответствие между компонентом протокола Kerberos и его функцией. Список 1 (Компонент): 1. KDC (Key Distribution Center) 2. TGT (Ticket-Granting Ticket) 3. TGS (Ticket Granting Server) 4. AS (Authentication Server) Список 2 (Функция): А. Выдает TGT после первоначальной аутентификации пользователя. Б. Центральный сервер, состоящий из AS и TGS, хранящий секретные ключи всех субъектов. В. Выдает билеты для доступа к конкретным сетевым сервисам. Г. Шифрованный билет, подтверждающий, что пользователь уже прошел аутентификацию, и используемый для получения билетов на сервисы. Ответ: 1Б, 2Г, 3В, 4А **Задание 6.6** Какой из перечисленных методов аутентификации относится к категории "что-то, что я знаю" (something I know)? Варианты ответов: а) Отпечаток пальца. б) Аппаратный токен (USB-ключ). в) Графический ключ (pattern) на смартфоне. г) Смарт-карта. Ответ: в)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: ответ "в", графический ключ — это секретная последовательность движений, которую пользователь знает и воспроизводит по памяти. Это знание, а не физический объект или биометрическая характеристика. **Задание 6.7** Какой основной принцип обеспечивает стойкость TOTP (Time-based One-Time Password) к атакам повторного использования? Варианты ответов: а) Использование криптографической хеш-функции. б) Синхронизация по времени между клиентом и сервером. в) Длина пароля в 8 символов. г) Использование сертификатов X.509. Ответ: б) Пояснение: ответ "б" верный, потому что весь механизм TOTP основан на том, что и клиент (приложение), и сервер генерируют один и тот же код, используя общий секрет и текущее время, поделенное на интервал (например, 30 секунд). По истечении интервала генерируется новый код, что делает предыдущий недействительным. **Задание 6.8** Как называется компонент в системе Kerberos, который выдает билеты для доступа к конкретным сетевым сервисам после того, как клиент предъявит ему TGT (Ticket-Granting Ticket)? Ответ: Сервер выдачи билетов (Ticket Granting Server (TGS)) Пояснение: TGS — это одна из двух основных частей KDC (наряду с AS — Authentication Server). Его роль — предоставлять доступ к сервисам, не требуя повторного ввода пароля

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			пользователя, что реализует концепцию Single Sign-On (SSO) в рамках домена Kerberos. **Задание 6.9** Какой термин описывает статистическую ошибку биометрической системы, при которой она не распознает зарегистрированного законного пользователя (ложный отказ в доступе)? Ответ: Ложный отказ (False Rejection Rate (FRR)) Пояснение: FRR — это один из двух ключевых показателей эффективности биометрической системы (наряду с FAR — False Acceptance Rate). Высокий FRR снижает удобство использования, так как законные пользователи часто сталкиваются с проблемами при аутентификации. Настройка системы часто представляет собой поиск баланса между FRR и FAR.
Тема 7 Управление доступом. Протоколирование и аудит	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с	**Задание 7.1** Какие из перечисленных свойств являются корректными для модели Белла-ЛаПадулы? Варианты ответов: а) Основная цель — предотвращение утечки информации к субъектам с более низким уровнем допуска. б) Модель является разновидностью дискреционного управления доступом (DAC). в) Модель формально описывает два свойства: «No Read Up» и «No Write Down». г) Владелец объекта может по своему усмотрению передать права доступа другому субъекту. Ответ: а, в. Пояснение: ответ "а" - это основная цель данной модели, разработанной для защиты государственных секретов. Ответ "в", «No Read Up» (простое свойство безопасности) и «No Write Down» (*-свойство) — это формальные правила, запрещающие чтение «сверху» и запись «вниз» по уровням классификации.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	основных требований информационной безопасности	применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	**Задание 7.2** Какие из перечисленных действий относятся к функциям активного аудита? Варианты ответов: а) Архивное хранение журналов событий в течение 5 лет. б) Немедленное оповещение администратора при обнаружении 5 неудачных попыток входа в систему за 1 минуту. в) Ежеквартальный анализ статистики событий для выявления аномалий. г) Автоматическая блокировка учетной записи при попытке доступа к файлу с повышенным уровнем секретности. Ответ: б, г. Пояснение: Ответ "б", мгновенное оповещение на основе анализа событий в реальном времени — ключевой признак активного аудита. Ответ "г", автоматическое реагирование (блокировка) на основе предопределенных правил — это высшая форма активного аудита, тесно связанная с системами IPS (Intrusion Prevention Systems). **Задание 7.3** Установите последовательность этапов процесса управления доступом при попытке субъекта получить доступ к объекту. Этапы: 1. Проверка прав доступа субъекта к объекту в соответствии с моделью безопасности. 2. Идентификация и аутентификация субъекта. 3. Фиксация события доступа в журнале аудита. 4. Предоставление или отказ в запрошенной операции (чтение/запись). Ответ: 2,1,4,3

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: Сначала система должна установить, кто совершает действие (2. Аутентификация). Затем она проверяет, имеет ли он право на это действие (1. Проверка прав). После принятия решения о доступе система его 4. Исполняет (предоставляет или отказывает). И, наконец, независимо от результата, факт попытки доступа 3 протоколируется. **Задание 7.4** Расположите модели управления доступом в порядке убывания гибкости для конечного пользователя (от самой гибкой к самой строгой). Модели: 1. Ролевая модель доступа (RBAC) 2. Мандатное управление доступом (MAC, модель Белла-ЛаПадулы) 3. Дискреционное управление доступом (DAC) Ответ: 3,1,2 Пояснение: DAC — наиболее гибкая: владелец данных сам решает, кому предоставить доступ. RBAC — менее гибкая: доступ определяется ролью, назначенной пользователю администратором. MAC — наименее гибкая (самая строгая): доступ жестко определяется системными политиками (метками безопасности), пользователь не может их изменить. **Задание 7.5** Установите соответствие между понятием в области протоколирования и аудита и его описанием. Список 1 (Понятие): 1. Журнал аудита (Audit Log) 2. Активный аудит 3. Невозбраняемость (Non-Repudiation) 4. Событие безопасности

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Список 2 (Описание): А. Зафиксированное в системе действие, которое может повлиять на безопасность. Б. Способность доказать, что конкретное действие было выполнено определенным пользователем. В. Защищенный от модификации хронологический record событий, имеющих отношение к безопасности. Г. Реальный мониторинг и автоматическое реагирование на события безопасности. Ответ: 1В, 2Г, 3Б, 4А **Задание 7.6** Какой основной принцип ролевой модели управления доступом (RBAC) позволяет эффективно управлять правами в больших организациях? Варианты ответов: а) Назначение прав доступа напрямую каждому пользователю. б) Сопоставление пользователей ролям, а ролей — разрешениям. в) Использование меток конфиденциальности для всех объектов системы. г) Предоставление владельцам данных полномочий по управлению доступом. Ответ: б) Пояснение: ответ "б" - это суть модели RBAC. Администратор управляет не правами тысяч пользователей, а правами десятков ролей и членством пользователей в этих ролях, что резко снижает сложность администрирования. **Задание 7.7** Какое из свойств модели Белла-ЛаПадула предотвращает утечку информации «сверху вниз» (от более высокого уровня классификации к более низкому)?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Варианты ответов: а) Простое свойство безопасности (No Read Up). б) Свойство целостности (No Write Up). в) *-свойство (No Write Down). г) Дискреционное свойство. Ответ: в) Пояснение: ответ "в" - свойство (No Write Down / "Не записывать вниз") запрещает субъекту с высоким уровнем доступа записывать информацию в объект с низким уровнем. Это прямо блокирует канал утечки, когда секретные данные могут быть скопированы в публичный файл. **Задание 7.8** Как называется свойство безопасности, обеспечиваемое средствами протоколирования и криптографии, которое не позволяет субъекту отказаться от совершенного им действия? Ответ: Невозбраняемость / Non-Repudiation. Пояснение: Это одно из ключевых свойств, которое выходит за рамки простого детектирования и обеспечивает юридическую значимость записей в журнале. Оно достигается за счет использования электронной подписи, временных меток и обеспечения целостности логов. **Задание 7.9** Как называется модель управления доступом, в которой права субъекта на доступ к объекту определяются владельцем этого объекта? Ответ: Дискреционное управление доступом / Discretionary Access Control (DAC). Пояснение: Это фундаментальное определение DAC. Ключевая фигура здесь —

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			"владелец" (owner), который обладает дискрецией (правом выбора) при назначении прав доступа другим пользователям. Это отличает DAC от мандатных и ролевых моделей, где права задаются централизованно.
Тема 8 Криптографические методы защиты	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информацион	**Задание 8.1** Какие из перечисленных утверждений являются корректными для симметричных криптосистем? Варианты ответов: а) Для шифрования и дешифрования используется один и тот же секретный ключ. б) Алгоритм RSA является классическим примером симметричной криптосистемы. в) Основная проблема — безопасная доставка секретного ключа сторонам. г) Они, как правило, работают медленнее, чем асимметричные системы при шифровании больших объемов данных. Ответ: а, в. Пояснение: ответ "а" - это прямое определение симметричного шифрования. Ответ "в", "Проблема распределения ключей" — это ключевой недостаток симметричных систем, так как ключ должен быть передан по защищенному каналу. **Задание 8.2** Какие из перечисленных алгоритмов являются блочными шифрами? Варианты ответов: а) AES (Advanced Encryption Standard) б) Шифр Цезаря в) ГОСТ 34.12-2015 ("Кузнечик" или "Магма") г) RSA Ответ: а, в.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
		ной безопасности на базовом уровне	Пояснение: ответ "а". AES — это современный стандарт блочного шифрования. Ответ "в", ГОСТ 34.12-2015 — это российский стандарт, определяющий блочные шифры "Кузнечик" и "Магма". **Задание 8.3** Установите последовательность этапов работы сети Фейштеля для одного раунда при шифровании блока данных. Этапы: 1. Применение раундовой функции F к правой половине блока и раундовому ключу. 2. Наложение результата функции F на левую половину блока с помощью операции XOR. 3. Разбиение входного блока на две равные части (L и R). 4. Обмен местами полученных половин (новые L и R). Ответ: 3,1,2,4 Пояснение: Это классическая структура раунда Фейштеля. Сначала блок разбивается (3). Затем к правой части R и ключу применяется функция F (1). Ее результат складывается по XOR с левой частью L (2). В конце раунда половинки меняются местами (4), чтобы результат функции F повлиял на следующий раунд. **Задание 8.4** Расположите алгоритмы шифрования в хронологическом порядке их создания/стандартизации (от самого старого к самому новому). Алгоритмы: 1. AES (Advanced Encryption Standard) 2. DES (Data Encryption Standard) 3. Шифр Цезаря 4. ГОСТ 28147-89 (предшественник ГОСТ 34.12-2015)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Ответ: 3,2,4,1 Пояснение: Шифр Цезаря — античный шифр (I в. до н.э.). DES — разработан в 1970-х и утвержден как стандарт в 1977 г. ГОСТ 28147-89 — советский/российский стандарт, введенный в 1989 г. AES — стал новым американским стандартом в 2001 г., сменив DES. **Задание 8.5** Установите соответствие между криптографическим понятием и его определением. Список 1 (Понятие): 1. Исходный текст 2. Криптостойкость 3. Ключ 4. Шифротекст Список 2 (Определение): А. Секретная информация, определяющая результат работы шифрующего алгоритма. Б. Устойчивость шифра к криптоанализу, то есть его способность противостоять попыткам дешифрования. В. Данные, полученные после применения шифра. Г. Исходные, незашифрованные данные, подлежащие защите. Ответ: 1Г, 2Б, 3А, 4В **Задание 8.6** Установите соответствие между алгоритмом шифрования и его ключевой характеристикой. Список 1 (Алгоритм): 1. DES

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			2. AES 3. RSA 4. ГОСТ 34.12-2015 ("Кузнечик") Список 2 (Характеристика): А. Симметричный блочный шифр с длиной блока 128 бит и переменной длиной ключа (128, 192, 256). Б. Симметричный блочный шифр с длиной блока 64 бита и ключом 56 бит, устаревший из-за малой длины ключа. В. Асимметричный алгоритм, стойкость которого основана на сложности факторизации больших чисел. Г. Российский стандарт симметричного блочного шифра с длиной блока 128 бит. Ответ: 1Б, 2А, 3В, 4Г **Задание 8.7** На чем основана криптографическая стойкость алгоритма RSA? Варианты ответов: а) На сложности решения задачи дискретного логарифмирования в конечном поле. б) На сложности инвертирования блочной сети Фейштеля без знания ключа. в) На сложности факторизации больших чисел, являющихся произведением двух простых чисел. г) На сложности вскрытия шифра простой замены частотным анализом. Ответ: в) Пояснение: ответ "в" - это фундаментальное положение RSA. Открытый ключ — это произведение двух больших простых чисел, а секретный ключ — одно из них. Задача взлома — найти эти простые множители, что является вычислительно сложной задачей для достаточно больших чисел.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 8.8 Какой из перечисленных алгоритмов является асимметричным? Варианты ответов: а) AES (Advanced Encryption Standard) б) ГОСТ 34.12-2015 ("Кузнечик") в) DES (Data Encryption Standard) г) RSA (Rivest–Shamir–Adleman) Ответ: г) Пояснение: ответ "г", RSA — это классический и наиболее известный асимметричный алгоритм, использующий пару ключей: открытый и закрытый. **Задание 8.9** Как называется основной метод криптоанализа, используемый для вскрытия шифров простой замены (например, шифра Цезаря), основанный на статистике появления символов в языке? Ответ: Частотный анализ / Frequency analysis. Пояснение: Это фундаментальный метод, использующий тот факт, что в любом естественном языке буквы и сочетания букв встречаются с определенной, predictable частотой. Сопоставляя частоту символов в шифротексте с эталонной частотой для языка, криптоаналитик может восстановить исходный текст. **Задание 8.10** Как называется архитектура (структура), используемая во многих блочных шифрах (например, в DES), которая разделяет блок на две части и обрабатывает их за несколько раундов с использованием раундовых ключей и специальной функции?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Ответ: Сеть Фейштеля / Feistel network. Пояснение: Сеть Фейштеля — это фундаментальная конструкция в криптографии. Ее ключевое преимущество заключается в том, что процессы шифрования и дешифрования практически идентичны, что упрощает реализацию как в аппаратном обеспечении (hardware), так и в программном обеспечении (software). Алгоритм DES является самым известным шифром, построенным на этой сети.
Тема 9 Контроль целостности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных	**Задание 9.1** Какие из перечисленных свойств являются обязательными требованиями для криптографической хэш-функции? Варианты ответов: а) Детерминированность: один и тот же вход всегда дает одинаковый хэш. б) Однонаправленность (невозможность восстановить входные данные по хэшу). в) Возможность целенаправленного подбора двух разных входов с одинаковым хэшем (коллизией). г) Высокая скорость работы при шифровании больших объемов данных. Ответ: а, б. Пояснение: ответ "а", детерминированность — фундаментальное свойство, без которого проверка целостности была бы невозможна. Ответ "б", однонаправленность — это свойство, которое делает хэш-функцию пригодной для контроля целостности, так как злоумышленник не может по контрольной сумме восстановить исходные данные. **Задание 9.2** Какие из следующих утверждений точно описывают свойства Электронной Цифровой Подписи (ЭЦП)?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
		технологий и с учётом основных требований информационной безопасности на базовом уровне	Варианты ответов: а) ЭЦП обеспечивает конфиденциальность подписанного документа. б) ЭЦП гарантирует целостность подписанного документа. в) ЭЦП обеспечивает неотказуемость (невозбраняемость) от авторства подписи. г) Для проверки ЭЦП всегда требуется секретный ключ. Ответ: б, в. Пояснение: ответ "б" верный, так как одна из основных функций ЭЦП — это контроль целостности. Любое изменение документа после подписания приведет к невалидности подписи. Ответ "в" верный, так как неотказуемость — ключевое юридическое свойство ЭЦП, которое не позволяет подписавшемуся отрицать факт подписания. **Задание 9.3** Установите правильную последовательность шагов для подписания электронного документа с использованием ЭЦП. Шаги: 1.Формирование электронной подписи путем шифрования хэша на секретном ключе отправителя. 2. Передача исходного документа и полученной электронной подписи получателю. 3. Вычисление хэш-суммы от исходного электронного документа. 4. Получение исходного электронного документа. Ответ: 4,3,1,2 Пояснение: Процесс начинается с наличия документа (4). Далее от него вычисляется хэш (3), который затем шифруется секретным ключом для создания подписи (1). И только после этого отправляются и документ, и подпись (2). **Задание 9.4**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Расположите в логической последовательности этапы проверки подлинности и целостности данных с помощью хэш-функции. Этапы: 1. Сравнение полученного хэша с исходным (хранящимся в безопасном месте) хэшем. 2. Получение данных и их контрольного хэша по незащищенному каналу. 3. Вычисление хэш-суммы от полученных данных. 4. Вывод о целостности данных: совпадение хэшей означает отсутствие изменений. Ответ: 2,3,1,4 Пояснение: Сначала обе стороны (хэш и данные) должны быть получены (2). Затем от данных вычисляется новый хэш (3). Этот новый хэш сравнивается с эталонным (1), и на основе этого делается вывод о целостности (4). **Задание 9.5** Установите соответствие между понятием в области контроля целостности и ЭЦП и его определением. Список 1 (Понятие): 1. Хэш-функция 2. Цифровой сертификат 3. Электронная подпись 4. Коллизия хэш-функции Список 2 (Определение): А. Электронный документ, связывающий открытый ключ с данными о его владельце и заверенный подписью Удостоверяющего Центра. Б. Ситуация, когда двум разным наборам данных соответствует одинаковое значение хэша. В. Криптографическое преобразование, ставящее в соответствие произвольному массиву

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			данных фиксированное значение хэша. Г. Реквизит электронного документа, позволяющий проверить его целостность и авторство. Ответ: 1В, 2А, 3Г, 4Б **Задание 9.6** Установите соответствие между алгоритмом/стандартом и его областью применения. Список 1 (Алгоритм/Стандарт): 1. ГОСТ Р 34.11-2012 ("Стрибог") 2. SHA-256 3. ГОСТ Р 34.10-2012 4. X.509 Список 2 (Область применения): А. Стандарт на функцию хэширования (Россия). Б. Стандарт на электронную цифровую подпись (Россия). В. Стандарт на формат цифровых сертификатов. Г. Функция хэширования (США, широко используется internationally). Ответ: 1А, 2Г, 3Б, 4В **Задание 9.7** Какое свойство хэш-функции описывает сопротивление нахождению коллизий? Варианты ответов: а) Детерминированность: один и тот же вход всегда дает одинаковый хэш. б) Стойкость к восстановлению прообраза: вычислительно невозможно подобрать входные данные по заданному хэшу. в) Стойкость к нахождению второго прообраза: вычислительно невозможно найти другой

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			вход с тем же хэшем, имея один вход. г) Лавинный эффект: незначительное изменение во входных данных вызывает значительное изменение хэша. Ответ: в) Пояснение: ответ "в" верный, так как это прямое определение сопротивления нахождению второго прообраза, которое является одним из аспектов стойкости к коллизиям. **Задание 9.8** Какой криптографический примитив является основой для создания Электронной Цифровой Подписи в алгоритмах наподобие RSA? Варианты ответов: а) Симметричное шифрование. б) Хэш-функция. в) Генератор псевдослучайных чисел. г) Асимметричное шифрование. Ответ: г) Пояснение: ответ "г" верный, так как ЭЦП основана на асимметричном шифровании. Секретный ключ используется для "шифрования" (подписания) хэша, а открытый — для "расшифровки" (проверки) подписи. **Задание 9.9** Как называется свойство хэш-функции, которое гарантирует, что вычислительно невозможно найти два разных входных сообщения, дающих одинаковый выходной хэш? Ответ: Устойчивость к коллизиям

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: Это самое строгое требование к криптографической хэш-функции. Если злоумышленник может найти коллизию, он может подменить одно сообщение другим с той же подписью или контрольной суммой, полностью обойдя механизм контроля целостности. **Задание 9.10** Как называется сторона, которая проверяет электронную подпись под документом, используя для этого открытый ключ подписавшего? Ответ: Проверяющий. Пояснение: В модели ЭЦП есть две ключевые роли: подписант (тот, кто создает подпись с помощью своего закрытого ключа) и проверяющий (тот, кто проверяет ее подлинность и целостность с помощью соответствующего открытого ключа).
Тема 10 Экранирование. Тунелирование	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической	**Задание 10.1** Какие из перечисленных функций относятся к основным задачам межсетевого экрана (firewall)? Варианты ответов: а) Шифрование всего исходящего интернет-трафика для обеспечения конфиденциальности. б) Блокирование несанкционированного доступа извне в защищаемую сеть. в) Контроль и фильтрация сетевого трафика на основе заданных правил. г) Защита от вирусов и вредоносного ПО на уровне содержимого файлов. Ответ: б, в. Пояснение: ответ "б" верный, так как это одна из первичных задач firewall — создание барьера между доверенной (внутренней) и недоверенной (внешней) сетью. Ответ "в" верный, потому что это базовая функция любого МЭ: анализ пакетов и принятие решения

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
	и с учетом основных требований информационной безопасности	культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	(пропустить/отклонить) на основе политики безопасности. **Задание 10.2** Какие из перечисленных технологий или протоколов используются для построения Виртуальных Частных Сетей (VPN)? Варианты ответов: а) IPsec (Internet Protocol Security) б) SMTP (Simple Mail Transfer Protocol) в) OpenVPN г) DNS (Domain Name System) Правильные ответы: а, в. Пояснение: ответ "а", IPsec — это стандартный набор протоколов для обеспечения безопасного обмена пакетами на сетевом уровне, широко используемый для VPN. Ответ "в", OpenVPN — это популярная реализация VPN с открытым исходным кодом, использующая библиотеки SSL/TLS **Задание 10.3** Установите последовательность обработки сетевого пакета классическим сетевым экраном с фильтрацией пакетов (packet filter). Этап обработки: 1. Принятие решения: пропустить пакет или отбросить. 2. Проверка пакета на соответствие правилам в списке контроля доступа (ACL). 3. Получение пакета на интерфейс. 4. Передача пакета целевому узлу в случае положительного решения. Ответ: 3,2,1,4

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Пояснение: Сначала пакет поступает на интерфейс (3). Затем МЭ анализирует его заголовки (IP, порты, флаги) на соответствие правилам (2). На основе этого анализа принимается решение (1), и если оно положительное, пакет передается дальше (4). **Задание 10.4** Расположите виды межсетевых экранов в порядке их появления и эволюции (от самого простого к более сложному). Виды экранов: 1. Межсетевой экран прикладного уровня (proxy) 2. Межсетевой экран с фильтрацией пакетов 3. Межсетевой экран нового поколения (NGFW) 4. Межсетевой экран с проверкой на уровне сессии (stateful inspection) Ответ: 2,4,1,3 Пояснение: Эволюция шла от простой фильтрации пакетов (2) к более умной stateful inspection (4), которая учитывает состояние соединений. Затем появились шлюзы прикладного уровня (1) для глубокого анализа конкретных сервисов. Современным этапом являются NGFW (3), объединяющие все предыдущие функции и добавляющие анализ содержимого и идентификацию приложений. **Задание 10.5** Установите соответствие между типом межсетевого экрана и его ключевым принципом работы. Список 1 (Тип МЭ): 1. Фильтрация пакетов (Packet Filter) 2. Stateful Inspection 3. Шлюз прикладного уровня (Application Proxy) 4. МЭ нового поколения (NGFW)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Список 2 (Принцип работы): А. Анализирует заголовки пакетов (IP-адреса, порты) без учета состояния соединения. Б. Анализирует трафик в контексте состояния соединений и может идентифицировать конкретные приложения. В. Полностью terminates и инициирует соединения от имени конечных узлов, анализируя данные на уровне приложений. Г. Отслеживает состояние активных соединений (например, по таблице состояний) и принимает решения на основе контекста. Ответ: 1А, 2Г, 3В, 4Б **Задание 10.6** Установите соответствие между понятием и его определением в контексте экранирования и туннелирования. Список 1 (Понятие): 1. Экранирование 2. Туннелирование 3. VPN 4. Демилитаризованная зона (DMZ) Список 2 (Определение): А. Метод инкапсуляции пакетов одного протокола в пакеты другого для их передачи по чужеродной сети. Б. Виртуальная сеть, создаваемая поверх другой сети (например, Интернет) с целью обеспечения конфиденциальности и целостности передаваемых данных. В. Размещение ресурсов, требующих ограниченного доступа извне, в изолированном сегменте сети. Г. Метод защиты сети, предполагающий установку барьера между различными

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			сегментами сети для контроля и фильтрации трафика. Ответ: 1Г, 2А, 3Б, 4В **Задание 10.7** Какой основной принцип лежит в основе работы межсетевого экрана с Stateful Inspection? Варианты ответов: а) Анализ только IP-адресов источника и назначения в каждом пакете по отдельности. б) Полное завершение на себе всех соединений и анализ данных на уровне приложений. в) Принятие решений на основе таблицы состояний активных соединений. г) Шифрование всего трафика, проходящего через устройство. Ответ: в) Пояснение: ответ "в" верный, так как ключевое отличие Stateful Inspection от простой фильтрации пакетов — это ведение таблицы состояний (state table). МЭ запоминает инициированные изнутри соединения и разрешает обратный трафик, относящийся к этим сессиям, даже без явного правила. **Задание 10.8** Какой из перечисленных протоколов работает на сетевом уровне (уровне 3 OSI) и является стандартом для построения защищенных VPN? Варианты ответов: а) SSL/TLS б) PPTP в) IPsec г) HTTP

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Ответ: в) Пояснение: ответ "в" верный, так как IPsec работает на сетевом уровне, обеспечивая "прозрачную" защиту для всех вышележащих протоколов. Это отраслевой стандарт для VPN типа "сеть-сеть" и удаленного доступа. **Задание 10.9** Как называется сегмент сети, расположенный между внутренней (доверенной) и внешней (недоверенной) сетью, в котором обычно размещаются общедоступные серверы (веб, почта)? Ответ: Демилитаризованная зона / DMZ. Пояснение: DMZ — это классическая архитектурная концепция экранирования. Она позволяет предоставить ограниченный доступ к публичным сервисам, не подвергая прямому риску всю внутреннюю сеть. Доступ в DMZ и из нее строго контролируется правилами межсетевого экрана. **Задание 10.10** Как называется технология, которая позволяет инкапсулировать трафик одного протокола (например, IP) внутри пакетов другого протокола для создания защищенного канала через общедоступную сеть? Ответ: Туннелирование / Tunneling. Пояснение: Туннелирование — это фундаментальный принцип, лежащий в основе VPN. Оно создает "виртуальный кабель" поверх небезопасной сети (например, Интернета), внутри которого передаются защищенные пакеты. Примеры: IPsec-туннель, SSL-туннель, GRE-туннель.
Тема 11 Анализ	ОПК-3 Способен	**И О П К - 3 . 1 .** Знать	**Задание 11.1** Какие из перечисленных действий являются целями проведения анализа защищенности

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
защищенности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	(security assessment)? Варианты ответов: а) Повышение производительности работы сетевого оборудования. б) Выявление уязвимостей в программном обеспечении и конфигурациях. в) Оценка соответствия системы требованиям политики информационной безопасности. г) Гарантированное устранение всех возможных уязвимостей. Правильные ответы: б, в. Пояснение: вариант "б" верный, так как это прямая задача анализа защищенности — проактивный поиск слабых мест до того, как ими воспользуется злоумышленник. Ответ "в" верный, так как аудит и оценка соответствия стандартам и внутренним политикам — одна из ключевых целей анализа. **Задание 12.2** Какие из перечисленных технологий являются основными методами детектирования для современных антивирусных программ? Варианты ответов: а) Сигнатурный анализ. б) Эвристический анализ. в) Сканирование портов. г) Проведение DDoS-атак на подозрительные серверы. Правильные ответы: а, б. Пояснение: вариант "а", сигнатурный анализ — это базовый метод, основанный на сравнении кода с базой известных сигнатур (отпечатков) вредоносных программ. Ответ "б", эвристический анализ — это продвинутый метод, позволяющий обнаруживать новые,

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			ранее неизвестные угрозы, путем анализа поведения и характеристик кода. **Задание 12.3** Установите правильную последовательность этапов проведения теста на проникновение (penetration test) после заключения договора. Этапы: 1.Документирование результатов и составление отчета с рекомендациями. 2. Активная фаза: эксплуатация уязвимостей для получения доступа. 3. Сканирование сети и систем для выявления активных хостов и служб. 4. Анализ собранной информации и выявление потенциальных уязвимостей. Ответ: 3421 Пояснение: Стандартная методология (например, PTES) начинается с разведки и сканирования (3). Затем следует анализ данных и поиск уязвимостей (4). После этого происходит непосредственная атака и закрепление в системе (2). Завершает процесс составление отчета (1). **Задание 12.4** Установите соответствие между типом вредоносного программного обеспечения и его определением. Список 1 (Тип вредоносного ПО): 1. Черви (Worms) 2. Трояны (Trojans) 3. Рекламное ПО (Adware) 4. Шпионское ПО (Spyware) Список 2 (Определение): А. Программы, маскирующиеся под легитимное ПО, но выполняющие скрытые вредоносные действия.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Б. Программы, демонстрирующие нежелательную рекламу и собирающие данные о пользователе для показа целевой рекламы. В. Самостоятельно распространяющиеся программы, которые для размножения используют сетевые каналы. Г. Программы, тайно собирающие информацию о действиях пользователя и передающие ее третьим лицам. Ответ: 1В, 2А, 3Б, 4Г **Задание 12.5** Установите соответствие между инструментом анализа защищенности и его основной функцией. Список 1 (Инструмент/Метод): 1. Сетевой сканер (e.g., Nmap) 2. Сканер уязвимостей (e.g., OpenVAS, Nessus) 3. Антивирусное ПО 4. Межсетевой экран (Firewall) Список 2 (Основная функция): А. Обнаружение и удаление вредоносного программного обеспечения на конечной точке. Б. Обнаружение активных сетевых узлов, открытых портов и запущенных служб. В. Автоматизированное выявление и оценка уязвимостей в программном обеспечении и конфигурациях. Г. Контроль и фильтрация сетевого трафика на основе заданных правил. Ответ: 1Б, 2В, 3А, 4Г **Задание 12.6** Какой метод антивирусной защиты позволяет обнаруживать новые, неизвестные ранее вредоносные программы путем анализа их поведения и характеристик кода?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Варианты ответов: а) Сигнатурный анализ. б) Эвристический анализ. в) Сравнение с белым списком (whitelisting). г) Контроль целостности файлов. Ответ: б) Пояснение: вариант "б", эвристический анализ — это единственный из перечисленных методов, который предназначен для обнаружения неизвестных угроз путем поиска подозрительных инструкций, шаблонов поведения или кода, характерных для вредоносных программ. **Задание 12.7** Что из перечисленного является прямым признаком заражения компьютера вредоносным программным обеспечением? Варианты ответов: а) Высокая производительность системы. б) Самопроизвольное открытие CD/DVD-привода. в) Стабильная работа всех программ. г) Отсутствие сетевой активности. Ответ: б) Пояснение: ответ "б" верный, так как некоторые вредоносные программы используют самопроизвольное открытие лотка CD/DVD как способ демонстрации своего присутствия или тестирования доступа к аппаратному обеспечению. Это классический симптом.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Тест по теме
			Задание 12.8 Как называется метод антивирусной защиты, который подразумевает запуск подозрительной программы в изолированной и контролируемой среде для наблюдения за ее поведением без риска для основной системы? Ответ: Песочница / Sandbox. Пояснение: Анализ в "песочнице" — это продвинутая технология, позволяющая детектировать сложные и полиморфные угрозы, которые могут обойти сигнатурный и эвристический анализ. Наблюдая за действиями программы в изоляции (попытки доступа к реестру, сетевые соединения, создание файлов), можно с высокой точностью определить ее вредоносность. **Задание 12.9** Как называется уникальный идентификатор, представляющий собой характерную последовательность данных, extracted из известного вредоносного ПО, который используется антивирусными программами для его опознания? Ответ: Сигнатура / Signature. Пояснение: Сигнатурный анализ — это основа работы традиционных антивирусов. Сигнатура является своеобразным "отпечатком пальца" вируса. Эффективность этого метода напрямую зависит от актуальности антивирусных баз, которые должны регулярно обновляться.

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.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
Тема 1 Введение в информационную безопасность Тема 2 Законодательный уровень информационной безопасности Тема 3 Стандарты и спецификации в области информационной безопасности Тема 4 Административный уровень информационной безопасности Тема 5 Процедурный уровень информационной безопасности	УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИУК-10.2.** Уметь реализовывать средства обеспечения законности и правопорядка в сфере противодействия экстремизма, терроризма, коррупционному поведению ИОПК-3.2. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на	**Задание 1.1.** Анализ документа на соответствие ФЗ-152 Проанализируйте приведенный текст Согласия на обработку персональных данных на соответствие требованиям ст. 9 ФЗ-152 «О персональных данных». Выявите недостающие обязательные сведения. Исходные данные: *Я, Иванов Иван Иванович, даю согласие ООО «Компания»* *на обработку своих персональных данных: ФИО, номера* *телефона и адреса электронной почты.* Ответ: Недостающие обязательные реквизиты согласно ст. 9 ФЗ-152: 1. Цель обработки персональных данных 2. Перечень действий с персональными данными 3. Срок действия согласия 4. Порядок отзыва согласия 5. Сведения о лице, получающем согласие (наименование, адрес) 6. Подпись субъекта ПДн **Задание 1.2.** Анализ политики безопасности

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
		базовом уровне	Проанализируйте фрагмент Политики информационной безопасности. Определите, каким принципам управления доступом соответствуют приведенные правила. Исходные данные: Раздел 5. Управление доступом: *5.1. Доступ к конфиденциальным документам предоставляется только сотрудникам с соответствующим уровнем допуска.* *5.2. Сотрудники отдела кадров не могут утверждать финансовые документы.* *5.3. Владелец файла может предоставить доступ другим сотрудникам по своему усмотрению.* Ответ: Соответствие принципам управления доступом: ● Правило 5.1 → Мандатное управление доступом (MAC). Основано на уровнях допуска (метках безопасности) ● Правило 5.2 → Ролевое управление доступом (RBAC). Основано на организационных ролях ● Правило 5.3 → Дискреционное управление доступом (DAC). Владелец самостоятельно управляет доступом

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			Задание 2.1. Разработка раздела регламента Разработайте раздел «Порядок обработки персональных данных» для Регламента информационной безопасности. Включите не менее 5 обязательных пунктов, соответствующих требованиям ФЗ-152. Исходные данные: 1. Компания обрабатывает персональные данные сотрудников и клиентов 2. Необходимо обеспечить соответствие ст. 18.1, 19 ФЗ-152 Ответ: ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 1. Все персональные данные классифицируются по категориям: a. Общедоступные b. Конфиденциальные c. Специальные категории 2. Для каждой категории определяются: a. Цели обработки b. Перечень обрабатываемых данных c. Сроки хранения 3. Обработка специальных категорий ПДн осуществляется только с письменного согласия субъекта. 4. Ежеквартально проводится оценка защищенности ПДн. 5. Назначены ответственные за организацию обработки ПДн

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			в каждом структурном подразделении. **Задание 2.2.** Разработка процедуры инцидент-менеджмента Разработайте процедуру «Действия при утечке персональных данных» согласно требованиям ст. 22.1 ФЗ-152. Исходные данные: 1. Обязанность уведомлять Роскомнадзор в течение 24 часов 2. Необходимость документирования всех инцидентов Ответ: ПРОЦЕДУРА: Действия при утечке персональных данных 1. Немедленно заблокировать соответствующие учетные записи и системы. 2. В течение 2 часов с момента обнаружения: ● Уведомить руководителя службы ИБ ● Начать сбор информации об инциденте 3. В течение 24 часов с момента обнаружения: ● Направить уведомление в Роскомнадзор ● Состав уведомления: характер ПДн, категории субъектов, предполагаемые причины, принятые меры 4. В течение 3 рабочих дней:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			● Проинформировать субъектов ПДн (если требуется) ● Задокументировать инцидент в журнале учета 5. В течение 10 рабочих дней: ● Провести расследование причин инцидента ● Разработать корректирующие мероприятия
Тема 6 Идентификация и аутентификация Тема 7 Управление доступом. Протоколирование и аудит Тема 8 Криптографические методы защиты Тема 9 Контроль целостности Тема10 Экранирование. Тунелирование Тема 11 Анализ защищенности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	**Задание 3.1**. Реализация функции хеширования Реализуйте на Python упрощенную хеш-функцию на основе алгоритма SHA-256. Функция должна принимать строку и возвращать ее хеш в hex-формате. Исходные данные: 1. Использовать встроенную библиотеку hashlib 2. Функция должна обрабатывать строки в кодировке UTF-8 3. Результат - строка из 64 hex-символов Ответ на языке python import hashlib def compute_sha256_hash(input_string): """ Вычисляет SHA-256 хеш для входной строки Args:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			input_string (str): Входная строка для хеширования
			Returns:
			str: Хеш в виде hex-строки (64 символа)
			"""
			# Преобразуем строку в байты
			input_bytes = input_string.encode('utf-8')
			# Создаем объект хеша SHA-256
			hash_object = hashlib.sha256()
			# Обновляем хеш данными
			hash_object.update(input_bytes)
			# Получаем hex-представление
			hex_digest = hash_object.hexdigest()
			return hex_digest
			# Пример использования
			if __name__ == "__main__":
			test_string = "Hello, Information Security!"

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			result_hash = compute_sha256_hash(test_string) print(f"Хеш строки '{test_string}':") print(result_hash) print(f"Длина хеша: {len(result_hash)} символов") **Задание 3.2**. Реализация симметричного шифрования Реализуйте на выбранном языке программирования функции для симметричного шифрования и дешифрования с использованием алгоритма AES в режиме GCM. Функции должны поддерживать работу с текстовыми строками. Исходные данные: 1. Использовать библиотеку cryptography 2. Режим шифрования: AES-GCM 3. Длина ключа: 256 бит 4. Автоматическая генерация nonce Ответ на языке python from cryptography.hazmat.primitives.ciphers.aead import AESGCM from cryptography.hazmat.primitives import hashes from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			import os
			import base64
			def generate_key_from_password(password: str, salt: bytes = None) -> tuple:
			"""
			Генерирует ключ AES из пароля используя PBKDF2
			Args:
			password (str): Пароль для генерации ключа
			salt (bytes): Соль (если None - генерируется новая)
			Returns:
			tuple: (ключ, соль)
			"""
			if salt is None:
			salt = os.urandom(16)
			kdf = PBKDF2HMAC(
			algorithm=hashes.SHA256(),

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			length=32, salt=salt, iterations=100000,) key = kdf.derive(password.encode('utf-8')) return key, salt def encrypt_aes_gcm(plaintext: str, key: bytes) -> str: """ Шифрует строку с использованием AES-GCM Args: plaintext (str): Текст для шифрования key (bytes): Ключ шифрования Returns: str: base64-encoded строка (nonce + ciphertext + tag) """ aesgcm = AESGCM(key)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			nonce = os.urandom(12)
			plaintext_bytes = plaintext.encode('utf-8')
			ciphertext = aesgcm.encrypt(nonce, plaintext_bytes, None)
			# Объединяем nonce и ciphertext для хранения
			encrypted_data = nonce + ciphertext
			return base64.b64encode(encrypted_data).decode('utf-8')
			def decrypt_aes_gcm(encrypted_data: str, key: bytes) -> str:
			"""
			Дешифрует строку, зашифрованную AES-GCM
			Args:
			encrypted_data (str): base64-encoded зашифрованные данные
			key (bytes): Ключ шифрования
			Returns:
			str: Расшифрованный текст
			"""
			try:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			encrypted_bytes = base64.b64decode(encrypted_data.encode('utf-8'))
			nonce = encrypted_bytes[:12]
			ciphertext = encrypted_bytes[12:]
			aesgcm = AESGCM(key)
			decrypted_bytes = aesgcm.decrypt(nonce, ciphertext, None)
			return decrypted_bytes.decode('utf-8')
			except Exception as e:
			raise ValueError(f"Ошибка дешифрования: {str(e)}")
			# Пример использования
			if __name__ == "__main__":
			# Генерация ключа из пароля
			password = "secure_password_123"
			key, salt = generate_key_from_password(password)
			# Шифрование
			original_text = "Конфиденциальное сообщение"

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			encrypted = encrypt_aes_gcm(original_text, key)
			print(f"Зашифрованный текст: {encrypted}")
			# Дешифрование
			decrypted = decrypt_aes_gcm(encrypted, key)
			print(f"Расшифрованный текст: {decrypted}")
			# Проверка
			print(f"Тексты совпадают: {original_text == decrypted}")
			Задание 4.1. Реализация RBAC системы
			Реализуйте на выбранном языке программирования простую систему ролевого управления доступом (RBAC). Система должна поддерживать создание ролей, назначение прав и проверку доступа.
			Исходные данные:
			1. Три предопределенные роли: admin, editor, viewer
			2. Права: read, write, delete, manage_users
			3. Пользователи могут иметь несколько ролей
			Ответ на языке python
			class RBACSystem:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			def __init__(self):
			# Предопределенные роли и их права
			self.roles = {
			'viewer': {'read'},
			'editor': {'read', 'write'},
			'admin': {'read', 'write', 'delete', 'manage_users'}
			}
			# Пользователи и их роли
			self.user_roles = {}
			def assign_role(self, username: str, role: str):
			"""Назначает роль пользователю"""
			if role not in self.roles:
			raise ValueError(f"Роль {role} не существует")
			if username not in self.user_roles:
			self.user_roles[username] = set()
			self.user_roles[username].add(role)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			def check_permission(self, username: str, permission: str) -> bool:
			"""Проверяет наличие права у пользователя"""
			if username not in self.user_roles:
			return False
			user_roles = self.user_roles[username]
			# Проверяем все роли пользователя
			for role in user_roles:
			if permission in self.roles[role]:
			return True
			return False
			def get_user_permissions(self, username: str) -> set:
			"""Возвращает все права пользователя"""
			if username not in self.user_roles:
			return set()
			permissions = set()
			for role in self.user_roles[username]:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			permissions.update(self.roles[role])
			return permissions
			# Пример использования
			if __name__ == "__main__":
			rbac = RBACSystem()
			# Назначаем роли пользователям
			rbac.assign_role('alice', 'admin')
			rbac.assign_role('bob', 'editor')
			rbac.assign_role('charlie', 'viewer')
			# Проверяем права
			users = ['alice', 'bob', 'charlie']
			permissions = ['read', 'write', 'delete', 'manage_users']
			print("Таблица прав пользователей:")
			print("User\t\t" + "\t".join(permissions))
			for user in users:
			row = [user]

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию
			for perm in permissions: has_perm = "✓" if rbac.check_permission(user, perm) else "✗" row.append(has_perm) print("\t\t".join(row)) # Демонстрация получения всех прав print(f"\nВсе права пользователя 'alice': {rbac.get_user_permissions('alice')}") **Задание 4.2**: Реализация системы аудита Реализуйте на выбранном языке программирвоания систему протоколирования и аудита безопасности. Система должна записывать события безопасности и предоставлять методы для их анализа. Исходные данные: 1. События: login_success, login_failed, access_denied, data_access 2. Уровни важности: INFO, WARNING, CRITICAL 3. Фильтрация событий по типу, пользователю и временному диапазону Ответ на языке python

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			import datetime
			from typing import List, Dict, Optional
			from enum import Enum
			class Severity(Enum):
			INFO = 1
			WARNING = 2
			CRITICAL = 3
			class AuditEvent:
			def __init__(self, event_type: str, username: str, severity: Severity, description: str):
			self.timestamp = datetime.datetime.now()
			self.event_type = event_type
			self.username = username
			self.severity = severity
			self.description = description
			def to_dict(self) -> Dict:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			return {
			'timestamp': self.timestamp.isoformat(),
			'event_type': self.event_type,
			'username': self.username,
			'severity': self.severity.name,
			'description': self.description
			}
			def __str__(self):
			return f"[{self.timestamp}] {self.severity.name}: {self.event_type} - {self.description} (user: {self.username})"
			class SecurityAuditLogger:
			def __init__(self):
			self.events: List[AuditEvent] = []
			def log_event(self, event_type: str, username: str, severity: Severity, description: str):
			"""Записывает событие безопасности"""
			event = AuditEvent(event_type, username, severity, description)

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			self.events.append(event)
			
			print(f"LOGGED: {event}") # Для демонстрации выводим в консоль
			
			def get_events_by_user(self, username: str) -> List[AuditEvent]:
			
			"""Возвращает события по пользователю"""
			
			return [event for event in self.events if event.username == username]
			
			def get_events_by_type(self, event_type: str) -> List[AuditEvent]:
			
			"""Возвращает события по типу"""
			
			return [event for event in self.events if event.event_type == event_type]
			
			def get_events_by_severity(self, severity: Severity) -> List[AuditEvent]:
			
			"""Возвращает события по уровню важности"""
			
			return [event for event in self.events if event.severity == severity]
			
			def get_events_in_time_range(self, start_time: datetime.datetime,
			
			end_time: datetime.datetime) -> List[AuditEvent]:
			
			"""Возвращает события в временном диапазоне"""

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			return [event for event in self.events if start_time <= event.timestamp <= end_time]
			
			def generate_security_report(self) -> Dict:
			
			"""Генерирует отчет по безопасности"""
			
			report = {
			
			'total_events': len(self.events),
			
			'events_by_type': {},
			
			'events_by_severity': {},
			
			'failed_logins': len(self.get_events_by_type('login_failed')),
			
			'access_denied': len(self.get_events_by_type('access_denied'))
			
			}
			
			for event in self.events:
			
			# Статистика по типам событий
			
			report['events_by_type'][event.event_type] = \
			
			report['events_by_type'].get(event.event_type, 0) + 1
			
			# Статистика по уровням важности

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			report['events_by_severity'][event.severity.name] = \
			report['events_by_severity'].get(event.severity.name, 0) + 1
			return report
			# Пример использования
			if __name__ == "__main__":
			# Создаем логгер
			auditor = SecurityAuditLogger()
			# Логируем различные события
			auditor.log_event('login_success', 'alice', Severity.INFO, 'Успешный вход в систему')
			auditor.log_event('data_access', 'alice', Severity.INFO, 'Доступ к конфиденциальным данным')
			auditor.log_event('login_failed', 'eve', Severity.WARNING, 'Неудачная попытка входа')
			auditor.log_event('access_denied', 'eve', Severity.CRITICAL, 'Попытка доступа к запрещенному ресурсу')
			auditor.log_event('login_success', 'bob', Severity.INFO, 'Успешный вход в систему')

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Задания к практическому занятию

			print("\n" + "="*50)
			print("События пользователя 'eve':")
			for event in auditor.get_events_by_user('eve'):
			  print(f" - {event}")
			print("\n" + "="*50)
			print("Критические события:")
			for event in auditor.get_events_by_severity(Severity.CRITICAL):
			  print(f" - {event}")
			print("\n" + "="*50)
			print("Отчет по безопасности:")
			report = auditor.generate_security_report()
			for key, value in report.items():
			  print(f" {key}: {value}")

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. 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 4 Административный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом	**Задание 4.1** Какие из перечисленных документов относятся к обязательным элементам Политики информационной безопасности организации верхнего уровня? Варианты ответов: а) Инструкция по настройке межсетевого экрана. б) Положение об обработке персональных данных. в) Регламент резервного копирования. г) Концепция информационной безопасности.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
	библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основных требований информационной безопасности на базовом уровне	Ответ: б, г. Пояснение: ответ "б", положение об обработке персональных данных — это документ уровня политики, устанавливающий основные принципы, цели и правила обработки ПДн в организации. ответ "г", концепция информационной безопасности — это основополагающий документ, определяющий стратегию, принципы и подходы к защите информации в организации. Является ядром политики безопасности. **Задание 4.2** Какие из следующих действий являются ключевыми элементами программы безопасности (Security Program)? Варианты ответов: а) Установка последних обновлений безопасности на серверы. б) Регулярное проведение аудитов и оценок рисков ИБ. в) Назначение ответственных за реализацию политик безопасности. г) Проведение тренингов по повышению осведомленности в области ИБ для сотрудников. Ответ: б, в, г. Пояснение: ответ "б", аудиты и оценка рисков — это управленческие процессы, являющиеся стержнем программы безопасности для контроля ее эффективности и выявления новых угроз. Ответ "в", назначение ответственных — это организационная мера, без которой невозможно выполнение программы (принцип персональной ответственности). Ответ "г", тренинги для сотрудников — это критически важный элемент программы, направленный на управление "человеческим фактором". **Задание 4.3**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Установите правильную последовательность этапов разработки и внедрения системы управления информационной безопасностью на административном уровне. Этапы: 1. Принятие и официальное утверждение высшим руководством Политики информационной безопасности. 2. Разработка и реализация конкретных мер контроля, стандартов и процедур. 3. Проведение анализа рисков информационной безопасности. 4. Создание организационной структуры и распределение ролей и ответственности в области ИБ. Ответ: 3,1,4,2 Пояснение: Классический подход следует логике управления рисками: сначала проводится анализ рисков (3), чтобы понять, от чего защищаться. На его основе формируется верховный документ — Политика (1), которую утверждает руководство. Далее создается организационная структура (4) для реализации политики. И только затем разрабатываются конкретные меры и процедуры (2). **Задание 4.4** Расположите этапы интеграции программы безопасности в жизненный цикл информационной системы (ЖЦ ИС) в хронологическом порядке. Этапы: 1. Формальный ввод системы в эксплуатацию при условии выполнения всех требований безопасности. 2. Разработка архитектуры системы с учетом требований безопасности и анализом угроз.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			3. Вывод системы из эксплуатации с обеспечением сохранности и безопасного уничтожения архивных данных. 4. Составление и утверждение технического задания, включающего раздел с требованиями по информационной безопасности. Ответ: 4 → 2 → 1 → 3 Пояснение: Безопасность должна закладываться на ранних стадиях. Сначала требования фиксируются в ТЗ (4). Затем на их основе проектируется безопасная архитектура (2). После реализации и тестирования система вводится в эксплуатацию (1). Завершающий этап ЖЦ — безопасный вывод из эксплуатации (3). **Задание 4.5** Установите соответствие между понятием административного уровня ИБ и его определением. Список 1 (Понятие): 1. Политика безопасности 2. Программа безопасности 3. Мера контроля (Control) 4. Аудит информационной безопасности Список 2 (Определение): А. Непрерывный управленческий процесс, направленный на реализацию политики, управление рисками и достижение целей в области ИБ. Б. Формальная проверка и оценка соответствия системы защиты установленным требованиям и политикам. В. Конкретное правило, процедура или практика, предназначенная для снижения риска. Г. Совокупность формализованных правил и подходов, определяющих цели и

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			основные направления деятельности организации в области ИБ. Ответ: 1Г, 2А, 3В, 4Б **Задание 4.6** Установите соответствие между этапом жизненного цикла системы и административной мерой безопасности, которая должна быть на нем применена. Список 1 (Этап ЖЦ): 1. Проектирование 2. Реализация (кодирование) 3. Эксплуатация 4. Утилизация Список 2 (Мера безопасности): А. Проведение регулярного обучения пользователей правилам безопасной работы. Б. Проведение модерирования кода (code review) на предмет наличия уязвимостей. В. Разработка модели угроз и требований к безопасности. Г. Составление регламента уничтожения/очистки носителей информации. Ответ: 1В, 2Б, 3А, 4Г **Задание 4.7** Что из перечисленного является основной целью Политики информационной безопасности верхнего уровня? Варианты ответов: а) Детально описать настройки всех сетевых устройств.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			б) Продемонстрировать клиентам использование передовых технологий шифрования. в) Формально определить ответственность руководства и общие направления обеспечения ИБ в организации. г) Заложить основы для последующей сертификации по международным стандартам. Ответ: в) Пояснение: ответ "в" - это прямая и первичная цель политики верхнего уровня: закрепить приверженность руководства, распределить ответственность и задать стратегический курс. **Задание 4.8** Какой принцип является наиболее важным для успешной синхронизации программы безопасности с жизненным циклом систем? Варианты ответов: а) Принцип «безопасность как неотъемлемая часть процесса» (Security by Design). б) Принцип простоты контроля. в) Принцип минимальных привилегий. г) Принцип разделения обязанностей. Ответ: а) Пояснение: ответ "а", Security by Design — это краеугольный камень интеграции ИБ в ЖЦ. Он означает, что вопросы безопасности рассматриваются не постфактум, а на самых ранних этапах (проектирование, разработка), что значительно эффективнее и дешевле.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Задание 4.9 Как называется основной документ, который формально декларирует приверженность высшего руководства организации целям в области информационной безопасности, устанавливает общие рамки и определяет ответственность? Ответ: Политика информационной безопасности (Information Security Policy). Пояснение: Именно этот документ, утвержденный на уровне топ-менеджмента, является точкой отсчета для всей дальнейшей деятельности в области ИБ. Он задает тон и определяет значимость безопасности для всей организации. **Задание 4.10** На какой стадии жизненного цикла информационной системы мероприятия по безопасности являются наиболее затратными и менее эффективными для исправления фундаментальных недостатков? Ответ: Стадия эксплуатации (или сопровождения). Пояснение: Исправление архитектурных или системных недоработок в области безопасности на стадии эксплуатации требует значительных переделок, остановки работающей системы и сопряжено с наибольшими затратами и рисками. Это подтверждает важность закладки безопасности на ранних стадиях (Projection и Development).
Тема 5 Процедурный уровень информационной	ОПК-3 Способен решать стандартные задачи профессиональн	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	**Задание 5.1** Какие из перечисленных мер относятся к процедурному уровню обеспечения информационной безопасности? Варианты ответов: а) Настройка правил фильтрации на межсетевом экране.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
безопасности	ой деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	б) Проведение вводного инструктажа по безопасности для нового сотрудника. в) Установка системы видеонаблюдения по периметру здания. г) Разработка регламента резервного копирования. Ответ: б, г. Пояснение: ответ "б", инструктаж сотрудника — это классическая процедурная мера, направленная на управление персоналом. Ответ "г", разработка регламента резервного копирования — это создание формальной процедуры, определяющей порядок действий для обеспечения поддержки работоспособности. **Задание 5.2** Какие действия входят в типовой план реагирования на инциденты информационной безопасности на процедурном уровне? Варианты ответов: а) Немедленное отключение всех серверов для предотвращения распространения угрозы. б) Сбор и сохранение доказательств (логов, дампов памяти). в) Установка последних сигнатур антивирусной программы. г) Уведомление руководителя и службы ИБ о факте инцидента. Ответ: б, г. Пояснение: ответ "б", сбор доказательств — это ключевая процедура для последующего анализа инцидента и, возможно, правовых действий. Ответ "г", уведомление ответственных лиц — это первоочередная процедурная action, без которой невозможно запустить процесс реагирования. **Задание 5.3**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Установите правильную последовательность этапов управления персоналом в контексте ИБ при увольнении сотрудника. Этапы: 1. Проведение выходного интервью с напоминанием о действующих обязательствах по соблюдению конфиденциальности. 2. Получение заявления об увольнении и уведомление службы ИБ. 3. Немедленное аннулирование всех учетных записей, пропусков и токенов доступа. 4. Инвентаризация и возврат всех информационных активов (ноутбуков, документов, ключей). Ответ: 2,3,4,1 Пояснение: Процедура должна минимизировать период, когда увольняемый сотрудник имеет доступ, но уже мотивирован его использовать в ущерб. Сначала служба ИБ получает уведомление (2), чтобы немедленно аннулировать доступы (3). Затем обеспечивается возврат активов (4), и в завершение проводится финальное интервью (1) для юридического закрепления обязательств. **Задание 5.4** Расположите в логической последовательности ключевые шаги процедуры реагирования на инцидент безопасности. Шаги: 1. Локализация инцидента и предотвращение его расширения. 2. Подготовка отчета и реализация мер по предотвращению повторения инцидента. 3. Обнаружение и идентификация инцидента.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			4. Ликвидация последствий инцидента и восстановление работоспособности. Ответ: 3,1,4,2 Пояснение: Стандартный цикл реагирования начинается с обнаружения (3). После подтверждения инцидента следует его локализация (1), чтобы остановить распространение ущерба. Далее происходит восстановление (4) систем и услуг. Завершает цикл постинцидентный анализ (2), направленный на улучшение системы защиты. **Задание 5.5** Установите соответствие между классом мер процедурного уровня и конкретным примером его реализации. Список 1 (Класс мер): 1. Управление персоналом 2. Физическая защита 3. Поддержка работоспособности 4. Реагирование на нарушения Список 2 (Пример реализации): А. Регламент проведения ежедневного резервного копирования критичных данных. Б. Процедура сопровождения посетителей на территории центра обработки данных. В. Обязательство сотрудника о неразглашении коммерческой тайны (NDA). Г. Чек-лист первоочередных действий при обнаружении заражения вирусом. Ответ: 1В, 2Б, 3А, 4Г **Задание 5.6**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Установите соответствие между элементом плана восстановительных работ и его описанием. Список 1 (Элемент плана): 1. Цель восстановления (RTO - Recovery Time Objective) 2. Приоритетность систем 3. Ответственные лица 4. Точка восстановления (RPO - Recovery Point Objective) Список 2 (Описание): А. Максимально допустимое время простоя системы после инцидента. Б. Распределение ролей и контактной информации команды для выполнения плана. В. Определение порядка восстановления информационных систем и сервисов. Г. Максимально допустимый объем потери данных за период между последней резервной копией и сбоем. Ответ: 1А, 2В, 3Б, 4Г **Задание 5.7** Какой из перечисленных документов является наиболее важным с точки зрения процедурного управления персоналом для нового сотрудника, имеющего доступ к конфиденциальной информации? Варианты ответов: а) Поздравительная открытка от коллектива. б) Ознакомительный тур по офису. в) Подписанное соглашение о конфиденциальности (NDA). г) График работы и перерывов.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Ответ: в) Пояснение: ответ "в", NDA — это юридически значимая процедурная мера, которая формально закрепляет обязанности сотрудника по защите информации и устанавливает ответственность за их нарушение. Это краеугольный камень управления рисками, связанными с персоналом. **Задание 5.8** Какая из перечисленных мер в наибольшей степени способствует поддержанию работоспособности информационной системы на процедурном уровне? Варианты ответов: а) Ежеквартальная смена паролей учетных записей пользователей. б) Регламентированное ежедневное резервное копирование данных. в) Установка решёток на окна серверной комнаты. г) Проведение ежегодной проверки знаний по ИБ. Ответ: б) Пояснение: ответ "б", регламент резервного копирования — это прямая процедурная мера, предназначенная specifically для обеспечения возможности восстановления работоспособности после сбоя, потери данных или иного инцидента **Задание 5.9** Как называется ключевой количественный показатель плана восстановления, который определяет максимально допустимое время простоя информационной системы или бизнес-процесса после сбоя? Ответ: Цель по времени восстановления

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Пояснение: RTO — это фундаментальный параметр для планирования восстановительных работ. Он диктует, насколько быстро процедуры восстановления должны быть выполнены, и определяет выбор соответствующих технологий и решений (например, «холодное» или «горячее» резервирование). **Задание 5.10** Какой процедурный документ, подписываемый сотрудником, юридически закрепляет его обязанность не разглашать конфиденциальную информацию компании как во время работы, так и после увольнения? Ответ: Соглашение о конфиденциальности Пояснение: NDA является основной процедурно-правовой мерой управления персоналом в области ИБ. Он создает правовые основания для привлечения сотрудника к ответственности в случае разглашения им информации, что служит сдерживающим фактором и инструментом защиты интересов организации.
Тема 8 Криптографические методы защиты	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографичес	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований	**Задание 8.1** Какие из перечисленных утверждений являются корректными для симметричных криптосистем? Варианты ответов: а) Для шифрования и дешифрования используется один и тот же секретный ключ. б) Алгоритм RSA является классическим примером симметричной криптосистемы. в) Основная проблема — безопасная доставка секретного ключа сторонам. г) Они, как правило, работают медленнее, чем асимметричные системы при

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
	кой культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	информационной безопасности на базовом уровне	шифровании больших объемов данных. Ответ: а, в. Пояснение: ответ "а" - это прямое определение симметричного шифрования. Ответ "в", "Проблема распределения ключей" — это ключевой недостаток симметричных систем, так как ключ должен быть передан по защищенному каналу. **Задание 8.2** Какие из перечисленных алгоритмов являются блочными шифрами? Варианты ответов: а) AES (Advanced Encryption Standard) б) Шифр Цезаря в) ГОСТ 34.12-2015 ("Кузнечик" или "Магма") г) RSA Ответ: а, в. Пояснение: ответ "а". AES — это современный стандарт блочного шифрования. Ответ "в", ГОСТ 34.12-2015 — это российский стандарт, определяющий блочные шифры "Кузнечик" и "Магма". **Задание 8.3** Установите последовательность этапов работы сети Фейштеля для одного раунда при шифровании блока данных. Этапы: 1. Применение раундовой функции F к правой половине блока и раундовому ключу.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			2. Наложение результата функции F на левую половину блока с помощью операции XOR. 3. Разбиение входного блока на две равные части (L и R). 4. Обмен местами полученных половин (новые L и R). Ответ: 3,1,2,4 Пояснение: Это классическая структура раунда Фейштеля. Сначала блок разбивается (3). Затем к правой части R и ключу применяется функция F (1). Ее результат складывается по XOR с левой частью L (2). В конце раунда половинки меняются местами (4), чтобы результат функции F повлиял на следующий раунд. **Задание 8.4** Расположите алгоритмы шифрования в хронологическом порядке их создания/стандартизации (от самого старого к самому новому). Алгоритмы: 1. AES (Advanced Encryption Standard) 2. DES (Data Encryption Standard) 3. Шифр Цезаря 4. ГОСТ 28147-89 (предшественник ГОСТ 34.12-2015) Ответ: 3,2,4,1 Пояснение: Шифр Цезаря — античный шифр (I в. до н.э.). DES — разработан в 1970-х и утвержден как стандарт в 1977 г. ГОСТ 28147-89 — советский/российский стандарт, введенный в 1989 г. AES — стал новым американским стандартом в 2001 г., сменив DES. **Задание 8.5**

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Установите соответствие между криптографическим понятием и его определением. Список 1 (Понятие): 1. Исходный текст 2. Криптостойкость 3. Ключ 4. Шифротекст Список 2 (Определение): А. Секретная информация, определяющая результат работы шифрующего алгоритма. Б. Устойчивость шифра к криптоанализу, то есть его способность противостоять попыткам дешифрования. В. Данные, полученные после применения шифра. Г. Исходные, незашифрованные данные, подлежащие защите. Ответ: 1Г, 2Б, 3А, 4В **Задание 8.6** Установите соответствие между алгоритмом шифрования и его ключевой характеристикой. Список 1 (Алгоритм): 1. DES 2. AES 3. RSA 4. ГОСТ 34.12-2015 ("Кузнечик") Список 2 (Характеристика):

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			А. Симметричный блочный шифр с длиной блока 128 бит и переменной длиной ключа (128, 192, 256). Б. Симметричный блочный шифр с длиной блока 64 бита и ключом 56 бит, устаревший из-за малой длины ключа. В. Асимметричный алгоритм, стойкость которого основана на сложности факторизации больших чисел. Г. Российский стандарт симметричного блочного шифра с длиной блока 128 бит. Ответ: 1Б, 2А, 3В, 4Г **Задание 8.7** На чем основана криптографическая стойкость алгоритма RSA? Варианты ответов: а) На сложности решения задачи дискретного логарифмирования в конечном поле. б) На сложности инвертирования блочной сети Фейштеля без знания ключа. в) На сложности факторизации больших чисел, являющихся произведением двух простых чисел. г) На сложности вскрытия шифра простой замены частотным анализом. Ответ: в) Пояснение: ответ "в" - это фундаментальное положение RSA. Открытый ключ — это произведение двух больших простых чисел, а секретный ключ — одно из них. Задача взлома — найти эти простые множители, что является вычислительно сложной задачей для достаточно больших чисел. **Задание 8.8** Какой из перечисленных алгоритмов является асимметричным?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Варианты ответов: а) AES (Advanced Encryption Standard) б) ГОСТ 34.12-2015 ("Кузнечик") в) DES (Data Encryption Standard) г) RSA (Rivest–Shamir–Adleman) Ответ: г) Пояснение: ответ "г", RSA — это классический и наиболее известный асимметричный алгоритм, использующий пару ключей: открытый и закрытый. **Задание 8.9** Как называется основной метод криптоанализа, используемый для вскрытия шифров простой замены (например, шифра Цезаря), основанный на статистике появления символов в языке? Ответ: Частотный анализ / Frequency analysis. Пояснение: Это фундаментальный метод, использующий тот факт, что в любом естественном языке буквы и сочетания букв встречаются с определенной, predictable частотой. Сопоставляя частоту символов в шифротексте с эталонной частотой для языка, криптоаналитик может восстановить исходный текст. **Задание 8.10** Как называется архитектура (структура), используемая во многих блочных шифрах (например, в DES), которая разделяет блок на две части и обрабатывает их за несколько раундов с использованием раундовых ключей и специальной функции?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Ответ: Сеть Фейштеля / Feistel network. Пояснение: Сеть Фейштеля — это фундаментальная конструкция в криптографии. Ее ключевое преимущество заключается в том, что процессы шифрования и дешифрования практически идентичны, что упрощает реализацию как в аппаратном обеспечении (hardware), так и в программном обеспечении (software). Алгоритм DES является самым известным шифром, построенным на этой сети.
Тема 10 Экранирование. Тунелирование	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	**Задание 10.1** Какие из перечисленных функций относятся к основным задачам межсетевого экрана (firewall)? Варианты ответов: а) Шифрование всего исходящего интернет-трафика для обеспечения конфиденциальности. б) Блокирование несанкционированного доступа извне в защищаемую сеть. в) Контроль и фильтрация сетевого трафика на основе заданных правил. г) Защита от вирусов и вредоносного ПО на уровне содержимого файлов. Ответ: б, в. Пояснение: ответ "б" верный, так как это одна из первичных задач firewall — создание барьера между доверенной (внутренней) и недоверенной (внешней) сетью. Ответ "в" верный, потому что это базовая функция любого МЭ: анализ пакетов и принятие решения (пропустить/отклонить) на основе политики безопасности. **Задание 10.2** Какие из перечисленных технологий или протоколов используются для построения Виртуальных Частных Сетей (VPN)?

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Варианты ответов: а) IPsec (Internet Protocol Security) б) SMTP (Simple Mail Transfer Protocol) в) OpenVPN г) DNS (Domain Name System) Правильные ответы: а, в. Пояснение: ответ "а", IPsec — это стандартный набор протоколов для обеспечения безопасного обмена пакетами на сетевом уровне, широко используемый для VPN. Ответ "в", OpenVPN — это популярная реализация VPN с открытым исходным кодом, использующая библиотеки SSL/TLS **Задание 10.3** Установите последовательность обработки сетевого пакета классическим сетевым экраном с фильтрацией пакетов (packet filter). Этап обработки: 1. Принятие решения: пропустить пакет или отбросить. 2. Проверка пакета на соответствие правилам в списке контроля доступа (ACL). 3. Получение пакета на интерфейс. 4. Передача пакета целевому узлу в случае положительного решения. Ответ: 3,2,1,4 Пояснение: Сначала пакет поступает на интерфейс (3). Затем МЭ анализирует его заголовки (IP, порты, флаги) на соответствие правилам (2). На основе этого анализа принимается решение (1), и если оно положительное, пакет передается дальше (4).

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Задание 10.4 Расположите виды межсетевых экранов в порядке их появления и эволюции (от самого простого к более сложному). Виды экранов: 1. Межсетевой экран прикладного уровня (proxy) 2. Межсетевой экран с фильтрацией пакетов 3. Межсетевой экран нового поколения (NGFW) 4. Межсетевой экран с проверкой на уровне сессии (stateful inspection) Ответ: 2,4,1,3 Пояснение: Эволюция шла от простой фильтрации пакетов (2) к более умной stateful inspection (4), которая учитывает состояние соединений. Затем появились шлюзы прикладного уровня (1) для глубокого анализа конкретных сервисов. Современным этапом являются NGFW (3), объединяющие все предыдущие функции и добавляющие анализ содержимого и идентификацию приложений. **Задание 10.5** Установите соответствие между типом межсетевого экрана и его ключевым принципом работы. Список 1 (Тип МЭ): 1. Фильтрация пакетов (Packet Filter) 2. Stateful Inspection 3. Шлюз прикладного уровня (Application Proxy) 4. МЭ нового поколения (NGFW) Список 2 (Принцип работы):

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			А. Анализирует заголовки пакетов (IP-адреса, порты) без учета состояния соединения. Б. Анализирует трафик в контексте состояния соединений и может идентифицировать конкретные приложения. В. Полностью terminates и инициирует соединения от имени конечных узлов, анализируя данные на уровне приложений. Г. Отслеживает состояние активных соединений (например, по таблице состояний) и принимает решения на основе контекста. Ответ: 1А, 2Г, 3В, 4Б **Задание 10.6** Установите соответствие между понятием и его определением в контексте экранирования и туннелирования. Список 1 (Понятие): 1. Экранирование 2. Туннелирование 3. VPN 4. Демилитаризованная зона (DMZ) Список 2 (Определение): А. Метод инкапсуляции пакетов одного протокола в пакеты другого для их передачи по чужеродной сети. Б. Виртуальная сеть, создаваемая поверх другой сети (например, Интернет) с целью обеспечения конфиденциальности и целостности передаваемых данных. В. Размещение ресурсов, требующих ограниченного доступа извне, в изолированном сегменте сети. Г. Метод защиты сети, предполагающий установку барьера между различными сегментами сети для контроля и фильтрации трафика.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			Ответ: 1Г, 2А, 3Б, 4В **Задание 10.7** Какой основной принцип лежит в основе работы межсетевого экрана с Stateful Inspection? Варианты ответов: а) Анализ только IP-адресов источника и назначения в каждом пакете по отдельности. б) Полное завершение на себе всех соединений и анализ данных на уровне приложений. в) Принятие решений на основе таблицы состояний активных соединений. г) Шифрование всего трафика, проходящего через устройство. Ответ: в) Пояснение: ответ "в" верный, так как ключевое отличие Stateful Inspection от простой фильтрации пакетов — это ведение таблицы состояний (state table). МЭ запоминает инициированные изнутри соединения и разрешает обратный трафик, относящийся к этим сессиям, даже без явного правила. **Задание 10.8** Какой из перечисленных протоколов работает на сетевом уровне (уровне 3 OSI) и является стандартом для построения защищенных VPN? Варианты ответов: а) SSL/TLS б) PPTP в) IPsec

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовой вариант контрольной работы
			г) HTTP Ответ: в) Пояснение: ответ "в" верный, так как IPsec работает на сетевом уровне, обеспечивая "прозрачную" защиту для всех вышележащих протоколов. Это отраслевой стандарт для VPN типа "сеть-сеть" и удаленного доступа. **Задание 10.9** Как называется сегмент сети, расположенный между внутренней (доверенной) и внешней (недоверенной) сетью, в котором обычно размещаются общедоступные серверы (веб, почта)? Ответ: Демилитаризованная зона / DMZ. Пояснение: DMZ — это классическая архитектурная концепция экранирования. Она позволяет предоставить ограниченный доступ к публичным сервисам, не подвергая прямому риску всю внутреннюю сеть. Доступ в DMZ и из нее строго контролируется правилами межсетевого экрана. **Задание 10.10** Как называется технология, которая позволяет инкапсулировать трафик одного протокола (например, IP) внутри пакетов другого протокола для создания защищенного канала через общедоступную сеть? Ответ: Туннелирование / Tunneling. Пояснение: Туннелирование — это фундаментальный принцип, лежащий в основе VPN. Оно создает "виртуальный кабель" поверх небезопасной сети (например, Интернета), внутри которого передаются защищенные пакеты. Примеры: IPsec-туннель, SSL-туннель, GRE-туннель.

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 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 3 Стандарты и спецификации в области информацио	ОПК-3 Способен решать стандартные задачи профессионал	**И О П К - 3 . 1 .** Знать принципы, методы и средства решения	**Задание 1:** Подготовьте реферат на тему: “Оценочные стандарты и технические спецификации” Что должно быть отражено

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
нной безопасности	ьной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи	Оценочный стандарт ГОСТ Р ИСО/МЭК 15408 `Общие критерии оценки безопасности информационных технологий`. Введение и общая модель. Функциональные компоненты безопасности. Компоненты доверия к безопасности. Сопутствующие документы. Управленческие стандарты информационной безопасности. ГОСТ Р ИСО/МЭК 17799 `Информационные технологии. Практические правила управления информационной безопасностью`. ГОСТ Р ИСО/МЭК 27001 `Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования`. **Задание 2:** Подготовьте реферат на тему: “Руководящие документы Гостехкомиссии России” Что может быть отражено: Приказ председателя Гостехкомиссии России от 19 июня 2002 г. №187 Решение председателя Гостехкомиссии России от 30 марта 1992 г. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» Положение о сертификации средств защиты информации по требованиям безопасности информации

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
		профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	
Тема 6 Идентификация и аутентифика	ОПК-3 Способен решать стандартные задачи профессионал	**ИОПК-3.1.** Знать принципы, методы и средства решения	**Задание 1:** Подготовьте реферат на тему:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
ция	ьной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи	“Идентификация и аутентификация” Что может быть отражено: Определение идентификации и аутентификации.Парольная аутентификация. Требования к паролям.Одноразовые пароли. **Задание 2:** Подготовьте реферат на тему: “Алгоритмы создания одноразовых паролей” Что может быть отражено: Принцип работы OTP Алгоритмы генерации OTP. Например: TOTP (Time-based One-Time Password Algorithm) — генерирует последовательность одноразовых паролей на основе текущего времени и секретного ключа. HMAC-основанный OTP (HOTP) — генерирует последовательность одноразовых паролей на основе секретного ключа и значения счётчика. HOTP через SMS или электронную почту — уникальный пароль генерируется сервером и отправляется пользователю через SMS или электронную почту, затем пользователь вводит этот пароль для аутентификации. **Задание 3:** Подготовьте реферат на тему: “Социальный инжиниринг.”

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
		профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	Что может быть отражено: Введение термина — он был впервые введён в 1960-х годах группой социологов, изучавших способы воздействия на людей с целью изменения их поведения. Использование социальной инженерии в разных сферах — например, в начале XX века её применяли правительства и бизнес для продвижения собственных целей, в 1970-х годах — в преступных целях. Распространение с появлением интернета — поддельные веб-сайты и электронные письма, которые выглядели законными, усыпляли бдительность пользователей.
Тема 10 Экранирование. Тунелирован	ОПК-3 Способен решать стандартные задачи	**ИОПК-3.1.** Знать принципы, методы и средства	**Задание 1:** Подготовьте реферат на тему:

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
ие	профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные	“Экранирование” Что может быть отражено: Понятие экранирования. Межсетевые экраны. Классификация межсетевых экранов. Виды межсетевых экранов. **Задание 2:** Подготовьте реферат на тему: “Тунелирование” Что может быть отражено: Понятие тунелирования. Виртуальные частные сети. VPN IPsec, PPTP. Разработка конфигурации межсетевого экрана.

Тема	Код и формулировка компетенции	Индикаторы достижения компетенции	Типовое задание для самостоятельной работы
		задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне	

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

4.5. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ КУРСОВЫХ РАБОТ

Курсовые работы не предусмотрены

Курсовая работа позволяет выявить степень владения базовыми знаниями, умениями и навыками, необходимыми для обучения, и определить уровень владения новым материалом.

Примерные индивидуальные задания (темы) для курсовых работ:

Критерии оценивания курсовой работы:

Оценка	Критерии оценивания
отлично	Содержание курсовой работы полностью соответствует заданию, содержащемуся в методических указаниях, и плану. Представлены результаты структурированного и логически последовательного обзора литературных и иных источников по теме исследования. Структура курсовой работы логически и методически выдержана. Верно определены исходные данные для расчетов. Все аналитические расчеты выполнены верно, корректно применены методы экономического анализа, не нарушена методика анализа предмета исследования. Все выводы и предложения убедительно аргументированы. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
хорошо	Содержание курсовой работы полностью соответствует заданию, содержащемуся в методических указаниях, и плану. Представлены результаты структурированного и логически последовательного обзора литературных и иных источников по теме исследования. Структура курсовой работы логически и методически выдержана. Верно определены исходные данные для расчетов. В расчетах допускаются незначительные (не искажающие общего итога оценки) погрешности/ошибки. Большинство выводов и предложений аргументировано, корректно применены методы экономического анализа, не нарушена методика анализа предмета исследования. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах, в оформлении таблиц. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и

	выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
удовлетворительно	Содержание курсовой работы полностью соответствует заданию, содержащемуся в методических указаниях, и плану. Результаты обзора литературных и иных источников представлены недостаточно полно, недостаточно логично и последовательно. Верно определены исходные данные для расчетов, но имеются грубые ошибки в расчетах. Аргументация выводов и предложений слабая или отсутствует. Экономические выводы носят констатирующий (описательный) характер. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
неудовлетворительно	Содержание курсовой работы не соответствует заданию, содержащемуся в методических указаниях, и плану. Неверно определены исходные данные для расчетов, неверно и не корректно применены методы экономического анализа. Экономические выводы содержат неверную экономическую оценку. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала, студент не может защитить свои решения, допускает грубые фактические ошибки при ответах на поставленные вопросы или вовсе не отвечает на них. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы

5. МАТЕРИАЛЫ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация проводится в форме зачета/зачета с оценкой/экзамена.

5.1. Вопросы к зачету:

1. Основы информационной безопасности: понятие, цели и задачи.
2. Угрозы информационной безопасности и их классификация.
3. Методы и средства защиты информации.
4. Криптографические методы защиты информации.
5. Сетевые технологии и информационная безопасность.
6. Безопасность операционных систем и приложений.
7. Антивирусная защита и её роль в обеспечении информационной безопасности.
8. Управление доступом и аутентификация пользователей.

9. Резервное копирование и восстановление данных.
10. Законодательство и стандарты в области информационной безопасности.
11. Социальная инженерия как метод реализации угроз информационной безопасности.
12. Модели безопасности: дискреционная (DAC), мандатная (MAC), ролевая (RBAC) и атрибутная (ABAC).
13. Обнаружение и предотвращение вторжений (IDS/IPS): принципы работы и применение.
14. Безопасность беспроводных сетей (Wi-Fi, Bluetooth, мобильные сети).
15. Защита персональных данных: принципы, методы и требования законодательства (на примере ФЗ-152).
16. Инциденты информационной безопасности: классификация, расследование и реагирование.
17. Аудит и мониторинг информационных систем: цели, методы и инструменты.
18. Безопасность облачных вычислений (IaaS, PaaS, SaaS): риски и модели ответственности.
19. Проблемы безопасности в Интернете вещей (IoT) и встроенных системах.
20. Цифровая подпись и электронная аутентификация: технологии и применение.
21. Средства обеспечения конфиденциальности: шифрование данных на диске, в транзите и в памяти.
22. Политики информационной безопасности организации: разработка, внедрение и контроль.
23. Безопасность веб-приложений: типичные уязвимости (OWASP Top 10) и методы защиты.
24. Фишинг, спуфинг и другие виды мошенничества в цифровой среде.
25. Этический хакинг и тестирование на проникновение (penetration testing).
26. Защита корпоративной сети: межсетевые экраны, шлюзы, сегментация и DMZ.
27. Управление уязвимостями и патч-менеджмент в ИТ-инфраструктуре.
28. Кибербезопасность критически важных информационных инфраструктур (КИИ).
29. Международные стандарты информационной безопасности (ISO/IEC 27001, NIST, COBIT).
30. Будущие вызовы информационной безопасности: квантовые вычисления, ИИ и децентрализованные технологии.

Критерии оценивания зачета с оценкой/экзамена:

Оценка	**Критерии оценивания**
зачтено	Обучающийся должен: уметь строить ответ в соответствии со структурой излагаемого вопроса; продемонстрировать прочное, достаточно полное усвоение знаний программного материала; продемонстрировать знание основных теоретических понятий; правильно формулировать определения; последовательно, грамотно и логически стройно изложить теоретический материал; продемонстрировать умения самостоятельной работы с литературой; уметь сделать достаточно обоснованные выводы по излагаемому материалу.
не зачтено	Обучающийся демонстрирует: незнание значительной части программного материала; не владение понятийным аппаратом дисциплины; существенные ошибки при изложении учебного материала; неумение строить ответ в соответствии со структурой излагаемого вопроса; неумение делать выводы по излагаемому материалу.

Критерии оценивания зачета с оценкой/экзамена:

Оценка	Критерии оценивания
отлично	Выставляется, если обучающимся правильно и полностью раскрыто содержание материала в пределах программы, чётко и правильно даны определения и раскрыто содержание понятий, точно использованы научные и технические термины, в ответе использованы ранее приобретённые теоретические знания, сделаны необходимые выводы и обобщения
хорошо	Выставляется, если обучающимся раскрыто основное содержание материала в пределах программы, даны определения и раскрыто содержание понятий, в ответе использованы ранее приобретённые теоретические знания, сделаны необходимые выводы и обобщения, но присутствуют незначительные нарушения в последовательности изложения, имеются одна-две неточности в содержании ответа
удовлетворительно	Выставляется, если обучающимся содержание учебного материала изложено фрагментарно, не всегда последовательно, не даны определения, не раскрыто содержание понятий, или они изложены с ошибками, допускаются ошибки и неточности в использовании научной терминологии, отсутствуют выводы и обобщения из предыдущего материала, или возможны ошибки в их изложении
неудовлетворительно	Выставляется, если обучающимся основное содержание учебного материала не раскрыто, не даются ответы на основные вопросы, допускаются грубые ошибки в определении понятий, в использовании терминологии, отсутствуют выводы и обобщения

6. 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

№ п/п	Тема занятия	Код компетенции	Индикатор	Тип задания	Задание		Уровень освоения компетенции
					Вариант 1	Вариант 2	
1	**Тема 1** Введение в информационную безопасность	**УК-10** Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИУК-10.1.** Знать природу экстремизма, терроризма, коррупционного поведения как социально-правового явления. Понимать общественную опасность экстремизма, терроризма, коррупционного поведения во всех их проявлениях, последствия и необходимость противодействия им **ИУК-10.2.** Уметь реализовывать средства обеспечения законности и правопорядка в сфере противодействия экстремизма, терроризма, коррупционному поведению	1,1	**1.** Установите соответствие между основным принципом построения систем защиты АИС и его содержанием. Список 1 (Принцип): 1. Принцип "простота контроля" 2. Принцип минимальных привилегий 3. Принцип неотвратимости наказания 4. Принцип комплексности защиты Список 2 (Содержание): А. Каждый пользователь должен иметь доступ только к тем ресурсам, которые необходимы для его прямых обязанностей. Б. Защита должна охватывать все компоненты АИС и все этапы информационного процесса. В. Механизмы безопасности должны быть максимально простыми для анализа и тестирования. Г. Любое нарушение политики безопасности должно фиксироваться и влечь за собой адекватные меры ответственности.	**1.** Установите соответствие между задачей системы информационной безопасности и мерой по ее реализации. Список 1 (Задача): 1. Защита от несанкционированного доступа (НСД) 2. Обнаружение инцидентов безопасности 3. Обеспечение аутентификации 4. Противодействие вредоносному программному обеспечению Список 2 (Мера): А. Внедрение системы двухфакторной аутентификации. Б. Установка и настройка антивирусного ПО и средств защиты от эксплойтов. В. Развертывание системы обнаружения вторжений (IDS/SIEM). Г. Настройка правил маршрутизации на межсетевом экране и использование механизмов контроля доступа. Ответ: 1Г, 2В, 3А, 4Б	**Базовый (1-3 минуты)**

					Ответ: 1В, 2А, 3Г, 4Б		
2	**Тема 2** Законодательный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	**ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИУК-10.1.** Знать природу экстремизма, терроризма, коррупционного поведения как социально-правового явления. Понимать общественную опасность экстремизма, терроризма, коррупционного поведения во всех их проявлениях, последствия и необходимость	4,4	**2.** Какие из перечисленных правовых актов являются в Российской Федерации специальными законами, непосредственно регулирующими отношения в сфере информационной безопасности? Варианты ответов: а) Гражданский кодекс РФ (часть 4). б) Федеральный закон «О персональных данных». в) Федеральный закон «Об информации, информационных технологиях и о защите информации». г) Трудовой кодекс РФ. Ответ: б, в. Пояснение: ответы "б" (ФЗ «О персональных данных») и "в" (ФЗ «Об информации, информационных технологиях и о защите информации») — это профильные («специальные») законы, целиком посвященные регулированию вопросов обработки информации и ее защиты.	**2.** В соответствии с Федеральным законом «О персональных данных», какие из перечисленных действий оператор обязан совершить до начала обработки персональных данных? Варианты ответов: а) Получить письменное согласие субъекта персональных данных на их обработку (за исключением случаев, предусмотренных законом). б) Уведомить уполномоченный орган (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. в) Назначить лицо, ответственное за организацию обработки персональных данных. г) Провести классификацию информационной системы персональных данных. Ответ: а, б. Пояснение: ответ "а" (Получение согласия) — это одно из ключевых оснований для правомерной обработки ПДн, прямо предусмотренное законом. Ответ "б"	**Повышенный (3-5 минут)**

			противодействия им **ИУК-10.2.** Уметь реализовывать средства обеспечения законности и правопорядка в сфере противодействия экстремизма, терроризма, коррупционному поведению			(Уведомление Роскомнадзора) — обязательная процедура для большинства операторов перед началом обработки, за некоторыми исключениями (например, обработка данных сотрудников).	
3	**Тема 3** Стандарты и спецификации в области информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на основе	2,2	**3.** Установите последовательность основных этапов цикла PDCA (Деминга) в контексте построения СМИБ согласно ГОСТ Р ИСО/МЭК 27001. Этапы: 1. Act (Воздействие) — предпринимать корректирующие и предупреждающие действия для постоянного улучшения СМИБ. 2. Plan (Планирование) — создавать политики, цели, процессы и меры управления, относящиеся к управлению рисками. 3. Do (Внедрение) — реализовывать процессы и меры управления ИБ. 4. Check (Проверка) —	**3.** Расположите в логической последовательности этапы работы с «Общими критериями» (ГОСТ Р ИСО/МЭК 15408). Этапы: 1. Выбор компонентов доверия к безопасности (например, уровень тестирования AVA_VAN). 2. Определение целевых показателей безопасности (Security Target) для конкретного продукта. 3. Выбор функциональных компонентов безопасности из каталога стандарта (например, FIA_UAU – аутентификация пользователя). 4. Формулирование целей безопасности для продукта и предположений о среде.	**Базовый (1-3 минуты)**

			информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		контролировать и анализировать performance процессов ИБ. Ответ: 2341 Пояснение: Классический цикл непрерывного улучшения начинается с Планирования (Plan), затем следует Внедрение (Do), далее Проверка (Check) эффективности внедренного, и завершается цикл Воздействием (Act) для корректировки и улучшения.	Ответ: 4312 Пояснение: Сначала определяются общие цели безопасности и предположения (4). На их основе выбираются конкретные функциональные требования (3) и требования доверия (1) из каталогов стандарта. Весь этот комплект требований оформляется в Заявлении о безопасности (Security Target) (2), который является основным документом для оценки.	
4	**Тема 4** Административный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь	3,3	**4.** Что из перечисленного является основной целью Политики информационной безопасности верхнего уровня? Варианты ответов: а) Детально описать настройки всех сетевых устройств. б) Продемонстрировать клиентам использование передовых технологий шифрования. в) Формально определить ответственность руководства и общие направления обеспечения ИБ в организации. г) Заложить основы для	**4.** Какой принцип является наиболее важным для успешной синхронизации программы безопасности с жизненным циклом систем? Варианты ответов: а) Принцип «безопасность как неотъемлемая часть процесса» (Security by Design). б) Принцип простоты контроля. в) Принцип минимальных привилегий. г) Принцип разделения обязанностей. Ответ: а)	**Повышенный (3-5 минут)**

			решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		последующей сертификации по международным стандартам. Ответ: в) Пояснение: ответ "в" - это прямая и первичная цель политики верхнего уровня: закрепить приверженность руководства, распределить ответственность и задать стратегический курс.	Пояснение: ответ "a", Security by Design — это краеугольный камень интеграции ИБ в ЖЦ. Он означает, что вопросы безопасности рассматриваются не постфактум, а на самых ранних этапах (проектирование, разработка), что значительно эффективнее и дешевле.	
5	**Тема 5** Процедурный уровень информационной безопасности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные	5,5	**5.** Как называется ключевой количественный показатель плана восстановления, который определяет максимально допустимое время простоя информационной системы или бизнес-процесса после сбоя? Ответ: Цель по времени восстановления Пояснение: RTO — это фундаментальный параметр для планирования восстановительных работ. Он диктует, насколько быстро процедуры восстановления должны быть выполнены, и	**5.** Какой процедурный документ, подписываемый сотрудником, юридически закрепляет его обязанность не разглашать конфиденциальную информацию компании как во время работы, так и после увольнения? Ответ: Соглашение о конфиденциальности Пояснение: NDA является основной процедурно-правовой мерой управления персоналом в области ИБ. Он создает правовые основания для привлечения сотрудника к ответственности в случае разглашения им информации,	**Высокий (5-10 минут)**

			задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		определяет выбор соответствующих технологий и решений (например, «холодное» или «горячее» резервирование).	что служит сдерживающим фактором и инструментом защиты интересов организации.	
6	**Тема 6** Идентификация и аутентификация	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи	5,5	**6.** Как называется компонент в системе Kerberos, который выдает билеты для доступа к конкретным сетевым сервисам после того, как клиент предъявит ему TGT (Ticket-Granting Ticket)? Ответ: Сервер выдачи билетов (Ticket Granting Server (TGS)) Пояснение: TGS — это одна из двух основных частей KDC (наряду с AS — Authentication Server). Его роль — предоставлять доступ к сервисам, не требуя повторного ввода пароля пользователя, что реализует концепцию Single Sign-On (SSO) в рамках	**6.** Какой термин описывает статистическую ошибку биометрической системы, при которой она не распознает зарегистрированного законного пользователя (ложный отказ в доступе)? Ответ: Ложный отказ (False Rejection Rate (FRR)) Пояснение: FRR — это один из двух ключевых показателей эффективности биометрической системы (наряду с FAR — False Acceptance Rate). Высокий FRR снижает удобство использования, так как законные пользователи часто сталкиваются с проблемами при аутентификации.	**Высокий (5-10 минут)**

			профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		домена Kerberos.	Настройка системы часто представляет собой поиск баланса между FRR и FAR.	
7	**Тема 7** Управление доступом. Протоколирование и аудит	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи профессиональной	4,4	**7.** Какие из перечисленных свойств являются корректными для модели Белла-ЛаПадулы? Варианты ответов: а) Основная цель — предотвращение утечки информации к субъектам с более низким уровнем допуска. б) Модель является разновидностью дискреционного управления доступом (DAC). в) Модель формально описывает два свойства: «No Read Up» и «No Write Down». г) Владелец объекта может по своему усмотрению передать права доступа другому субъекту.	**7.** Какие из перечисленных действий относятся к функциям активного аудита? Варианты ответов: а) Архивное хранение журналов событий в течение 5 лет. б) Немедленное оповещение администратора при обнаружении 5 неудачных попыток входа в систему за 1 минуту. в) Ежеквартальный анализ статистики событий для выявления аномалий. г) Автоматическая блокировка учетной записи при попытке доступа к файлу с повышенным уровнем секретности. Ответ: б, г.	**Повышенный (3-5 минут)**

			деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		Ответ: а, в. Пояснение: ответ "а" - это основная цель данной модели, разработанной для защиты государственных секретов. Ответ "в", «No Read Up» (простое свойство безопасности) и «No Write Down» (*-свойство) — это формальные правила, запрещающие чтение «сверху» и запись «вниз» по уровням классификации.	Пояснение: Ответ "б", мгновенное оповещение на основе анализа событий в реальном времени — ключевой признак активного аудита. Ответ "г", автоматическое реагирование (блокировка) на основе предопределенных правил — это высшая форма активного аудита, тесно связанная с системами IPS (Intrusion Prevention Systems).	
8	**Тема 8** Криптографические методы защиты	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи	2,2	**8.** Установите последовательность этапов работы сети Фейштеля для одного раунда при шифровании блока данных. Этапы: 1. Применение раундовой функции F к правой половине блока и раундовому ключу. 2. Наложение результата функции F на левую половину блока с помощью операции XOR. 3. Разбиение входного блока на две равные части (L и R). 4. Обмен местами полученных половин (новые L и R). Ответ: 3,1,2,4	**8.** Расположите алгоритмы шифрования в хронологическом порядке их создания/стандартизации (от самого старого к самому новому). Алгоритмы: 1. AES (Advanced Encryption Standard) 2. DES (Data Encryption Standard) 3. Шифр Цезаря 4. ГОСТ 28147-89 (предшественник ГОСТ 34.12-2015) Ответ: 3,2,4,1 Пояснение: Шифр Цезаря — античный шифр (I в. до н.э.). DES — разработан в 1970-х и	**Базовый (1-3 минуты)**

			профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		Пояснение: Это классическая структура раунда Фейштеля. Сначала блок разбивается (3). Затем к правой части R и ключу применяется функция F (1). Ее результат складывается по XOR с левой частью L (2). В конце раунда половинки меняются местами (4), чтобы результат функции F повлиял на следующий раунд.	утвержден как стандарт в 1977 г. ГОСТ 28147-89 — советский/российский стандарт, введенный в 1989 г. AES — стал новым американским стандартом в 2001 г., сменив DES.	
9	**Тема 9** Контроль целостности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи	1,1	**9.** Установите соответствие между понятием в области контроля целостности и ЭЦП и его определением. Список 1 (Понятие): 1. Хэш-функция 2. Цифровой сертификат 3. Электронная подпись 4. Коллизия хэш-функции Список 2 (Определение): А. Электронный документ, связывающий открытый ключ с данными о его владельце и заверенный подписью Удостоверяющего Центра. Б. Ситуация, когда двум разным наборам данных соответствует одинаковое значение хэша.	**9.** Установите соответствие между алгоритмом/стандартом и его областью применения. Список 1 (Алгоритм/Стандарт): 1. ГОСТ Р 34.11-2012 ("Стрибог") 2. SHA-256 3. ГОСТ Р 34.10-2012 4. X.509 Список 2 (Область применения): А. Стандарт на функцию хэширования (Россия). Б. Стандарт на электронную цифровую подпись (Россия). В. Стандарт на формат цифровых сертификатов. Г. Функция хэширования	**Базовый (1-3 минуты)**

			профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		В. Криптографическое преобразование, ставящее в соответствие произвольному массиву данных фиксированное значение хэша. Г. Реквизит электронного документа, позволяющий проверить его целостность и авторство. Ответ: 1В, 2А, 3Г, 4Б	(США, широко используется internationally). Ответ: 1А, 2Г, 3Б, 4В	
10	**Тема 10** Экранирование. Тунелирование	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи профессиональной	3,3	**10.** Какой из перечисленных протоколов работает на сетевом уровне (уровне 3 OSI) и является стандартом для построения защищенных VPN? Варианты ответов: а) SSL/TLS б) PPTP в) IPsec г) HTTP Ответ: в) Пояснение: ответ "в" верный, так как IPsec работает на сетевом уровне, обеспечивая "прозрачную" защиту для всех вышележащих протоколов. Это отраслевой стандарт для VPN типа "сеть-сеть" и	**10.** Как называется сегмент сети, расположенный между внутренней (доверенной) и внешней (недоверенной) сетью, в котором обычно размещаются общедоступные серверы (веб, почта)? Ответ: Демилитаризованная зона / DMZ. Пояснение: DMZ — это классическая архитектурная концепция экранирования. Она позволяет предоставить ограниченный доступ к публичным сервисам, не подвергая прямому риску всю внутреннюю сеть. Доступ в DMZ и из нее строго контролируется правилами межсетевого экрана.	**Повышенный (3-5 минут)**

			деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		удаленного доступа.		
11	**Тема 11** Анализ защищенности	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИОПК-3.1.** Знать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне **ИОПК-3.2.** Уметь решать стандартные задачи профессиональной деятельности на	4,4	**11.** Какие из перечисленных действий являются целями проведения анализа защищенности (security assessment)? Варианты ответов: а) Повышение производительности работы сетевого оборудования. б) Выявление уязвимостей в программном обеспечении и конфигурациях. в) Оценка соответствия системы требованиям политики информационной безопасности. г) Гарантированное устранение всех возможных уязвимостей. Правильные ответы: б, в. Пояснение: вариант "б"	**11.** Какие из перечисленных технологий являются основными методами детектирования для современных антивирусных программ? Варианты ответов: а) Сигнатурный анализ. б) Эвристический анализ. в) Сканирование портов. г) Проведение DDoS-атак на подозрительные серверы. Правильные ответы: а, б. Пояснение: вариант "а", сигнатурный анализ — это базовый метод, основанный на сравнении кода с базой известных сигнатур (отпечатков) вредоносных программ. Ответ "б", эвристический анализ — это	**Повышенный (3-5 минут)**

			основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учётом основных требований информационной безопасности на базовом уровне		верный, так как это прямая задача анализа защищенности — проактивный поиск слабых мест до того, как ими воспользуется злоумышленник. Ответ "в" верный, так как аудит и оценка соответствия стандартам и внутренним политикам — одна из ключевых целей анализа.	продвинутый метод, позволяющий обнаруживать новые, ранее неизвестные угрозы, путем анализа поведения и характеристик кода.	

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