Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.ДЭ.05.02 Информационный менеджмент

(индекс, наименование дисциплины в соответствии с учебным планом)

38.03.04 Государственное и муниципальное управление

(код, наименование направления подготовки/специальности)

Управление государственными проектами и программами

(наименование образовательной программы)

очная

(форма обучения)

Год набора 2026
Город Донецк

Автор(ы)-составитель(и) РПД:

Морозов Е.Л., канд. гос.упр., доцент, заведующий кафедры инновационного менеджмента и управления проектами

Заведующий кафедрой:

Морозов Е.Л., канд. гос.упр., доцент, заведующий кафедры инновационного менеджмента и управления проектами

Рабочая программа дисциплины *Информационный менеджмент* одобрена на заседании кафедры *инновационного менеджмента и управления проектами Факультета государственной службы и управления Донецкого филиала РАНХиГС*.

Протокол № 9 от «от 16 марта 2026 г.

СОДЕРЖАНИЕ

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

Дисциплина *Б1.В.01.ДЭ.05.02 Информационный менеджмент* обеспечивает формирование у обучающихся следующих компетенций:

ОТФ/ТФ и реквизиты ПС	Код компе-тенции	Наименование компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
Результаты форсайт-сессии (протокол от 13.03.2026)	ПК-1.	Способен осуществлять организационно-управленческую деятельность в сфере государственной политики, диагностировать ключевые проблемы социально-экономического развития государства, применять современные технологии организационно-управленческой деятельности	ПК-1.6	Использует современные цифровые платформы, сервисы и технологии в организационно-управленческой деятельности органов власти для повышения качества государственных услуг и эффективности внутренних процессов	ПК-1.6 З-1 Знать современные цифровые платформы, сервисы и технологии, применяемые в системе госуправления ПК-1.6 З-1 Знать цифровые инструменты управления проектами и задачи цифровой трансформации госуправления ПК-1.6 У-1 Уметь использовать цифровые платформы для сбора и анализа данных, а также для предоставления государственных услуг в электронном виде ПК-1.6 У-2 Уметь применять специализированное ПО и цифровые сервисы для планирования, мониторинга и контроля реализации проектов и внутренних административных процессов.

A/01.6 Разработка инвестиционного проекта 08.036 Специалист по работе с инвестиционными проектами (Приказ Минтруда № 497н от 23.09.2024)	ПК-2	Способен разрабатывать инвестиционный проект	ПК-2.6	Готовит производственный план	ПК-2.6 З.3 Знает основы работы в операционных системах ПК-2.6 З.4 Знает основы работы в прикладных программах по созданию презентаций и слайд-шоу ПК-2.6 З.5 Знает основные антивирусные программы ПК-2.6 З.6 Знает принципы организации данных в системах управления базами данных ПК-2.6 З.7 Знает порядок редактирования данных в системах управления базами данных ПК-2.6 У.1 Умеет управлять размещением цифровой информации, в том числе на дисковых хранилищах локальной и глобальной компьютерной сети ПК-2.6 У.2 Умеет формировать медиатеки для структурированного хранения и каталогизации цифровой информации ПК-2.6 У.3 Умеет применять подходы безопасной работы в информационно-телекоммуникационной сети «Интернет» (защита персональных данных, антивирусная защита, информационная гигиена) ПК-2.6 У.4 Умеет использовать системы управления базами

					данных для просмотра данных в электронных базах данных ПК-2.6 У.5 Умеет изменять данные электронной базы данных с использованием систем управления базами данных
A/01.6 Сбор и анализ первичной информации в рамках реализации проекта государственно-частного партнерства 08.041 Специалист в сфере управления проектами государственно-частного партнерства (Приказ Минтруда России от 20.07.2020 № 431н)	ПК-3	Способен осуществлять сбор и анализ первичной информации в рамках реализации проекта государственно-частного партнерства	ПК-3.1	Осуществляет сбор и анализ исходных данных, необходимых для оценки реализуемости проекта государственно-частного партнерства	ПК-3.1 У.1 Умеет анализировать данные из множественных источников и оценивать качество и достоверность полученной информации по явным и неявным признакам ПК-3.1 У.2 Умеет применять программное обеспечение (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) для работы с информацией ПК-3.1 У.3 Умеет собирать, анализировать, систематизировать сведения и данные, документировать требования к проектам и процессам организации, их ресурсному окружению

2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины: 2,00 з.е., 72 ак. час., из них:
Лекции: 14 ак. час;
Практические: 14 ак. час;
Контактная работа на аттестацию в период экзаменационных сессий: 4 ак.час;
Итого ауд.: 32 ак. час;
Контактная работа: 28 ак. час;
Сам. работа: 40 ак. час;

Дисциплина *Б1.В.01.ДЭ.05.02 Информационный менеджмент* относится к вариативной части блока Б1 «Дисциплины (модули)» и является элективной дисциплиной 4-го уровня. Дисциплина реализуется на 4 курсе, в 7 семестре.

Предшествующие дисциплины: «Современные информационные технологии в социальных науках», «Информационные технологии в профессиональной деятельности», «Цифровые технологии в профессиональной деятельности» , «Статистика».

Последующие дисциплины:, «Проектно-технологическая практика».

Изучение дисциплины направлено на формирование профессиональных компетенций, необходимых для эффективного управления информационными ресурсами, информационными системами и технологиями в системе государственного и муниципального управления, а также для обеспечения информационной безопасности при реализации государственных проектов и программ.

3. Содержание и структура дисциплины

3.1. Структура дисциплины (*Очная форма обучения)*

№ п/п		Объем дисциплины, ак.час.											Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий							Самостоятельная работа			
			Период теоретического обучения				Период промежуточной аттестации (сессия)						
			Занятия лекционного типа	Занятия семинарского типа		КСР	КЭ	Каттэк	Контроль				
			Л	ЛР	ПЗ					СРкр	СРэк	СР	
Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента													
Тема 1.1	Информационный менеджмент: сущность, цели, задачи и место в системе государственного управления	15	2	0	2	0	0	0	0	0	0	6	Тестирование Кейс-задание Доклад/эссе
Тема 1.2	Информационные ресурсы, технологии и системы: классификация и архитектура	19	4	0	4	0	0	0	0	0	0	6	Тестирование Кейс-задание Доклад/эссе
Тема 1.3	Нормативно-правовое регулирование информационной безопасности и защиты персональных данных											5	
Раздел 2. Кибербезопасность и защита персональных данных в информационном менеджменте													
Тема 2.1.	Киберугрозы и система обеспечения информационной безопасности в государственных проектах	19	4	0	4	0	0	0	0	0	0	6	Тестирование Кейс-задание Решение задачи Доклад/эссе
Тема 2.2.	Организация защиты персональных данных в государственных информационных системах	19	4	0	4	0	0	0	0	0	0	6	Тестирование Кейс-задание Доклад/эссе
Тема 2.3.	Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография											6	

№ п/п		Объем дисциплины, ак.час.											Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий							Самостоятельная работа			
			Период теоретического обучения				Период промежуточной аттестации (сессия)						
			Занятия лекционного типа	Занятия семинарского типа		КСР	КЭ	Каттэк	Контроль				
			Л	ЛР	ПЗ					СРкр	СРэк	СР	
Тема 2.4.	Управление рисками информационной безопасности и реагирование на инциденты											5	
Промежуточная аттестация		4	0	0	0	0	0	4	0	0	0	40	Зачет
Итого:		**72**	**14**	**0**	**14**	**0**	**0**	**4**	**0**	**0**	**0**	**40**	

Используемые сокращения: Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях). ВЛ – видео лекции. ЛР – лабораторные работы. ПЗ – практические занятия (за исключением лабораторных работ). ИК – индивидуальные консультации. КСР – контроль самостоятельной работы КЭ – консультации перед экзаменом. Каттэк – контактная работа на аттестацию в период экзаменационных сессий. Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта. СРэк – самостоятельная работа на подготовку к экзамену.СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента

Тема 1.1. Информационный менеджмент: сущность, цели, задачи и место в системе государственного управления

Лекция 1.1. Информационный менеджмент как функция управления

На лекции рассматриваются понятие, цели и задачи информационного менеджмента, а также информация как стратегический ресурс современной организации. Изучаются предмет, объект и субъект информационного менеджмента. Анализируются основные функции информационного менеджмента: планирование информационной деятельности, организация информационных процессов, координация и контроль. Особое внимание уделяется современным трендам информационного менеджмента в государственном секторе, включая импортозамещение программного обеспечения, повышение цифровой зрелости органов власти и цифровую трансформацию государственного управления. Рассматривается взаимосвязь информационного менеджмента и проектного управления в органах власти, а также роль информационного менеджера в структуре государственного органа.

Практическое занятие 1.1. Анализ систем информационного менеджмента в государственном учреждении

На практическом занятии студенты анализируют информационную инфраструктуру реального государственного или муниципального учреждения (по выбору). Проводится выявление проблем информационного обеспечения управленческой деятельности, разрабатываются предложения по совершенствованию информационного менеджмента в органе власти. Итогом занятия является подготовка аналитической справки по результатам анализа, которая защищается перед аудиторией. В процессе работы используются методы системного анализа и экспертной оценки.

Тема 1.2. Информационные ресурсы, технологии и системы: классификация и архитектура

Лекция 1.2. Классификация и архитектура информационных систем

В ходе лекции раскрываются понятия информационных ресурсов, информационных технологий (ИТ) и информационных систем (ИС), а также их соотношение. Рассматривается классификация информационных систем: ERP-системы (управление предприятием), CRM-системы (управление взаимоотношениями с клиентами), системы электронного документооборота (СЭД), государственные информационные системы (ГИС), экспертные системы и системы поддержки принятия решений. Изучаются архитектуры информационных систем: файл-серверная, клиент-серверная (двухуровневая и трехуровневая), сервис-ориентированная архитектура (SOA). Анализируются вопросы выбора платформы и операционной системы для государственных ИС, включая сравнительный анализ Windows, Linux и отечественных операционных систем (Astra Linux, Ред ОС).

Практическое занятие 1.2. Проектирование архитектуры информационной системы для государственного проекта

На практическом занятии студенты разрабатывают техническое задание на создание информационной системы для реализации государственного проекта. Проводится обоснование выбора архитектуры ИС для конкретной задачи (на примере ГИС в социальной сфере). Осуществляется сравнительный анализ операционных систем для государственных информационных систем с учетом требований импортозамещения. Результаты работы представляются в виде презентации и защищаются перед аудиторией.

Тема 1.3. Нормативно-правовое регулирование информационной безопасности и защиты персональных данных

Лекция 1.3. Правовые основы и безопасность информационных систем

На лекции изучаются ключевые нормативные правовые акты в сфере информационной безопасности. Рассматривается Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», включая правовой режим информации,

ограничение доступа и создание государственных информационных систем. Детально анализируется Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: понятие персональных данных, принципы их обработки, согласие субъекта персональных данных, обязанности оператора. Изучаются требования ФСТЭК России и ФСБ России к защите информации в государственных информационных системах, а также Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Рассматриваются виды ответственности за нарушение законодательства о персональных данных (административная, уголовная, гражданско-правовая).

Практическое занятие 1.3. Разработка локальных актов по защите персональных данных

На практическом занятии студенты анализируют типовую модель угроз и акт определения уровня защищенности информационной системы персональных данных. Разрабатывают фрагмент Положения об обработке и защите персональных данных в организации. Составляют Политику оператора в отношении обработки персональных данных для размещения на официальном сайте. Готовят проект приказа о назначении лица, ответственного за организацию обработки персональных данных. Все разработанные документы обсуждаются и корректируются в группе.

Раздел 2. Кибербезопасность и защита персональных данных в информационном менеджменте

Тема 2.1. Киберугрозы и система обеспечения информационной безопасности в государственных проектах

Лекция 2.1. Классификация угроз информационной безопасности

В лекции раскрывается понятие угрозы информационной безопасности, рассматриваются источники угроз (антропогенные, техногенные, природные). Изучается классификация угроз по виду: угрозы конфиденциальности, целостности, доступности и права собственности. Особое внимание уделяется угрозам безопасности персональных данных: несанкционированный доступ, утечка, модификация, уничтожение. Анализируются современные киберугрозы для государственных информационных систем: DDoS-атаки, фишинг, вредоносное программное обеспечение, атаки на канальном и сетевом уровне (ARP-spoofing, MAC-spoofing, VLAN hopping). Рассматриваются принципы построения системы защиты информации в организации, включая правовые, организационные и технические меры.

Практическое занятие 2.1. Анализ угроз информационной безопасности для государственного проекта

На практическом занятии студенты идентифицируют актуальные угрозы для конкретной государственной информационной системы (по выбору). Строят модель угроз и оценивают вероятность их реализации. Разрабатывают перечень организационных и технических мер защиты. Решают кейс по выявлению уязвимостей в типовой ИТ-инфраструктуре государственного органа, используя методологию анализа защищенности и результаты моделирования угроз.

Тема 2.2. Организация защиты персональных данных в государственных информационных системах

Лекция 2.2. Правовой режим и организационные меры защиты персональных данных

На лекции изучаются категории персональных данных: общедоступные, специальные, биометрические и иные. Рассматривается правовой статус оператора персональных данных: права, обязанности, ответственность. Анализируется порядок получения согласия субъекта на обработку персональных данных, а также случаи обработки персональных данных без согласия. Изучается локальное нормативное регулирование обработки персональных данных в организации. Рассматривается понятие обезличивания персональных данных, методы обезличивания и требования Роскомнадзора. Анализируются правовые последствия нарушения требований к обработке персональных данных.

Практическое занятие 2.2. Разработка документов оператора персональных данных

На практическом занятии студенты разрабатывают форму согласия на обработку персональных данных (для работника, клиента, иного субъекта). Составляют перечень мер, направленных на обеспечение выполнения обязанностей оператора персональных данных. Готовят уведомление об обработке персональных данных в Роскомнадзор. Проводят анализ судебной практики по спорам, связанным с нарушением Федерального закона № 152-ФЗ «О персональных данных», и формулируют рекомендации для оператора.

Тема 2.3. Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография

Лекция 2.3. Технические меры защиты информации

В лекции рассматриваются межсетевые экраны (брандмауэры): их классификация, принципы работы, особенности конфигурации для государственных информационных систем. Изучаются системы обнаружения и предотвращения атак (IDS/IPS), включая сетевые и хостовые системы, сигнатурный и поведенческий анализ. Раскрываются вопросы использования средств криптографической защиты информации (СКЗИ): шифрование данных, электронная подпись, сертификация ФСБ России. Анализируются антивирусная защита, анализ защищенности, контроль доступа. Рассматриваются методы мониторинга безопасности сетей: снифферы, анализ сетевого трафика с использованием Wireshark, выявление аномалий.

Практическое занятие 2.3. Настройка средств защиты информации

На практическом занятии студенты анализируют конфигурацию межсетевого экрана для типовой государственной информационной системы. Знакомятся с работой системы обнаружения атак (на примере ViPNet IDS NS или доступного аналога). Проводят анализ перехваченного сетевого трафика и выявление признаков атак. Выполняют практическую работу по настройке антивирусной защиты и политик безопасности на условном сегменте государственной информационной системы.

Тема 2.4. Управление рисками информационной безопасности и реагирование на инциденты

Лекция 2.4. Риск-ориентированный подход к обеспечению информационной безопасности

На лекции раскрываются понятие и методы оценки рисков информационной безопасности, включая количественную и качественную оценку. Изучаются этапы управления рисками: идентификация, анализ, оценка, обработка, мониторинг. Рассматривается планирование реагирования на инциденты информационной безопасности, распределение ролей и ответственности. Анализируется порядок действий при утечке персональных данных: локализация инцидента, расследование, уведомление регуляторов (Роскомнадзора, ФСТЭК). Изучаются принципы построения рациональной системы защиты информации, обеспечивающей баланс между затратами на защиту и эффективностью мер.

Практическое занятие 2.4. Разработка плана реагирования на инциденты

На практическом занятии студенты разрабатывают модель угроз и проводят оценку рисков для государственного проекта. Составляют план реагирования на инциденты информационной безопасности (на примере утечки персональных данных). Выполняют расчет ожидаемой стоимости рисков и обосновывают бюджет на меры защиты. Проводится деловая игра «Реагирование на кибератаку в государственном проектном офисе», в ходе которой отрабатываются командные действия по локализации, расследованию и ликвидации последствий инцидента. Итогом является защита разработанного проектного решения.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также

«ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

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

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных. Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор. Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

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

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. Внимательно прочитать предложенные вариант-ты ответа. Выбрать один верный ответ. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. Внимательно прочитать предложенные вариант-ты ответа. Выбрать несколько правильных ответов. Записать только номера (или буквы) выбранного варианта ответа (например, 1 - 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. Внимательно прочитать предложенные варианты ответа. Построить верную последовательность из предложенных элементов. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр

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

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

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

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

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

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

5.1. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек): в ходе реализации дисциплины Б1.О.01.02.07 «Организационное поведение» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам): тестовые задания; кейс-задания; решение задач.

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

Раздел/Темы	ТЗ	КЗ
Р-1. / Т-1.1.	5	5
Р-1. / Т-1.2.	5	5
Р-1. / Т-1.3.	5	5
Р-2. / Т-2.1.	5	5
Р-2. / Т-2.2.	5	5
Р-2. / Т-2.3.	5	5
Р-2. / Т-2.4.	5	5
Итого: 70	**35**	**35**

ТЗ – тестовое задание; КЗ – кейс-задания; З -решение задачи, Д/Э – доклад/эссе

РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ И НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОГО МЕНЕДЖМЕНТА

Тема 1.1. Информационный менеджмент: сущность, цели, задачи и место в системе государственного управления

1.1.1. Тестовые задания

Задание 1

Расположите в логической последовательности этапы внедрения системы информационного менеджмента в органе государственной власти:

А) Разработка технического задания и выбор программного обеспечения.

Б) Анализ текущего состояния информационной инфраструктуры и выявление проблем.

В) Обучение персонала и ввод системы в эксплуатацию.

Г) Определение целей и задач информационного менеджмента.

Д) Оценка эффективности внедрения и корректировка.

Задание 2

Установите соответствие между функцией информационного менеджмента и её содержанием применительно к государственному органу:

Функция информационного менеджмента	Содержание функции
1. Формирование технологического ресурса	А. Повышение квалификации сотрудников в области ИТ и информационной безопасности
2. Управление персоналом	Б. Выбор архитектуры ИС, закупка оборудования и программного обеспечения
3. Обеспечение комплексной защищенности	В. Разработка стратегии развития информационной системы на 3-5 лет
4. Планирование в сфере обработки информации	Г. Аттестация объектов информатизации, установка средств криптографической защиты

Задание 3

Выберите **все верные** утверждения о роли информационного менеджмента в системе государственного и муниципального управления. **Кратко обоснуйте** каждый выбранный ответ.

а) Информационный менеджмент нацелен исключительно на автоматизацию бухгалтерского учёта в государственных учреждениях.

б) Одной из задач информационного менеджмента является обеспечение электронного документооборота между органами власти.

в) Информационный менеджмент не связан с проектным управлением и реализуется самостоятельно.

г) Внедрение информационного менеджмента способствует повышению открытости и прозрачности деятельности органов власти.

д) Информационный менеджмент не требует учета требований законодательства о персональных данных.

Задание 4

Какие три основных функции выполняет информационный менеджмент в государственном проектном офисе? Раскройте каждую из них и приведите пример реализации в конкретном государственном проекте.

Задание 5 (открытое)

Проанализируйте ситуацию: в региональном министерстве внедрена система электронного документооборота, однако 60% сотрудников продолжают распечатывать документы для визирования и используют бумажные носители. Руководитель проектного офиса связывает это с низкой цифровой грамотностью. Укажите не менее трёх возможных причин сложившейся ситуации (не связанных с обучением). Предложите комплекс организационных и управленческих решений.

1.1.2. Кейс-задания

Кейс 1. Внедрение СЭД в администрации муниципального района

В администрации муниципального района запущен проект по внедрению системы электронного документооборота (СЭД). Через 4 месяца после начала эксплуатации выяснилось, что руководители структурных подразделений не используют систему для согласования документов, ссылаясь на её неудобство и отсутствие интеграции с порталом госуслуг. Финансирование проекта освоено на 70%, но фактически система не работает.

Вопросы: 1) Какие ошибки были допущены на этапе планирования и внедрения информационной системы? 2) Какие функции информационного менеджмента не были реализованы? 3) Предложите план корректирующих мероприятий с указанием сроков и ответственных.

Кейс 2. Конфликт между ИТ-подразделением и профильными отделами

В государственном учреждении сложилась ситуация, когда ИТ-подразделение разрабатывает и внедряет информационные системы без участия профильных отделов. В результате системы не соответствуют реальным потребностям пользователей, а сотрудники профильных отделов отказываются работать с ними. Руководитель учреждения считает, что виноваты ИТ-специалисты.

Вопросы: 1) Как информационный менеджмент должен регулировать взаимодействие между ИТ-подразделением и пользователями? 2) Какая функция информационного менеджмента была проигнорирована? 3) Предложите регламент взаимодействия при разработке и внедрении информационных систем.

Кейс 3. Недостижение показателей «цифровой зрелости»

Регион отчитался о выполнении всех мероприятий по цифровой трансформации, однако показатель «цифровой зрелости» в сфере здравоохранения вырос лишь на 5% при плановых 20%. При этом бюджетные средства освоены полностью.

Вопросы: 1) Какие показатели эффективности информационного менеджмента, помимо освоения бюджета, следует оценивать? 2) Какие причины могли привести к такому расхождению? 3) Предложите систему KPI для оценки деятельности проектного офиса цифровой трансформации.

1.1.3. Темы докладов / эссе

1. Эволюция информационного менеджмента в системе государственного управления Российской Федерации.
2. Сравнительный анализ моделей информационного менеджмента в государственном и коммерческом секторах.
3. Роль информационного менеджера в структуре современного органа власти.
4. Взаимосвязь информационного менеджмента и проектного управления в реализации национальных проектов.
5. Зарубежный опыт информационного менеджмента в государственном секторе (Эстония, Сингапур, Великобритания).
6. Преодоление сопротивления персонала при внедрении информационных систем в государственных учреждениях.
7. Оценка эффективности информационного менеджмента: подходы, методы, показатели для государственных органов.

Тема 1.2. Информационные ресурсы, технологии и системы: классификация и архитектура

1.2.1. Тестовые задания

Задание 1

Расположите этапы создания государственной информационной системы (ГИС) в хронологической последовательности согласно жизненному циклу ИС:

А) Эксплуатация и сопровождение ГИС.

Б) Проектирование архитектуры и разработка технического задания.

В) Анализ потребностей и формирование требований.

Г) Внедрение и опытная эксплуатация.

Д) Тестирование и ввод в промышленную эксплуатацию.

Задание 2

Установите соответствие между типом информационной системы и её назначением в деятельности государственного органа:

Тип информационной системы	Назначение
1. ERP-система	А. Автоматизация документооборота и согласования

2. СЭД (система электронного документооборота)	Б. Управление взаимоотношениями с гражданами и организациями
3. CRM-система	В. Комплексное планирование ресурсов и бюджетирование
4. ГИС (государственная информационная система)	Г. Реализация государственных функций в электронном виде (ЕПГУ, ГИС ЖКХ)

Задание 3

Выберите **все верные** утверждения об архитектуре «клиент-сервер» применительно к государственным информационным системам. **Кратко обоснуйте** выбор.

а) При двухуровневой архитектуре вся бизнес-логика реализуется на стороне клиента («толстый клиент»), что упрощает администрирование.

б) Трехуровневая архитектура (клиент – сервер приложений – сервер БД) обеспечивает лучшую масштабируемость и безопасность.

в) Архитектура «файл-сервер» является наиболее предпочтительной для ГИС с большим количеством пользователей.

г) Использование сервис-ориентированной архитектуры (SOA) позволяет интегрировать разнородные государственные информационные системы.

д) Отечественные операционные системы (Astra Linux) не поддерживают клиент-серверную архитектуру.

Задание 4

Назовите не менее трёх критериев выбора платформы и операционной системы для государственной информационной системы. По каждому критерию поясните, почему он важен именно для государственных органов.

Задание 5 (открытое)

Сравните архитектуры «файл-сервер» и «клиент-сервер» с точки зрения безопасности, производительности и стоимости владения. Для какого типа государственных проектов (малое муниципальное учреждение vs федеральная ГИС) каждая из архитектур подходит лучше? Аргументируйте.

1.2.2. Кейс-задания

Кейс 1. Выбор архитектуры для регионального портала госуслуг

Регион планирует создать портал для записи граждан на приём в медицинские учреждения. Ожидаемая нагрузка – до 100 000 пользователей в день. Бюджет проекта ограничен, но требования к безопасности высокие, так как будут обрабатываться персональные данные и сведения о здоровье.

Вопросы: 1) Какую архитектуру информационной системы (двухуровневую, трёхуровневую, SOA) вы предложите? 2) Какие критерии выбора были определяющими? 3) Обоснуйте выбор операционной системы для серверов с учётом требований импортозамещения.

Кейс 2. Интеграция разрозненных ГИС

В регионе функционируют несколько государственных информационных систем (ГИС образования, ГИС здравоохранения, ГИС социальной защиты), которые не обмениваются данными между собой. Это приводит к тому, что граждане многократно предоставляют одни и те же документы. Руководитель проектного офиса предлагает создать единую платформу.

Вопросы: 1) Какая архитектура (например, сервис-ориентированная) позволит решить проблему интеграции? 2) Какие технические и организационные сложности могут возникнуть? 3) Предложите дорожную карту интеграции существующих ГИС без их замены.

Кейс 3. Импортозамещение операционной системы

Государственное учреждение до 2027 года должно перейти с ОС Windows на отечественную операционную систему. Сотрудники привыкли к Windows, многие прикладные программы работают только под Windows. Бюджет на переобучение и замену ПО ограничен.

Вопросы: 1) Какие отечественные операционные системы могут быть рассмотрены в качестве замены? 2) Какие риски связаны с переходом и как их минимизировать? 3) Разработайте план миграции с указанием этапов, сроков и необходимых ресурсов.

1.2.3. Темы докладов / эссе

1. Эволюция архитектур информационных систем: от файл-сервера к SOA и микросервисам.
2. Сравнительный анализ отечественных операционных систем для государственных информационных систем (Astra Linux, Ред ОС, Альт и др.).
3. Проблемы интеграции государственных информационных систем: технические, организационные, правовые аспекты.
4. Применение технологий искусственного интеллекта в государственных информационных системах: перспективы и ограничения.
5. Открытые данные как информационный ресурс: формирование, публикация, использование в государственном управлении.
6. Выбор СУБД для государственной информационной системы: отечественные и зарубежные решения.
7. Требования к отказоустойчивости и непрерывности работы государственных информационных систем: методы и средства обеспечения.

Тема 1.3. Нормативно-правовое регулирование информационной безопасности и защиты персональных данных

1.3.1. Тестовые задания

Задание 1

Расположите в хронологической последовательности этапы обработки персональных данных оператором государственной информационной системы в соответствии с 152-ФЗ:

А) Получение согласия субъекта на обработку персональных данных.

Б) Уничтожение или обезличивание персональных данных при достижении целей.

В) Сбор персональных данных в соответствии с заявленными целями.

Г) Уведомление Роскомнадзора о начале обработки (при необходимости).

Д) Обеспечение безопасности персональных данных при их хранении и передаче.

Задание 2

Установите соответствие между видом ответственности за нарушение законодательства о персональных данных и её характеристикой:

Вид ответственности	Характеристика
1. Административная	А. Компенсация морального вреда, взыскание убытков
2. Уголовная	Б. Штраф по ст. 13.11 КоАП РФ, предупреждение
3. Гражданско-правовая	В. Увольнение, выговор, замечание
4. Дисциплинарная	Г. Штраф до 200 000 рублей или лишение свободы до 4 лет (ст. 137 УК РФ)

Задание 3

Выберите **все верные** утверждения о правовом режиме персональных данных. **Обоснуйте** выбор.

а) Биометрические персональные данные (фотография, отпечатки пальцев) могут обрабатываться без согласия субъекта.

б) Оператор персональных данных обязан опубликовать Политику обработки персональных данных на своём сайте.

в) Согласие на обработку персональных данных может быть отозвано субъектом в любое время.

г) Обработка персональных данных без согласия допускается, если это необходимо для защиты жизни и здоровья субъекта.

д) Обезличенные персональные данные могут свободно распространяться без каких-либо ограничений.

Задание 4

Перечислите не менее четырёх обязанностей оператора персональных данных, установленных статьёй 18.1 Федерального закона № 152-ФЗ.

Задание 5 (открытое)

В государственном учреждении произошла утечка персональных данных сотрудников и клиентов. Расследование показало, что доступ к базе данных не был защищён паролем, а удалённый администратор использовал незащищённый канал связи. Какие требования 152-ФЗ и приказов ФСТЭК были нарушены? Опишите алгоритм действий руководителя проекта после обнаружения инцидента (локализация, уведомление, расследование).

1.3.2. Кейс-задания

Кейс 1. Утечка персональных данных в ГИС здравоохранения

В ГИС здравоохранения региона произошла утечка персональных данных врачей и пациентов. Расследование показало, что тестовый контур системы не был изолирован от продуктивной среды, а сотрудник подрядчика скопировал данные на личный ноутбук.

Вопросы: 1) Какие статьи 152-ФЗ и требования ФСТЭК нарушены? 2) Кто несёт ответственность: заказчик, подрядчик или ответственный за обработку ПДн? 3) Разработайте план мероприятий по предотвращению подобных инцидентов в будущем.

Кейс 2. Использование иностранного облачного сервиса

Региональный проектный офис использует бесплатную версию зарубежного облачного сервиса (Google Docs) для совместной работы над документами, содержащими персональные данные граждан. Руководитель считает, что это удобно и не требует затрат.

Вопросы: 1) Какие нормативные требования нарушены (укажите конкретные законы и подзаконные акты)? 2) Каковы возможные последствия (юридические, финансовые, репутационные)? 3) Предложите план перехода на отечественную платформу с минимизацией рисков.

Кейс 3. Несвоевременное уведомление Роскомнадзора

Государственное учреждение начало обработку персональных данных граждан в новой информационной системе, но не направило уведомление в Роскомнадзор, считая, что обработка осуществляется на основании трудового законодательства. При плановой проверке выявлено нарушение.

Вопросы: 1) Правомерна ли позиция учреждения? В каких случаях уведомление не требуется? 2) Какая ответственность предусмотрена за данное нарушение? 3) Подготовьте проект уведомления об обработке персональных данных для направления в Роскомнадзор.

1.3.3. Темы докладов / эссе

1. Эволюция законодательства о персональных данных в Российской Федерации.
2. Соотношение понятий «персональные данные» и «тайна частной жизни» в праве.
3. Практика привлечения к ответственности за нарушение 152-ФЗ: анализ судебных решений.
4. Трансграничная передача персональных данных: правовые ограничения и механизмы.
5. Обезличивание персональных данных: методы, требования, практика применения.
6. Согласие на обработку персональных данных: форма, содержание, порядок отзыва.
7. Правовые аспекты использования биометрических персональных данных в государственных информационных системах.

РАЗДЕЛ 2. КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОМ МЕНЕДЖМЕНТЕ

Тема 2.1. Киберугрозы и система обеспечения информационной безопасности в государственных проектах

2.1.1. Тестовые задания

Задание 1

Расположите этапы анализа угроз информационной безопасности для государственной информационной системы в логической последовательности:

А) Выявление уязвимостей системного и прикладного программного обеспечения.

Б) Определение потенциальных нарушителей и их возможностей.

В) Разработка модели угроз и оценка вероятности реализации.

Г) Описание актуальных угроз для конкретной информационной системы.

Д) Анализ последствий реализации угроз (ущерб конфиденциальности, целостности, доступности).

Задание 2

Установите соответствие между типом угрозы информационной безопасности и её описанием:

Тип угрозы	Описание
1. Угроза конфиденциальности	А. Нарушение работоспособности информационной системы (DDoS-атака)
2. Угроза целостности	Б. Несанкционированное ознакомление с данными, утечка
3. Угроза доступности	В. Уничтожение или искажение информации
4. Угроза права собственности	Г. Нарушение авторских прав, незаконное использование ПО

Задание 3

Выберите **все верные** утверждения об источниках угроз информационной безопасности в государственных проектах. **Обоснуйте** выбор.

а) Только внешние злоумышленники (хакеры) представляют реальную угрозу для государственных ИС.

б) Внутренние нарушители (сотрудники, подрядчики) обладают доступом к информации и могут нанести значительный ущерб.

в) Техногенные угрозы (сбои оборудования, отключение электропитания) не учитываются в модели угроз.

г) Социальная инженерия является эффективным методом получения доступа к защищаемой информации.

д) Угрозы, связанные с наличием недекларированных возможностей в программном обеспечении, актуальны только для зарубежного ПО.

Задание 4

Назовите не менее трёх каналов утечки информации, характерных для государственных информационных систем. Для каждого канала предложите метод противодействия.

Задание 5 (открытое)

Опишите порядок разработки модели угроз для государственной информационной системы, обрабатывающей персональные данные. Какие нормативные документы регламентируют этот процесс? Какие разделы должна содержать модель угроз?

2.1.2. Кейс-задания

Кейс 1. Фишинговая атака на государственное учреждение

Сотрудники регионального министерства получили электронное письмо, якобы от руководителя, с просьбой срочно перейти по ссылке и ввести логин и пароль от корпоративной почты. Несколько сотрудников перешли по ссылке и ввели свои учётные данные. Через некоторое время был зафиксирован несанкционированный доступ к внутренним документам.

Вопросы: 1) Какой тип угрозы реализован в данном случае? 2) Какие организационные и технические меры должны быть приняты для предотвращения подобных атак? 3) Разработайте программу повышения осведомлённости сотрудников в области информационной безопасности.

Кейс 2. DDoS-атака на портал государственных услуг

В день начала приёма заявлений в первые классы портал государственных услуг региона подвергся DDoS-атаке. Портал был недоступен в течение 4 часов. Многие граждане не смогли подать заявления.

Вопросы: 1) К какому виду угроз (конфиденциальность, целостность, доступность) относится DDoS-атака? 2) Какие меры защиты от DDoS-атак должны быть предусмотрены для государственных порталов? 3) Предложите план действий по восстановлению работоспособности портала и информированию граждан.

Кейс 3. Инсайдерская угроза в проектном офисе

Сотрудник проектного офиса, увольняясь, скопировал на флеш-накопитель базу данных с персональными данными участников государственного проекта. Система обнаружения утечек (DLP) не зафиксировала копирование, так как данные были заархивированы с паролем.

Вопросы: 1) Какие недостатки системы защиты информации выявлены в данном случае? 2) Какие организационные меры должны быть реализованы для предотвращения инсайдерских угроз? 3) Предложите технические решения для контроля копирования данных на съёмные носители.

2.1.3. Темы докладов / эссе

1. Классификация угроз информационной безопасности для государственных информационных систем.
2. Методы социальной инженерии и способы защиты от них в государственных учреждениях.
3. Анализ реальных кибератак на государственные информационные системы в Российской Федерации (2019-2025).
4. Роль человеческого фактора в обеспечении информационной безопасности: психологические аспекты.
5. Побочные электромагнитные излучения и наводки (ПЭМИН) как канал утечки информации: методы защиты.
6. Сравнительный анализ отечественных и зарубежных подходов к моделированию угроз.
7. Мониторинг безопасности сетей: снифферы, анализ трафика, выявление аномалий (технический обзор).

Тема 2.2. Организация защиты персональных данных в государственных информационных системах

2.2.1. Тестовые задания

Задание 1

Расположите в правильной последовательности действия оператора при выявлении факта неправомерной обработки персональных данных:

А) Принятие мер по устранению нарушений или уничтожению персональных данных.

Б) Выявление факта неправомерной обработки (проверка, аудит, инцидент).

В) Уведомление субъекта персональных данных (при необходимости).

Г) Оценка вреда, который может быть причинён субъекту.

Д) Уведомление Роскомнадзора о выявленном нарушении.

Задание 2

Установите соответствие между категорией персональных данных и её характеристикой:

Категория персональных данных	Характеристика
1. Специальные категории	А. Данные, полученные только из общедоступных источников
2. Биометрические	Б. Сведения о расовой, национальной принадлежности, религии, здоровье
3. Общедоступные	В. Иные категории, не относящиеся к специальным, биометрическим или общедоступным
4. Иные категории	Г. Данные, характеризующие физиологические особенности человека и используемые для установления личности

Задание 3

Выберите **все верные** утверждения о мерах по обеспечению безопасности персональных данных. **Обоснуйте** выбор.

а) Назначение лица, ответственного за организацию обработки персональных данных, является обязательным для всех операторов.

б) Использование сертифицированных средств защиты информации не требуется для государственных информационных систем 4-го класса защищённости.

в) Оценка эффективности принимаемых мер по защите персональных данных проводится до ввода информационной системы в эксплуатацию.

г) Учёт машинных носителей персональных данных не обязателен, если данные хранятся в облаке.

д) При обработке персональных данных без средств автоматизации достаточно ограничить физический доступ к документам.

Задание 4

Перечислите не менее трёх методов обезличивания персональных данных, установленных приказом Роскомнадзора № 996. Для каждого метода приведите пример применения.

Задание 5 (открытое)

В государственном учреждении обрабатываются персональные данные в информационной системе 3-го класса защищённости. Какие требования к защите информации установлены для данного класса? Составьте перечень необходимых организационных и технических мер.

2.2.2. Кейс-задания

Кейс 1. Обработка биометрических персональных данных

Муниципальное учреждение внедряет систему контроля доступа с использованием отпечатков пальцев для сотрудников и посетителей. Руководитель считает, что достаточно устного согласия сотрудников.

Вопросы: 1) Какие требования 152-ФЗ предъявляются к обработке биометрических персональных данных? 2) В какой форме должно быть получено согласие? 3) Разработайте форму согласия на обработку биометрических персональных данных.

Кейс 2. Назначение ответственного за обработку персональных данных

В небольшом государственном учреждении (30 сотрудников) руководитель возложил обязанности по организации обработки персональных данных на секретаря без издания приказа и внесения изменений в должностную инструкцию. При проверке Роскомнадзор выявил нарушение.

Вопросы: 1) Обязательно ли назначение ответственного за обработку персональных данных для государственных учреждений? 2) Какие требования к такому назначению установлены законом? 3) Подготовьте проект приказа о назначении ответственного и фрагмент должностной инструкции.

Кейс 3. Обезличивание персональных данных для публикации

Региональное министерство планирует опубликовать на открытом портале данные о получателях социальных выплат (сумма выплаты, район проживания, возраст, пол). При этом фамилии, имена и точные адреса будут удалены. Руководитель считает, что этого достаточно для обезличивания.

Вопросы: 1) Соответствует ли такой подход требованиям приказа Роскомнадзора № 996? 2) Какие методы обезличивания необходимо применить, чтобы исключить возможность идентификации? 3) Оцените риск деобезличивания при публикации таких данных и предложите дополнительные меры.

2.2.3. Темы докладов / эссе

1. Правовой статус биометрических персональных данных: особенности обработки и хранения.
2. Требования к материальным носителям персональных данных: законодательство и практика.
3. Обезличивание персональных данных: методы, ограничения, риски деобезличивания.
4. Ведение реестра операторов персональных данных: порядок, сроки, ответственность.
5. Международный опыт защиты персональных данных: GDPR и российское законодательство (сравнительный анализ).
6. Локальные акты оператора персональных данных: перечень, содержание, порядок принятия.
7. Проблемы применения законодательства о персональных данных в государственных учреждениях: практические кейсы и пути решения.

Тема 2.3. Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография

2.3.1. Тестовые задания

Задание 1

Расположите в порядке возрастания уровня защищённости (от наименее защищённого к наиболее защищённому) типы межсетевых экранов:

А) Межсетевой экран с отслеживанием состояния соединений (Stateful).

Б) Пакетный фильтр (Stateless).

В) Межсетевой экран прикладного уровня (Application Gateway).

Г) Межсетевой экран с функцией обнаружения атак (NGFW — Next Generation Firewall).

Задание 2

Установите соответствие между типом средства защиты информации и его функциональным назначением:

Средство защиты	Назначение
1. IDS (система обнаружения атак)	А. Фильтрация сетевого трафика по правилам
2. IPS (система предотвращения атак)	Б. Выявление признаков атак и оповещение администратора
3. Межсетевой экран (брандмауэр)	В. Активное блокирование атакующих пакетов в реальном времени
4. Сниффер	Г. Перехват и анализ сетевого трафика

Задание 3

Выберите **все верные** утверждения о криптографических методах защиты информации. **Обоснуйте** выбор.

а) Симметричное шифрование использует один ключ для шифрования и дешифрования.

б) Асимметричное шифрование использует открытый и закрытый ключи; закрытый ключ можно восстановить из открытого.

в) Электронная подпись предназначена для подтверждения подлинности и целостности документа, а также для установления авторства.

г) Средства криптографической защиты информации (СКЗИ) подлежат обязательной сертификации ФСБ России для использования в государственных ИС.

д) Шифрование персональных данных не требуется, если доступ к информационной системе ограничен паролем.

Задание 4

Перечислите не менее трёх методов обнаружения атак, используемых в IDS. Для каждого метода опишите его преимущества и недостатки.

Задание 5 (открытое)

В государственной информационной системе установлен межсетевой экран, настроенный по принципу «всё, что не запрещено, разрешено». Какие риски создаёт такая конфигурация? Предложите правила фильтрации для типовой ГИС (веб-портал, доступ к БД из внутренней сети, запрет доступа из интернета к административным интерфейсам).

2.3.2. Кейс-задания

Кейс 1. Внедрение IDS/IPS в государственном учреждении

Государственное учреждение закупило и установило систему обнаружения атак (IDS). Однако через месяц работы система генерирует сотни ложных срабатываний, и администратор её отключил. Руководитель считает, что IDS бесполезна.

Вопросы: 1) Какие причины могут вызывать ложные срабатывания IDS? 2) Как правильно настроить IDS для минимизации ложных срабатываний? 3) В чём разница между IDS и IPS и почему в данном случае, возможно, следовало выбрать IPS?

Кейс 2. Анализ перехваченного трафика

Специалист по информационной безопасности с помощью сниффера Wireshark обнаружил в сети государственного учреждения большое количество ARP-запросов с одного IP-адреса, направленных на все устройства в сегменте. Также зафиксированы ответы ARP, подменяющие MAC-адрес шлюза по умолчанию.

Вопросы: 1) Какой тип атаки был обнаружен (ARP-spoofing)? 2) Каковы цели злоумышленника? 3) Какие меры защиты от ARP-атак могут быть реализованы на коммутаторах и рабочих станциях?

Кейс 3. Выбор СКЗИ для ГИС

Региональная ГИС должна обеспечить шифрование каналов связи между центральным офисом и 50 удалёнными точками, а также электронную подпись отчётности. Бюджет ограничен. Руководитель предлагает использовать бесплатное зарубежное криптографическое ПО.

Вопросы: 1) Правомерно ли использование зарубежных СКЗИ в государственных информационных системах? 2) Какие требования предъявляются к СКЗИ для ГИС? 3) Предложите отечественные сертифицированные решения и обоснуйте выбор.

2.3.3. Темы докладов / эссе

1. Сравнительный анализ сигнатурного и поведенческого методов обнаружения атак.
2. Применение технологий машинного обучения в системах обнаружения вторжений (IDS/IPS).
3. Межсетевые экраны нового поколения (NGFW): возможности и перспективы использования в государственных сетях.
4. Анализ протоколов канального уровня и уязвимости (ARP-spoofing, MAC-flooding, VLAN hopping).
5. Криптографическая защита информации: стандарты РФ (ГОСТ 28147-89, ГОСТ Р 34.10-2012).
6. Практика использования снифферов для диагностики сетей и выявления атак (на примере Wireshark).
7. Построение защищённых каналов связи для государственных информационных систем (VPN, TLS, отечественные решения).

Тема 2.4. Управление рисками информационной безопасности и реагирование на инциденты

2.4.1. Тестовые задания

Задание 1

Расположите этапы управления рисками информационной безопасности в логической последовательности согласно методологии PMBOK и рекомендациям ФСТЭК:

А) Планирование реагирования на риски (выбор стратегий).

Б) Мониторинг и контроль рисков.

В) Идентификация рисков (составление реестра).

Г) Качественный и количественный анализ рисков.

Д) Планирование управления рисками (определение методологии).

Задание 2

Установите соответствие между типом риска информационной безопасности и примером для проекта цифровой трансформации:

Тип риска	Пример
1. Технологический риск	А. Отказ персонала использовать новую информационную систему
2. Организационный риск	Б. Уязвимость в используемом программном обеспечении
3. Человеческий риск	В. Изменение законодательства о персональных данных в ходе проекта
4. Правовой риск	Г. Отсутствие резервного копирования, приведшее к потере данных

Задание 3

Выберите **все верные** утверждения о методах реагирования на инциденты информационной безопасности. **Обоснуйте** выбор.

а) При обнаружении утечки персональных данных оператор обязан уведомить Роскомнадзор в течение 24 часов.

б) Локализация инцидента предполагает отключение поражённого сегмента сети от остальной инфраструктуры.

в) Расследование причин инцидента проводится только правоохранительными органами, оператор не участвует.

г) После устранения последствий инцидента необходимо провести анализ и скорректировать систему защиты.

д) Уведомление субъектов персональных данных об утечке не требуется, если данные были зашифрованы.

Задание 4

Назовите не менее трёх стратегий реагирования на риски информационной безопасности и для каждой приведите пример применения в государственном проекте.

Задание 5 (открытое)

По проекту создания ГИС выявлен риск: вероятность утечки персональных данных через тестовый контур — 20%, возможный ущерб — 10 млн рублей. Рассчитайте ожидаемую стоимость риска (EMV). Какие стратегии реагирования могут быть применены для снижения этого риска? Предложите конкретные мероприятия и оцените их эффективность.

2.4.2. Кейс-задания

Кейс 1. Утечка персональных данных в ГИС здравоохранения (продолжение)

В ГИС здравоохранения произошла утечка персональных данных врачей и пациентов. Расследование установило, что доступ к тестовому контуру системы не был защищён паролем, а удалённый администратор использовал незащищённый канал связи. Руководитель проекта не имел утверждённого плана реагирования на инциденты.

Вопросы: 1) Разработайте план реагирования на инцидент (по шагам, с указанием ответственных и сроков). 2) Какие уведомления и в какие сроки должны быть направлены? 3) Предложите корректирующие мероприятия для проектной команды.

Кейс 2. Оценка рисков при переходе на отечественное ПО

Правительство региона приняло решение о переходе на отечественное офисное ПО в течение 2 лет. Идентифицированы риски: несовместимость с existing СЭД (вероятность 40%, задержка 4 мес., потери 2 млн руб.); обучение персонала (вероятность 70%, затраты 1 млн руб.); отказ сотрудников от использования (вероятность 30%, снижение производительности 15%).

Вопросы: 1) Рассчитайте ожидаемую стоимость (EMV) для каждого риска. 2) Определите суммарный резерв на управление рисками. 3) Предложите стратегии реагирования для двух наиболее критичных рисков.

Кейс 3. План реагирования на DDoS-атаку

В проектном офисе разрабатывается план реагирования на DDoS-атаку на портал государственных услуг. Определены роли: руководитель проекта, администратор ИС, пресс-секретарь, юрист.

Вопросы: 1) Опишите алгоритм действий каждой роли в первые 30 минут после обнаружения атаки. 2) Разработайте шаблон сообщения для информирования граждан о временной недоступности портала. 3) Предложите состав антикризисного набора документов (checklist) для отработки DDoS-атаки.

2.4.3. Темы докладов / эссе

1. Методы количественной и качественной оценки рисков информационной безопасности: сравнительный анализ.
2. Построение карты рисков информационной безопасности для государственного проекта цифровой трансформации.
3. Страхование киберрисков в государственном секторе: возможности и ограничения.
4. План обеспечения непрерывности деятельности (BCP) государственной информационной системы: структура и разработка.
5. Роль Национального координационного центра по компьютерным инцидентам (НКЦКИ) в реагировании на атаки на ГИС.
6. Проведение учений по отработке реагирования на инциденты: методика и опыт.
7. Анализ реальных кейсов реагирования на инциденты в государственных информационных системах (из открытых источников).

Критерии оценки тестовых заданий (закрытого и комбинированного типа: на последовательность, соответствие, множественный выбор с обоснованием, открытые аналитические/расчётные)

Оценка (баллы)	Критерии для заданий на последовательность / соответствие	Критерии для заданий множественного выбора с обоснованием	Критерии для заданий открытого типа (аналитических / расчётных)
5 (отлично)	Полностью верная последовательность / все пары соответствия установлены верно.	Выбраны все правильные варианты, дано чёткое, логичное обоснование (с опорой на теорию, без ошибок).	Ответ полный, развёрнутый, содержит необходимые расчёты (где нужно), ссылки на теорию, примеры, выводы. Отсутствуют фактические и логические ошибки.
4 (хорошо)	Допущена одна ошибка (например, переставлены два соседних элемента или одна пара неверна).	Выбраны все правильные варианты, но обоснование неполное, слишком общее, с незначительными неточностями.	Ответ в целом верный, но допущены незначительные неточности (например, неполный перечень факторов, отсутствует один шаг в рассуждении, арифметическая ошибка, не повлиявшая на суть вывода).
3 (удовлетворительно)	Допущены две ошибки (две пары неверны или последовательность нарушена в двух местах).	Выбраны не все верные варианты (пропущен один верный или добавлен один неверный), обоснование слабое, формальное.	Ответ неполный: раскрыта только часть вопроса, отсутствуют примеры, нет ссылок на теорию, расчёты содержат грубые ошибки, но основная мысль понятна.
2 (неудовлетворительно)	Допущено три и более ошибок.	Выбрано менее половины верных вариантов или обоснование полностью отсутствует.	Ответ поверхностный, содержит грубые теоретические ошибки, расчёты неверны, выводы противоречат условию.
1 (плохо)	Задание не выполнено или все ответы неверны.	Задание не выполнено, нет	Ответ отсутствует, полностью не по существу вопроса.

		выбора и обоснования.	

Примечание: для заданий закрытого типа с выбором одного правильного ответа (не входящих в комбинированные) можно применять: 5 – верно, 0 – неверно. Но выше приведены критерии для комбинированных заданий, которые включают требование обоснования или последовательности.

Критерии оценки кейсовых заданий (полнота анализа, обоснованность, практическая применимость)

Оценка (баллы)	Критерии
5 (отлично)	– Верно идентифицированы все ключевые проблемы ситуации. – Анализ проведён с использованием не менее двух теорий/моделей (например, модели управления проектами, модели рисков, модели жизненного цикла, портфельного управления и др.). – Предложено 3–4 конкретных, реализуемых в государственном секторе шага (или ответа на поставленные вопросы). – Решение обосновано, учтены возможные ограничения (бюджетные, правовые, этические). – Сформулированы чёткие выводы.
4 (хорошо)	– Проблема определена правильно, но использована только одна теоретическая модель или анализ неполный. – Предложено 2–3 шага без детализации ограничений. – В целом решение реалистично и соответствует специфике госслужбы, но не хватает глубины или одного из элементов обоснования.
3 (удовлетворительно)	– Проблема выделена, но анализ поверхностный, без опоры на теорию. – Предложен один очевидный шаг или решение носит формальный характер, не учитывает особенности государственного управления. – Ответ даёт частичное понимание ситуации.
2 (неудовлетворительно)	– Ситуация проанализирована неверно, ключевые проблемы не выявлены. – Предложенные действия нереалистичны или не связаны с проблемой. – Отсутствуют ссылки на теорию.
1 (плохо)	– Задание не выполнено, ответ отсутствует или полностью не по теме кейса.

Критерии оценки решения задач

Оценка (баллы)	Критерии
5 (отлично)	– Формулы или метод решения выбраны верно. – Все расчёты выполнены без ошибок (арифметических, логических). – Ответ содержит интерпретацию полученных результатов (выводы, рекомендации). – При необходимости – единицы измерения указаны, графические построения (сетевые графики) выполнены аккуратно.
4 (хорошо)	– Ход решения верный, но допущена одна незначительная арифметическая ошибка, не повлиявшая на общий вывод. – Вывод сформулирован, но не полностью раскрыт или недостаточно обоснован. – Графическое представление (например, диаграмма Ганта, сетевой график) имеет незначительные неточности.

3 (удовлетворительно)	– Использована правильная формула, но в расчётах есть грубые ошибки (например, неверно подставлены значения), из-за чего получен неверный численный результат. – Вывод отсутствует или не соответствует полученным числам. – Часть решения отсутствует.
2 (неудовлетворительно)	– Метод решения выбран неверно (например, для EVM используются не те показатели). – Расчёты полностью неверны. – Выводы не сделаны или противоречат условию.
1 (плохо)	– Задание не выполнено, решение отсутствует, или представлены только общие фразы без расчётов.

Критерии оценки эссе / доклада

Баллы	Критерии
5	Структура: введение, основная часть, заключение. Раскрыта тема с привлечением не менее 3 научных источников (учебники, статьи). Использованы модели ОП (теории) для анализа. Приведены конкретные примеры из госуправления. Личная позиция аргументирована. Оформление соответствует требованиям (ссылки, список лит-ры, грамотность).
4	Тема раскрыта, но источников менее 3 или примеры из госсектора общие. Есть незначительные нарушения структуры или ошибки в оформлении. Личная позиция выражена, но слабо аргументирована.
3	Содержание поверхностное, теория не применена или грубо искажена. Примеры отсутствуют или не относятся к теме. Нарушена структура, много орфографических ошибок.

5.3. Два тематических блока дисциплины завершаются контрольной точкой (далее – КТ).

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

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,15	15
КТ 2	100	0,15	15
Итого:	x	0,3	30

Формула расчета результата контрольной точки:

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

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

По дисциплине предусмотрены 2 контрольные точки (КТ1, КТ2). Каждая соответствует одному разделу. Каждый тест КТ состоит из 30 заданий. Максимальная оценка за тест КТ – 100 баллов.

Контрольная точка 1 (Раздел 1)

Темы: Тема 1.1 (Информационный менеджмент: сущность, цели, задачи), Тема 1.2 (Информационные ресурсы, технологии и системы: классификация и архитектура), Тема 1.3

(Нормативно-правовое регулирование информационной безопасности и защиты персональных данных)

Задание 1 (Тема 1.1)

Расположите в логической последовательности этапы формирования портфеля проектов информатизации в государственном органе:

А) Утверждение паспортов проектов информатизации.

Б) Определение целевых показателей «цифровой зрелости» по направлениям деятельности.

В) Мониторинг реализации проектов и корректировка портфеля.

Г) Разработка стратегии цифровой трансформации государственного органа.

Д) Отбор проектных инициатив, обеспечивающих достижение целевых показателей.

Задание 2 (Тема 1.1)

Установите соответствие между функцией информационного менеджмента и её содержанием применительно к деятельности государственного проектного офиса:

Функция информационного менеджмента	Содержание функции
1. Планирование в сфере обработки информации	А. Назначение ответственного за обработку персональных данных, разработка локальных актов
2. Формирование организационной структуры	Б. Разработка долгосрочных и краткосрочных планов развития ИС, бюджетирование
3. Обеспечение комплексной защищенности	В. Определение места ИТ-подразделения в иерархии органа власти, распределение полномочий
4. Управление персоналом	Г. Повышение квалификации сотрудников, обучение работе с информационными системами

Задание 3 (Тема 1.1)

Выберите **все верные** утверждения о роли проектного офиса цифровой трансформации в обеспечении информационного менеджмента. **Кратко обоснуйте** каждый выбранный ответ.

а) Проектный офис цифровой трансформации отвечает исключительно за техническую реализацию проектов, не участвуя в управлении информационными ресурсами.

б) Одной из функций проектного офиса является координация деятельности по внедрению государственных информационных систем.

в) Проектный офис не взаимодействует с федеральными органами власти, его отчётность предоставляется только руководителю региона.

г) Проектный офис должен обеспечивать мониторинг достижения показателей «цифровой зрелости».

д) Проектный офис участвует в разработке технических заданий на создание информационных систем с учётом требований импортозамещения.

Задание 4 (Тема 1.2)

Расположите в порядке возрастания сложности внедрения и стоимости владения (от простейшего к наиболее комплексному) варианты архитектуры информационной системы для государственного учреждения:

А) Двухуровневая архитектура «клиент-сервер» («толстый клиент»).

Б) Сервис-ориентированная архитектура (SOA) с интеграцией разнородных систем.

В) Архитектура «файл-сервер».

Г) Трёхуровневая архитектура «клиент-сервер» с выделенным сервером приложений.

Задание 5 (Тема 1.2)

Установите соответствие между типом информационной системы и примером её реализации в государственном секторе:

Тип информационной системы	Пример реализации
1. Государственная информационная система (ГИС)	А. Система «1С:Зарплата и кадры» в бюджетном учреждении
2. ERP-система	Б. Портал государственных услуг (ЕПГУ)

3. Система электронного документооборота (СЭД)	В. Комплексное планирование бюджета в ГИИС «Электронный бюджет»
4. CRM-система	Г. Система «Дело» для автоматизации согласования документов

Задание 6 (Тема 1.2, 1.3)

Выберите **все верные** утверждения о требованиях к защите персональных данных при их обработке в государственных информационных системах. **Кратко обоснуйте** каждый выбранный ответ.

а) Для всех государственных информационных систем требуется аттестация на соответствие требованиям ФСТЭК России.

б) Информационные системы, обрабатывающие персональные данные, подразделяются на 4 класса защищённости (К1 – К4).

в) При обработке персональных данных без использования средств автоматизации не требуется принимать никаких мер по их защите.

г) Средства криптографической защиты информации, используемые в ГИС, подлежат сертификации ФСБ России.

д) Оператор персональных данных вправе не уведомлять Роскомнадзор о начале обработки, если данные обрабатываются в соответствии с трудовым законодательством.

Задание 7 (Тема 1.3)

Проанализируйте следующую ситуацию:

Государственное учреждение в рамках реализации национального проекта разработало ГИС для предоставления гражданам мер социальной поддержки. В конкурсной документации отсутствовало требование об использовании средств криптографической защиты информации, а также не были определены класс защищённости информационной системы. Победитель конкурса предложил решение на основе зарубежной облачной платформы с хранением персональных данных за пределами Российской Федерации.

Вопросы:

1. Какие нарушения нормативных требований (укажите конкретные законы и подзаконные акты) допущены заказчиком?
2. Каковы возможные последствия для заказчика и подрядчика при подписании такого контракта и в ходе его исполнения?
3. Предложите алгоритм действий руководителя проектного офиса, который обнаружил указанные нарушения на этапе подписания контракта (до его заключения).

Контрольная точка 2 (Раздел 2)

Темы: Тема 2.1 (Киберугрозы и система обеспечения информационной безопасности в государственных проектах), Тема 2.2 (Организация защиты персональных данных в государственных информационных системах), Тема 2.3 (Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография), Тема 2.4 (Управление рисками информационной безопасности и реагирование на инциденты)

Задание 1 (Тема 2.1)

Расположите этапы построения модели угроз информационной безопасности для государственной информационной системы в логической последовательности:

А) Оценка последствий реализации угроз для конфиденциальности, целостности и доступности информации.

Б) Определение перечня актуальных угроз на основе анализа уязвимостей и возможностей нарушителя.

В) Описание потенциальных нарушителей и их характеристик (уровень знаний, ресурсы, мотивация).

Г) Анализ защищаемой информации и определение категорий обрабатываемых персональных данных.

Д) Выявление уязвимостей системного и прикладного программного обеспечения, а также аппаратной платформы.

Задание 2 (Тема 2.1, 2.3)

Установите соответствие между типом атаки и уровнем модели OSI, на котором она реализуется, а также методом противодействия:

Тип атаки	Уровень OSI	Метод противодействия
1. ARP-spoofing	А. Физический уровень	1. Использование IDS/IPS
2. CAM-table overflow	Б. Канальный уровень	2. Настройка DHCP Snooping
3. Отказ в обслуживании (DDoS)	В. Сетевой уровень	3. Фильтрация трафика на межсетевом экране
4. Подмена default gateway	Г. Прикладной уровень	4. Ограничение количества MAC-адресов на порту

Задание 3 (Тема 2.2)

Выберите **все верные** утверждения о правовом режиме биометрических персональных данных при их обработке в государственных информационных системах. **Кратко обоснуйте** каждый выбранный ответ.

а) Биометрические персональные данные могут обрабатываться без согласия субъекта, если это необходимо для проведения государственной судебной экспертизы.

б) Фотография гражданина, размещённая на портале государственных услуг, не является биометрическими персональными данными, так как не используется для установления личности.

в) При обработке биометрических персональных данных обязательно использование сертифицированных средств криптографической защиты информации.

г) Хранение биометрических персональных данных вне информационных систем допускается без каких-либо требований к материальным носителям.

д) Согласие на обработку биометрических персональных данных должно быть оформлено в письменной форме.

Задание 4 (Тема 2.3)

Расположите в порядке возрастания уровня защищённости (от наименее защищённого к наиболее защищённому) следующие методы фильтрации сетевого трафика:

А) Межсетевой экран с отслеживанием состояния соединений (Stateful).

Б) Пакетный фильтр (Stateless) с проверкой IP-адресов и портов.

В) Межсетевой экран прикладного уровня (Application Gateway) с анализом содержимого пакетов.

Г) Межсетевой экран нового поколения (NGFW) с функцией обнаружения и предотвращения атак.

Задание 5 (Тема 2.2, 2.4)

Установите соответствие между методом обезличивания персональных данных и его описанием:

Метод обезличивания	Описание
1. Метод введения идентификаторов	А. Разделение массива персональных данных на несколько частей с раздельным хранением
2. Метод изменения состава или семантики	Б. Замена части сведений идентификаторами с созданием таблицы соответствия
3. Метод декомпозиции	В. Перестановка отдельных значений или групп значений атрибутов
4. Метод перемешивания	Г. Изменение состава персональных данных путём обобщения или удаления части сведений

Задание 6 (Тема 2.4)

Выберите **все верные** утверждения о порядке управления рисками информационной безопасности в государственных проектах. **Кратко обоснуйте** каждый выбранный ответ.

а) Количественная оценка рисков предполагает расчёт ожидаемой стоимости риска (EMV) как произведение вероятности на величину ущерба.

б) При идентификации рисков учитываются только внешние угрозы (хакерские атаки, стихийные бедствия).

в) Стратегия «принятия риска» означает, что никакие меры по его снижению не принимаются, а риск остаётся на балансе организации.

г) Мониторинг рисков должен осуществляться непрерывно на протяжении всего жизненного цикла проекта.

д) План реагирования на инциденты информационной безопасности не требуется для государственных информационных систем 4-го класса защищённости.

Задание 7 (Темы 2.1, 2.2, 2.3, 2.4)

Проанализируйте следующую ситуацию:

В региональном проектном офисе разрабатывается ГИС «Мониторинг общественного транспорта». В реестре рисков не были учтены угрозы, связанные с использованием зарубежного программного обеспечения, а также не проведена оценка рисков утечки персональных данных (система обрабатывает данные о пассажирах, включая информацию о маршрутах передвижения). В ходе опытной эксплуатации была зафиксирована утечка обезличенных, по мнению разработчика, данных (IP-адреса, время входа, геолокация).

Вопросы:

1. Какие категории персональных данных обрабатываются в системе? Требуется ли согласие субъектов на их обработку?
2. Какие нормативные требования (152-ФЗ, 149-ФЗ, приказы ФСТЭК) нарушены при проектировании и эксплуатации ГИС?
3. Рассчитайте ожидаемую стоимость риска утечки, если вероятность реализации угрозы оценена в 15%, а возможный ущерб (штрафы, репутационные потери, затраты на уведомление) — 8 млн рублей. Какой резерв необходимо заложить на управление этим риском?
4. Предложите комплекс организационных и технических мер по устранению выявленных нарушений и снижению рисков. Разработайте план мероприятий с указанием сроков и ответственных.

Распределение баллов (100 баллов) в соответствии с типом заданий

Тип задания	Количество в тесте	Баллов за одно задание	Всего баллов
На соответствие (установить пары)	6	4	24
На последовательность (расположить этапы/шаги)	6	4	24
Множественный выбор с обоснованием (выбрать все правильные ответы + кратко объяснить)	8	4	32
Открытого типа (развёрнутый аналитический или расчётный ответ)	10	2	20
Итого	30		100

Критерии оценивания каждого типа заданий

Задания на соответствие (6 заданий, макс. 4 балла каждое)

Что делать: Соединить элементы из левого столбца с элементами из правого столбца (например, «модель ОП – её характеристика»). Ответ записать в виде пар «1-А, 2-Б, 3-В».

Критерии:

Баллы	Критерий
4	Все пары верны
3	Одна ошибка (одна пара неверна или пропущена)
2	Две ошибки
1	Три ошибки

0	Четыре и более ошибок / задание не выполнено

Задания на последовательность (6 заданий, макс. 4 балла каждое)

Что делать:

Расположить этапы, шаги или понятия в правильном хронологическом или логическом порядке. Ответ записать в виде последовательности букв (например, «А, Б, В, Г»).

Критерии:

Баллы	Критерий
4	Полностью верная последовательность
3	Одна перестановка соседних элементов
2	Две перестановки или одна более грубая ошибка
1	Три ошибки
0	Четыре и более ошибок / задание не выполнено

Задания типа «множественный выбор с обоснованием» (8 заданий, макс. 4 балла каждое)

Что делать:

*Выбрать **все** правильные варианты из предложенных (обычно 2–4 ответа).*

***Кратко** (1–2 предложения) обосновать, почему вы выбрали именно эти варианты (и, если нужно, почему остальные неверны).*

Критерии:

Баллы	Критерий
4	Выбраны все верные варианты и дано логичное, чёткое обоснование (связь с теорией)
3	Выбраны все верные варианты, но обоснование неполное / слишком общее / с неточностями
2	Выбраны не все верные варианты (пропущен один верный или добавлен один неверный), обоснование социально
1	Выбрано менее половины верных вариантов или обоснование отсутствует
0	Задание не выполнено или все ответы неверны

Пример правильного обоснования***:***

«Верны пункты А и В, так как, согласно теории Герцберга, мотиваторами являются содержание работы и признание, а зарплата – гигиенический фактор, поэтому пункт Б не подходит».

Задания открытого типа (10 заданий, макс. 2 балла каждое)

Что делать:

*Дать **развёрнутый** ответ.*

*Для **аналитического** задания: описать не менее 2–3 факторов / причин / мероприятий, использовать теоретическую модель, при возможности привести пример из практики государственной службы.*

*Для **расчётного** задания: записать формулу, подставить цифры, выполнить вычисления, **обязательно** сделать словесный вывод.*

Критерии:

Баллы	Критерий
2	Полный ответ: – аналитический: названы 2–3 фактора, есть ссылка на теорию (фамилия учёного, название модели), пример; – расчётный: формула верна, расчёты без ошибок, вывод обоснован.
1	Неполный ответ: – аналитический: назван только 1 фактор, нет примера или нет связи с теорией; – расчётный: незначительная арифметическая ошибка при верной логике, или нет вывода.

0	Ответ отсутствует, полностью неверен или содержит грубые теоретические ошибки.

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Для выполнения тестовых заданий, ситуационных задач студенту разрешается использование MS Ecxel, калькулятора, а также НПА.

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

6.1. Промежуточная аттестация проводится в форме *зачета.*

Вопросы для подготовки к зачету по дисциплине

Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента

1. Раскройте понятие, цели и задачи информационного менеджмента. Почему информация рассматривается как стратегический ресурс современной организации?
2. Охарактеризуйте предмет, объект и субъект информационного менеджмента. Перечислите основные функции информационного менеджмента и раскройте их содержание.
3. Каковы современные тренды информационного менеджмента в государственном секторе? Дайте характеристику импортозамещению программного обеспечения, показателям «цифровой зрелости» и цифровой трансформации.
4. Как информационный менеджмент связан с проектным управлением в органах власти? Какую роль выполняет проектный офис цифровой трансформации?
5. Что понимается под информационными ресурсами? Назовите виды информационных ресурсов и охарактеризуйте их особенности как объекта управления.
6. Приведите классификацию информационных систем (ERP, CRM, СЭД, ГИС). Для каждого типа приведите примеры использования в государственном секторе.
7. Охарактеризуйте основные архитектуры информационных систем: файл-сервер, клиент-сервер (двухуровневая, трехуровневая), сервис-ориентированная архитектура (SOA). Укажите их достоинства и недостатки.
8. Каковы критерии выбора платформы и операционной системы для государственной информационной системы? Почему требования импортозамещения являются приоритетными?
9. Раскройте основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: правовой режим информации, ограничение доступа, государственные информационные системы.
10. Охарактеризуйте Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: понятие персональных данных, принципы их обработки, согласие субъекта, обязанности оператора.
11. Какие категории персональных данных выделяются в законодательстве (общедоступные, специальные, биометрические, иные)? Каков правовой режим каждой категории?
12. Какие требования к защите информации в государственных информационных системах установлены ФСТЭК России? Раскройте понятия аттестации, классов защищенности, сертификации средств защиты информации.
13. Охарактеризуйте основные положения Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
14. Перечислите виды ответственности за нарушение законодательства о персональных данных (административная, уголовная, гражданско-правовая, дисциплинарная). По каждому виду приведите примеры санкций.

Раздел 2. Кибербезопасность и защита персональных данных в информационном менеджменте

15. Дайте определение понятию «угроза информационной безопасности». Охарактеризуйте классификацию угроз по виду (конфиденциальность, целостность, доступность, право собственности).

16. Каковы источники угроз информационной безопасности (антропогенные, техногенные, природные)? Охарактеризуйте внешних и внутренних нарушителей.

17. Назовите и охарактеризуйте современные киберугрозы для государственных информационных систем (DDoS-атаки, фишинг, вредоносное программное обеспечение).

18. Какие атаки на канальном и сетевом уровне вы знаете (ARP-spoofing, MAC-spoofing, VLAN hopping, CAM-table overflow)? В чем заключается принцип каждой атаки и каковы способы защиты?

19. Раскройте принципы построения системы защиты информации в организации. Охарактеризуйте правовые, организационные и технические меры.

20. Охарактеризуйте правовой статус оператора персональных данных. Каковы его права, обязанности и ответственность?

21. В каком порядке получается согласие субъекта на обработку персональных данных? Назовите случаи, когда обработка персональных данных допускается без согласия субъекта.

22. Какие локальные нормативные акты должен разработать оператор персональных данных? Каковы требования к их содержанию?

23. Что такое обезличивание персональных данных? Охарактеризуйте методы обезличивания: введение идентификаторов, изменение состава или семантики, декомпозиция, перемешивание. Каковы требования Роскомнадзора к обезличиванию?

24. Что такое межсетевой экран (брандмауэр)? Приведите классификацию межсетевых экранов (пакетные фильтры, Stateful, прикладного уровня, NGFW). Охарактеризуйте принципы их работы.

25. Каковы назначение и принципы работы систем обнаружения и предотвращения атак (IDS/IPS)? В чем отличие сетевых IDS от хостовых? Охарактеризуйте сигнатурный и поведенческий методы обнаружения.

26. Что относится к средствам криптографической защиты информации (СКЗИ)? Охарактеризуйте симметричное и асимметричное шифрование, электронную подпись. Каковы требования к сертификации СКЗИ для использования в государственных информационных системах?

27. Как осуществляется мониторинг безопасности сетей? Что такое снифферы? Охарактеризуйте анализатор трафика Wireshark и возможности его использования для выявления атак.

28. Раскройте понятие и методы оценки рисков информационной безопасности. В чем отличие количественной оценки от качественной?

29. Охарактеризуйте этапы управления рисками информационной безопасности: идентификация, анализ, оценка, обработка, мониторинг. Какие стратегии реагирования на риски существуют?

30. Каков порядок планирования реагирования на инциденты информационной безопасности? Опишите алгоритм действий оператора при обнаружении утечки персональных данных (локализация, расследование, уведомление регуляторов).

31. Раскройте принципы построения рациональной системы защиты информации (запрет доступа по умолчанию, простота механизма защиты, перекрытие всех каналов утечки, разделение полномочий, предоставление минимальных полномочий, обособленность механизма защиты, психологическая привлекательность).

32. Какова роль Национального координационного центра по компьютерным инцидентам (НКЦКИ) в обеспечении кибербезопасности государственных информационных систем? Каков порядок взаимодействия операторов с НКЦКИ при возникновении инцидентов?

6.2. Типовые оценочные материалы промежуточной аттестации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента

Тема 1.1. Информационный менеджмент: сущность, цели, задачи и место в системе государственного управления

Задание 1.1.1

Расположите в правильной последовательности этапы формирования стратегии информационного менеджмента в государственном органе:

А) Определение целевых показателей эффективности информационной деятельности.

Б) Анализ текущего состояния информационной инфраструктуры и кадрового потенциала.

В) Разработка программы мероприятий по достижению поставленных целей.

Г) Формулирование целей информационного менеджмента в соответствии со стратегией развития органа власти.

Д) Оценка ресурсных потребностей (финансовых, технических, человеческих).

Задание 1.1.2

Установите соответствие между уровнем управления информационной деятельностью и решаемыми задачами:

Уровень управления	Решаемые задачи
1. Стратегический уровень	А. Мониторинг текущей загрузки серверов, устранение сбоев
2. Тактический уровень	Б. Определение роли информационной системы в достижении целей государственной программы
3. Оперативный уровень	В. Разработка плана закупок оборудования на квартал, обучение сотрудников работе с новой системой

Задание 1.1.3

Выберите **все верные** утверждения о принципах эффективного информационного менеджмента в государственном секторе. **Кратко обоснуйте** каждый выбранный ответ.

а) Информационная система должна проектироваться с учётом действующих административных регламентов, а не наоборот.

б) Информационный менеджмент должен быть централизован, все решения принимаются исключительно на федеральном уровне.

в) Эффективность информационного менеджмента оценивается только по показателям освоения бюджетных средств.

г) Внедрение информационных систем требует сопровождения организационными изменениями (обучение, мотивация персонала).

д) Информационные системы государственных органов должны разрабатываться с учётом требований интеграции с ГИИС «Электронный бюджет».

Задание 1.1.4

Назовите не менее трёх факторов, определяющих специфику информационного менеджмента в государственных органах по сравнению с коммерческими организациями. Раскройте влияние каждого фактора на организацию информационной деятельности.

Задание 1.1.5

В государственном учреждении внедрена новая информационная система. Через год эксплуатации выяснилось, что показатели эффективности использования системы не достигнуты: 40% сотрудников не используют систему в полном объёме, данные обновляются несвоевременно. Проанализируйте возможные причины. Предложите систему ключевых показателей эффективности (KPI) для оценки использования информационной системы.

Тема 1.2. Информационные ресурсы, технологии и системы: классификация и архитектура

Задание 1.2.1

Расположите этапы проектирования государственной информационной системы в хронологической последовательности:

А) Разработка технического проекта (архитектура, состав модулей, интерфейсы).

Б) Формирование требований к информационной системе (функциональных и

нефункциональных).

В) Ввод системы в опытную эксплуатацию.

Г) Проведение приёмочных испытаний и подписание акта ввода в эксплуатацию.

Д) Разработка рабочей документации и программирование модулей.

Задание 1.2.2

Установите соответствие между компонентом информационной системы и его характеристикой:

Компонент ИС	Характеристика
1. Техническое обеспечение	А. Совокупность методов, алгоритмов и программ, реализующих функции системы
2. Программное обеспечение	Б. Комплекс правовых норм, регулирующих создание и эксплуатацию ИС
3. Информационное обеспечение	В. Компьютеры, сетевое оборудование, периферийные устройства
4. Правовое обеспечение	Г. Совокупность форм документов, классификаторов, базы данных

Задание 1.2.3

Выберите **все верные** утверждения о преимуществах сервис-ориентированной архитектуры (SOA) для государственных информационных систем. **Кратко обоснуйте** выбор.

а) SOA позволяет многократно использовать одни и те же сервисы разными приложениями, что снижает затраты на разработку.

б) Внедрение SOA требует полной замены всех существующих информационных систем, так как они несовместимы с сервисной архитектурой.

в) SOA упрощает интеграцию информационных систем разных ведомств за счёт использования стандартных протоколов и форматов.

г) SOA гарантирует абсолютную безопасность данных, так как все сервисы изолированы.

д) SOA обеспечивает гибкость и масштабируемость, позволяя добавлять новые сервисы без перестройки всей системы.

Задание 1.2.4

Назовите не менее трёх критериев выбора системы управления базами данных (СУБД) для государственной информационной системы. Для каждого критерия поясните, почему он значим для государственных органов.

Задание 1.2.5

Сравните подходы к созданию информационных систем «с нуля» (собственная разработка) и на основе типового (платформенного) решения. Укажите преимущества и недостатки каждого подхода для государственного учреждения с ограниченным бюджетом. Приведите примеры ситуаций, когда предпочтительна собственная разработка, а когда — типовое решение.

Тема 1.3. Нормативно-правовое регулирование информационной безопасности и защиты персональных данных

Компетенции:

Задание 1.3.1

Расположите в правильной последовательности действия оператора при получении требования Роскомнадзора об уточнении, блокировании или уничтожении персональных данных:

А) Уведомление субъекта персональных данных о принятых мерах (при необходимости).

Б) Получение мотивированного требования от Роскомнадзора.

В) Принятие мер по уточнению, блокированию или уничтожению персональных данных.

Г) Проведение внутренней проверки для подтверждения обоснованности требования.

Д) Направление в Роскомнадзор уведомления о результатах рассмотрения требования.

Задание 1.3.2

Установите соответствие между правовым документом и его основным содержанием в сфере информационной безопасности:

Правовой документ	Основное содержание

1. Указ Президента РФ № 188 от 06.03.1997	А. Перечень сведений конфиденциального характера
2. Постановление Правительства РФ № 687 от 15.09.2008	Б. Требования к защите персональных данных в ИСПДн
3. Постановление Правительства РФ № 1119 от 01.11.2012	В. Положение об особенностях обработки ПДн без использования средств автоматизации
4. Приказ ФСТЭК России № 21 от 18.02.2013	Г. Состав и содержание организационных и технических мер по обеспечению безопасности ПДн

Задание 1.3.3

Выберите **все верные** утверждения о порядке трансграничной передачи персональных данных. **Кратко обоснуйте** выбор.

а) Трансграничная передача персональных данных допускается только в страны, являющиеся сторонами Конвенции Совета Европы о защите персональных данных.

б) Для трансграничной передачи персональных данных в страны, не обеспечивающие адекватную защиту, требуется письменное согласие субъекта.

в) Оператор обязан уведомить Роскомнадзор о каждой трансграничной передаче персональных данных.

г) Запрет на трансграничную передачу персональных данных не распространяется на случаи, когда это необходимо для исполнения договора с субъектом.

д) Трансграничная передача персональных данных граждан Российской Федерации возможна только при условии локализации баз данных на территории РФ.

Задание 1.3.4

Перечислите не менее четырёх случаев, когда оператор персональных данных вправе осуществлять обработку персональных данных без уведомления Роскомнадзора (в соответствии с ч. 2 ст. 22 Федерального закона № 152-ФЗ).

Задание 1.3.5

В государственном учреждении обработка персональных данных осуществляется с использованием средств автоматизации. При проведении внутреннего аудита установлено, что не назначено лицо, ответственное за организацию обработки персональных данных, не утверждён перечень лиц, имеющих доступ к персональным данным, не проводится оценка вреда субъектам. Какие правовые последствия могут наступить для учреждения при проверке Роскомнадзором? Разработайте план устранения выявленных нарушений с указанием сроков и ответственных.

Раздел 2. Кибербезопасность и защита персональных данных в информационном менеджменте

Тема 2.1. Киберугрозы и система обеспечения информационной безопасности в государственных проектах

Задание 2.1.1

Расположите в логической последовательности действия по организации защиты информации в государственной информационной системе:

А) Разработка организационно-распорядительных документов по защите информации.

Б) Проведение аттестации информационной системы на соответствие требованиям безопасности.

В) Классификация информационной системы и определение требуемого уровня защищённости.

Г) Ввод системы в эксплуатацию с оформлением аттестата соответствия.

Д) Выбор и внедрение сертифицированных средств защиты информации.

Задание 2.1.2

Установите соответствие между типом уязвимости и возможной мерой по её устранению:

Тип уязвимости	Мера устранения
1. Использование устаревшего программного обеспечения	А. Настройка прав доступа, разделение тестового и продуктивного контуров

2. Несанкционированный доступ к тестовой среде	Б. Установка антивирусного ПО и регулярное сканирование
3. Отсутствие антивирусной защиты	В. Регулярное обновление версий ПО, установка патчей безопасности
4. Передача паролей по открытым каналам	Г. Использование защищённых протоколов (HTTPS, SSH), внедрение многофакторной аутентификации

Задание 2.1.3

Выберите **все верные** утверждения о методах противодействия атакам на канальном уровне сетевой модели OSI. **Кратко обоснуйте** выбор.

а) Для защиты от ARP-spoofing на коммутаторах можно настроить функцию Dynamic ARP Inspection (DAI).

б) Атака MAC-flooding приводит к переполнению таблицы MAC-адресов коммутатора, после чего он начинает работать как концентратор (широковещательная рассылка).

в) Защита от CAM-table overflow обеспечивается ограничением количества MAC-адресов на порту коммутатора.

г) Атака VLAN hopping невозможна, если все порты коммутатора настроены в режиме access.

д) Использование протокола STP не связано с безопасностью канального уровня и не влияет на защиту от атак.

Задание 2.1.4

Назовите не менее трёх методов защиты от вредоносного программного обеспечения, которые должны быть реализованы в государственной информационной системе. Для каждого метода укажите, на каком уровне (сетевом, хостовом, организационном) он реализуется.

Задание 2.1.5

При проведении анализа защищённости государственной информационной системы были выявлены следующие недостатки: на рабочих станциях не установлено антивирусное программное обеспечение, не настроены политики паролей, отсутствует контроль установки программного обеспечения пользователями. Оцените риски, связанные с каждым недостатком. Предложите приоритетный порядок устранения недостатков и обоснуйте его.

Тема 2.2. Организация защиты персональных данных в государственных информационных системах

Задание 2.2.1

Расположите в правильной последовательности этапы проведения оценки вреда, который может быть причинён субъектам персональных данных при нарушении Федерального закона № 152-ФЗ:

А) Определение степени возможного ущерба для субъекта (высокая, средняя, низкая).

Б) Формирование акта оценки вреда и его утверждение.

В) Идентификация обрабатываемых персональных данных и категорий субъектов.

Г) Выбор наивысшей степени вреда при наличии разных категорий субъектов.

Д) Анализ возможных последствий нарушения для прав и свобод субъектов.

Задание 2.2.2

Установите соответствие между видом нарушения законодательства о персональных данных и возможной мерой ответственности (по КоАП РФ):

Вид нарушения	Мера ответственности (штраф на юридическое лицо)
1. Обработка ПДн без согласия субъекта (ст. 13.11 ч. 2 КоАП РФ)	А. от 30 000 до 60 000 рублей
2. Невыполнение обязанности по опубликованию Политики обработки ПДн (ст. 13.11 ч. 3)	Б. от 15 000 до 75 000 рублей
3. Невыполнение требования субъекта об уточнении или уничтожении ПДн (ст. 13.11 ч. 5)	В. от 15 000 до 30 000 рублей
4. Необеспечение сохранности ПДн при их обработке без средств автоматизации (ст. 13.11 ч. 6)	Г. от 25 000 до 45 000 рублей

Задание 2.2.3

Выберите **все верные** утверждения о праве субъекта персональных данных на доступ к своим персональным данным. **Кратко обоснуйте** выбор.

а) Субъект имеет право на получение информации об источниках получения его персональных данных (если они получены не от него).

б) Оператор обязан предоставить субъекту копию персональных данных бесплатно.

в) Оператор может отказать в предоставлении информации, если запрос не содержит номера документа, удостоверяющего личность.

г) Субъект имеет право требовать исключения или исправления неверных персональных данных.

д) Оператор обязан ответить на запрос субъекта в течение 10 рабочих дней.

Задание 2.2.4

Назовите не менее трёх требований, предъявляемых к содержанию согласия на обработку персональных данных, разрешённых субъектом для распространения (в соответствии с Приказом Роскомнадзора от 24.02.2021 № 18).

Задание 2.2.5 (открытое)

Государственное учреждение планирует передать персональные данные граждан (фамилия, имя, отчество, адрес, телефон) третьей организации для осуществления доставки уведомлений. Разработайте проект согласия на обработку персональных данных, включая поручение на передачу третьему лицу. Укажите все необходимые элементы в соответствии с ч. 4 ст. 9 Федерального закона № 152-ФЗ.

Тема 2.3. Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография

Задание 2.3.1

Расположите в порядке убывания уровня защищённости (от наиболее защищённого к наименее защищённому) следующие средства защиты информации:

А) Антивирусная программа с эвристическим анализом и поведенческими блокираторами.

Б) Межсетевой экран нового поколения (NGFW) с функциями IPS и фильтрацией приложений.

В) Базовый межсетевой экран (пакетный фильтр) без инспектирования содержимого.

Г) Комплексная система защиты, включающая межсетевой экран, IDS/IPS, DLP-систему и антивирус.

Задание 2.3.2

Установите соответствие между режимом работы системы обнаружения атак и его характеристикой:

Режим работы	Характеристика
1. Пассивный (IDS)	А. Анализ трафика, блокировка подозрительных пакетов, перенастройка межсетевого экрана
2. Активный (IPS)	Б. Сбор и анализ трафика, генерация сигналов тревоги, без воздействия на трафик
3. Инлайн (inline)	В. Получение копии трафика через SPAN-порт, не влияет на его прохождение
4. Промиссинговый режим (promiscuous)	Г. Установка устройства в разрыв канала, активное влияние на передаваемый трафик

Задание 2.3.3

Выберите **все верные** утверждения о применении криптографических методов защиты информации в государственных информационных системах. **Кратко обоснуйте** выбор.

а) Использование криптографических средств, не сертифицированных ФСБ России, допускается для информации, не содержащей сведения, составляющие государственную тайну.

б) Электронная подпись позволяет установить авторство документа и проверить его целостность.

в) Асимметричное шифрование использует один ключ для шифрования и дешифрования, что обеспечивает высокую скорость работы.

г) Для шифрования каналов связи в государственных информационных системах рекомендуется использовать отечественные сертифицированные средства.

д) Хранение ключей шифрования в открытом виде в коде приложения не является нарушением, если само приложение защищено от несанкционированного доступа.

Задание 2.3.4

Назовите не менее трёх режимов работы межсетевого экрана (брандмауэра) и для каждого укажите, на каком уровне модели OSI он осуществляет фильтрацию.

Задание 2.3.5 (открытое)

В государственной информационной системе с высокими требованиями к безопасности необходимо организовать защищённый канал между центральным офисом и удалённым филиалом. Предложите решение, включающее выбор средств криптографической защиты информации (с обоснованием), протоколы и схему организации VPN-соединения. Укажите, какие требования предъявляются к сертификации выбранных средств.

Тема 2.4. Управление рисками информационной безопасности и реагирование на инциденты

Задание 2.4.1

Расположите этапы обработки инцидента информационной безопасности в государственной информационной системе в хронологической последовательности:

А) Локализация инцидента (изоляция поражённых сегментов, отключение учётных записей).

Б) Обнаружение инцидента (срабатывание IDS, сообщение пользователя, выявление аномалий).

В) Устранение последствий и восстановление работоспособности системы.

Г) Регистрация инцидента в журнале учёта событий безопасности.

Д) Расследование причин инцидента и анализ уязвимостей.

Е) Уведомление регуляторов (Роскомнадзора, ФСТЭК) при утечке персональных данных.

Задание 2.4.2

Установите соответствие между стратегией реагирования на риск информационной безопасности и её описанием:

Стратегия реагирования	Описание
1. Избежание риска	А. Передача риска страховой компании или подрядчику
2. Снижение риска	Б. Отказ от деятельности, связанной с риском (например, отказ от обработки определённых категорий данных)
3. Передача риска	В. Принятие риска на себя, создание резервного фонда
4. Принятие риска	Г. Внедрение дополнительных мер защиты для снижения вероятности или последствий

Задание 2.4.3

Выберите **все верные** утверждения о порядке взаимодействия оператора с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). **Кратко обоснуйте** выбор.

а) Операторы государственных информационных систем обязаны информировать ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу персональных данных.

б) Информирование осуществляется через Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

в) Уведомление направляется только в случае, если ущерб от инцидента превысил 1 млн рублей.

г) Порядок взаимодействия утверждён Приказом ФСБ России от 13.02.2023 № 77.

д) Оператор вправе не уведомлять о компьютерных инцидентах, если они не привели к утечке персональных данных.

Задание 2.4.4

Назовите не менее трёх количественных показателей (метрик) для оценки эффективности системы реагирования на инциденты информационной безопасности (например, MTTR, MTTA). Раскройте смысл каждого показателя.

Задание 2.4.5 (открытое)

В государственной информационной системе, обрабатывающей персональные данные, произошёл инцидент: злоумышленник скомпрометировал учётную запись администратора и скопировал базу данных. С момента обнаружения инцидента прошло 2 часа.

Вопросы:

1. Опишите дальнейший алгоритм действий (по шагам, с указанием ответственных).
2. Какие органы и в какие сроки необходимо уведомить?
3. Какие документы должны быть оформлены по результатам реагирования?
4. Разработайте проект уведомления Роскомнадзора об инциденте.

6.3. Критерии и шкала оценивания на основе БРС.

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

6.3. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Для выполнения тестовых заданий студенту разрешается использование MS Ecxel, калькулятора, финансовых таблиц.

7. Методические материалы по освоению дисциплины (модуля)

В рамках освоения дисциплины предусмотрены следующие формы работы: посещение лекций, практических занятий, подготовка докладов.

Дисциплина разбита на темы, которые представляют собой логически завершенные блоки и являются комплексом знаний, умений и навыков, которые подлежат контролю.

Контроль освоения тем включает в себя прохождение тестирования. В курсе используются классические аудиторные методы проведения занятий.

Освоение темы на лекции, при выполнении внеаудиторной (самостоятельной) работы, завершается на семинарском занятии.

Проведение занятий в форме лекций имеет своей целью обеспечение студентов теоретическими знаниями, развитие интереса к учебной деятельности и конкретной учебной дисциплине, сформирование ориентиров для самостоятельной работы над курсом. В ходе обучения применяются лекции следующих типов: вводная, информационная и обзорная, проблемная.

На семинарских занятиях предполагается рассматривать наиболее важные, существенные, сложные вопросы, которые наиболее трудно усваиваются при самостоятельном изучении дисциплины.

Для успешного овладения приемами решения конкретных задач предлагаются следующие этапы:

- предварительное ознакомление с методикой решения задач. На этом этапе студенту предлагаются типовые задачи, решение которых позволяет отработать приемы, использующиеся при их решении, осознать связь между полученными теоретическими знаниями и конкретными проблемами, на решение которых они могут быть направлены;

- рассматриваются задачи и ситуации, приближенные к практике государственного и муниципального управления;

- выполнение контрольной работы, позволяющей проверить навыки решения конкретных задач.

После каждого контрольного задания предусмотрено проведение консультаций по анализу наиболее типичных ошибок и выработке совместных рекомендаций по методике решения задач.

Внеаудиторная самостоятельная работа студентов над курсом организована в форме домашней работы, логически продолжающей аудиторные занятия по заданию преподавателя с установленными сроками исполнения.

Дидактические цели:

закрепление, углубление, расширение и систематизация знаний;

формирование умений;

самостоятельное овладение новым программным материалом;

развитие самостоятельности мышления.

Требования к выполнению самостоятельной работы.

1. Самостоятельная работа должна выполняться в соответствии заданием преподавателя.

2. Результаты самостоятельной работы должны иметь научную или практическую значимость, демонстрировать компетентность автора в раскрываемых вопросах, проявлять умения использовать теоретические знания при выполнении практических задач.

3. Самостоятельная работа, выполненная в письменной форме, должна быть оформлена в соответствии с требованиями и представлена для контроля преподавателю в установленные сроки.

Выполнение указанных требований учитывается при оценке самостоятельной работы обучающегося.

Виды самостоятельной работы: проработка лекций, чтение обязательной и дополнительной литературы, подготовка к опросу, написание реферата.

При самостоятельной подготовке к занятиям студенту необходимо:

- изучить теоретический материал по данной теме (конспект занятия); - ознакомиться с литературой, рекомендованной преподавателем;

- выполнить задания, предложенные преподавателем, к занятию;

- составить перечень вопросов, вызывающих затруднения, неясности или сомнения, обсудить их с преподавателем или на занятии.

Этапы выполнения самостоятельной работы:

- определение целей самостоятельной работы;
- конкретизация поставленной задачи;
- самооценка готовности к самостоятельной работе по решению поставленной или выбранной задачи;
- выбор путей и средств для решения поставленной задачи;
- планирование (самостоятельно или с помощью преподавателя) самостоятельной работы по решению задачи;
- реализация программы выполнения самостоятельной работы;
- самоконтроль промежуточных и конечного результатов работы, их корректировка - определение причин и устранение выявленных ошибок.

Вопросы для самостоятельной подготовки к занятиям лекционного курса

Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента

Тема 1.1. Информационный менеджмент: сущность, цели, задачи и место в системе государственного управления

1. Раскройте эволюцию понятия «информационный менеджмент». Какие этапы становления информационного менеджмента как самостоятельной дисциплины можно выделить?
2. Охарактеризуйте роль информации как стратегического ресурса в деятельности современного государственного органа. В чем отличие информации от других видов ресурсов?
3. Каковы основные цели и задачи информационного менеджмента в государственном секторе? Как они соотносятся с целями цифровой трансформации государственного управления?
4. Какие функции выполняет информационный менеджмент? Охарактеризуйте каждую функцию применительно к деятельности государственного проектного офиса.
5. Какова роль информационного менеджера в структуре органа власти? Какие компетенции необходимы современному информационному менеджеру в государственном секторе?

Тема 1.2. Информационные ресурсы, технологии и системы: классификация и архитектура

6. Что понимается под информационным ресурсом? Какие виды информационных ресурсов существуют и как они классифицируются?
7. В чем различие между информационными технологиями и информационными системами? Приведите примеры соотношения этих понятий.
8. Охарактеризуйте основные типы информационных систем, используемых в государственном управлении: ERP, CRM, СЭД, ГИС. В чем их функциональные различия?
9. Какие архитектуры информационных систем существуют (файл-сервер, клиент-сервер, SOA)? В чем их преимущества и недостатки для государственных информационных систем?
10. Каковы критерии выбора операционной системы и платформы для государственной информационной системы? Почему сегодня приоритет отдаётся отечественному программному обеспечению?

Тема 1.3. Нормативно-правовое регулирование информационной безопасности и защиты персональных данных

11. Какие нормативные правовые акты составляют основу правового регулирования информационной безопасности в Российской Федерации?
12. Раскройте основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
13. Какие права и обязанности оператора персональных данных установлены Федеральным законом от 27.07.2006 № 152-ФЗ?
14. Что такое «категории персональных данных»? Чем отличаются специальные, биометрические и общедоступные персональные данные?

15. Какие требования к защите информации предъявляют ФСТЭК России и ФСБ России к государственным информационным системам?

Раздел 2. Кибербезопасность и защита персональных данных в информационном менеджменте

Тема 2.1. Киберугрозы и система обеспечения информационной безопасности в государственных проектах

16. Что понимается под угрозой информационной безопасности? Как классифицируются угрозы по виду, характеру и источникам?

17. Какие угрозы являются наиболее актуальными для государственных информационных систем (DDoS, фишинг, вредоносное ПО)?

18. Что такое атаки на канальном уровне модели OSI (ARP-spoofing, MAC-spoofing, VLAN hopping)? Каков принцип их реализации?

19. Из каких элементов складывается система обеспечения информационной безопасности в государственном органе?

20. Каковы основные принципы построения системы защиты информации (запрет доступа по умолчанию, простота, перекрытие каналов утечки и др.)?

Тема 2.2. Организация защиты персональных данных в государственных информационных системах

21. Каков порядок получения согласия субъекта на обработку персональных данных? В каких случаях согласие не требуется?

22. Какие локальные нормативные акты должен разработать оператор персональных данных? Каковы требования к их содержанию?

23. Что такое обезличивание персональных данных? Какие методы обезличивания установлены приказом Роскомнадзора № 996?

24. Каков порядок уведомления Роскомнадзора о начале обработки персональных данных? В каких случаях уведомление не требуется?

25. Как осуществляется уничтожение персональных данных? Какие документы подтверждают факт уничтожения?

Тема 2.3. Технические средства и технологии кибербезопасности: IDS/IPS, межсетевые экраны, криптография

26. Что такое межсетевой экран (брандмауэр)? Как классифицируются межсетевые экраны по принципу работы?

27. В чем отличие системы обнаружения атак (IDS) от системы предотвращения атак (IPS)? Какие методы обнаружения используются в этих системах?

28. Что относится к средствам криптографической защиты информации (СКЗИ)? Каковы требования к их сертификации для использования в государственных информационных системах?

29. Что такое сниффер (анализатор трафика)? Как злоумышленники используют снифферы и как от них защититься?

30. Каковы основные протоколы и технологии организации защищённых каналов связи (VPN, TLS, IPsec)?

Тема 2.4. Управление рисками информационной безопасности и реагирование на инциденты

31. Что понимается под риском информационной безопасности? Какие существуют методы оценки рисков (количественные и качественные)?

32. Назовите и охарактеризуйте основные этапы управления рисками информационной безопасности.

33. Какие стратегии реагирования на риски существуют? В каких случаях применяется каждая стратегия?

34. Каков порядок действий оператора при обнаружении инцидента информационной безопасности (утечки персональных данных)?

35. Какова роль Национального координационного центра по компьютерным инцидентам (НКЦКИ)? Каков порядок взаимодействия операторов с НКЦКИ?

Вопросы для самостоятельной подготовки к семинарским занятиям

Раздел 1. Теоретические и нормативно-правовые основы информационного менеджмента

Семинар по теме 1.1. Информационный менеджмент как функция управления

1. Проведите сравнительный анализ подходов к информационному менеджменту в государственном и коммерческом секторах. Какие практики могут быть заимствованы государственными органами?

2. Проанализируйте типовую структуру управления информационной деятельностью в региональном органе власти. Какие недостатки такой структуры вы можете выделить?

3. Разработайте предложения по совершенствованию информационного менеджмента в государственном учреждении, где информационная система внедрена, но не используется персоналом в полном объёме.

4. Подготовьте аргументы для руководства о необходимости создания проектного офиса цифровой трансформации и выделения отдельной штатной единицы информационного менеджера.

Семинар по теме 1.2. Информационные ресурсы, технологии и системы

5. Сравните архитектуры «файл-сервер» и «клиент-сервер» с точки зрения безопасности, производительности и стоимости владения. Для какого типа государственных учреждений каждая архитектура предпочтительнее?

6. Проанализируйте современные тенденции в развитии государственных информационных систем (облачные технологии, искусственный интеллект, цифровые двойники). Какие перспективы их применения в государственном управлении?

7. Разработайте критерии выбора СУБД для государственной информационной системы с учётом требований импортозамещения.

8. Обсудите проблему интеграции разрознённых информационных систем в регионе. Какие архитектурные решения позволяют решить эту проблему без полной замены существующих систем?

Семинар по теме 1.3. Нормативно-правовое регулирование информационной безопасности

9. Проанализируйте судебную практику по спорам, связанным с нарушением Федерального закона № 152-ФЗ. Какие типичные нарушения допускаются государственными учреждениями?

10. Разработайте чек-лист для проверки готовности государственного учреждения к проверке Роскомнадзора по вопросам обработки персональных данных.

11. Подготовьте проект ответа на требование Роскомнадзора о предоставлении документов, подтверждающих принятие мер по защите персональных данных.

12. Обсудите правовые риски использования зарубежных облачных сервисов в деятельности государственных органов. Какие альтернативы существуют?

Раздел 2. Кибербезопасность и защита персональных данных

Семинар по теме 2.1. Киберугрозы и система обеспечения информационной безопасности

13. Проведите анализ типовой модели угроз для государственной информационной системы, обрабатывающей персональные данные. Какие угрозы являются наиболее критичными?

14. Разработайте программу повышения осведомлённости сотрудников государственного учреждения в области информационной безопасности.

15. Проанализируйте реальный кейс кибератаки на государственную информационную систему (из открытых источников). Какие меры позволили бы предотвратить или минимизировать последствия?

16. Подготовьте рекомендации по усилению защиты от атак на канальном уровне для локальной сети государственного учреждения.

Семинар по теме 2.2. Организация защиты персональных данных

17. Разработайте форму согласия на обработку персональных данных для посетителей государственного учреждения (сбор фамилии, контактного телефона, цели визита).

18. Составьте перечень мер по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

19. Проанализируйте методы обезличивания персональных данных и выберите оптимальный для публикации статистических данных о получателях социальных выплат (с сохранением возможности анализа).

20. Подготовьте план мероприятий по приведению обработки персональных данных в государственном учреждении в соответствие с требованиями 152-ФЗ.

Семинар по теме 2.3. Технические средства кибербезопасности

21. Проведите сравнительный анализ отечественных средств криптографической защиты информации (СКЗИ), сертифицированных ФСБ России. Какие решения наиболее оптимальны для государственной информационной системы среднего масштаба?

22. Разработайте правила фильтрации трафика для межсетевого экрана, обеспечивающие доступ к веб-порталу ГИС из сети Интернет и запрещающие доступ к административным интерфейсам.

23. Проанализируйте лог-файлы системы обнаружения атак и определите характер атаки (по описанию). Предложите меры реагирования.

24. Настройте политику антивирусной защиты для сегмента сети, в котором обрабатываются персональные данные.

Семинар по теме 2.4. Управление рисками и реагирование на инциденты

25. Проведите количественную оценку рисков информационной безопасности для типового государственного проекта. Рассчитайте ожидаемую стоимость рисков (EMV) и обоснуйте резерв бюджета.

26. Разработайте план реагирования на инцидент информационной безопасности для государственной информационной системы, обрабатывающей персональные данные.

27. Проведите деловую игру «Реагирование на утечку персональных данных»: распределите роли, проиграйте действия, подготовьте необходимые документы (уведомления, акты, отчёты).

28. Проанализируйте эффективность применяемых в государственном учреждении мер защиты информации и предложите направления их совершенствования с учётом принципа рациональности (баланс затрат и эффективности).

В рамках дисциплины «*Информационный менеджмент*» разработаны и доступны обучающимся развёрнутые учебно-методические материалы для самостоятельной работы, включающие: методические указания для работы на семинарских занятиях с рекомендациями по выполнению заданий и кейсов, подготовке к тестированию и написанию эссе/докладов. Все указанные материалы размещены в электронной информационно-образовательной среде. Доступ к материалам осуществляется по индивидуальному логину и паролю студента.

8. Учебная литература и ресурсы информационно- телекоммуникационной сети Интернет

8.1. Основная литература

1. Камолов, С. Г. Цифровое государственное управление : учебник для вузов / С. Г. Камолов, Н. Д. Александров. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2025. — 287 с. — (Высшее образование). — ISBN 978-5-534-21027-9. — URL: https://urait.ru/bcode/559179 (дата обращения: 19.05.2026).

2. Косоруков, А. А. Цифровые технологии в системе государственного и муниципального управления : учебник для вузов / А. А. Косоруков. — Москва : Ай Пи Ар Медиа, 2024. — 208 с. — ISBN 978-5-4497-2492-4. — URL: https://www.iprbookshop.ru/134011.html (дата обращения: 19.05.2026).

3. Романова, Ю. Д. Информационные технологии в менеджменте (управлении) : учебник и практикум для вузов / Ю. Д. Романова [и др.] ; под ред. Ю. Д. Романовой. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2025. — 467 с. — (Высшее образование). — ISBN 978-5-534-17035-1. — URL: https://urait.ru/book/informacionnye-tehnologii-v-menedzhmente-upravlenii-565605 (дата обращения: 19.05.2026).

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2024. — 416 с. — ISBN 978-5-8199-0754-2. — URL: https://znanium.ru/catalog/document?id=442922 (дата обращения: 19.05.2026).

8.2. Дополнительная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — URL: https://www.urait.ru/bcode/537247 (дата обращения: 19.05.2026).

2. Косоруков, А. А. Цифровизация государственного управления : учебное пособие / А. А. Косоруков. — Москва : Ай Пи Ар Медиа, 2025. — 244 с. — ISBN 978-5-4497-2491-7. — URL: https://library.arsu.kz/?p=32021 (дата обращения: 19.05.2026).

3. Менеджмент : учебник для вузов / под общ. ред. В. Г. Антонова. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2025. — (Высшее образование). — URL: https://urait.ru/book/menedzhment-560008 (дата обращения: 19.05.2026).

8.3. Нормативные правовые акты

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 28.12.2025). — URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.05.2026).

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025). — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 19.05.2026).

3. Федеральный закон от 28.12.2024 № 519-ФЗ «О внесении изменений в статьи 10 и 11 Федерального закона "О персональных данных" и отдельные законодательные акты Российской Федерации». — URL: https://legalacts.ru/doc/federalnyi-zakon-ot-28122024-n-519-fz-o-vnesenii-izmenenii/ (дата обращения: 19.05.2026).

4. Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств...» (ред. от 28.11.2025). — URL: https://www.consultant.ru/document/cons_doc_LAW_189522/ (дата обращения: 19.05.2026).

5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных...». — URL: https://www.consultant.ru/document/cons_doc_LAW_137672/ (дата обращения: 19.05.2026).

6. Приказ Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к обезличиванию персональных данных...». — URL: https://www.consultant.ru (дата обращения: 19.05.2026).

7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер...». — URL: https://www.consultant.ru/document/cons_doc_LAW_145539/ (дата обращения: 19.05.2026).

8.4. Интернет-ресурсы

1. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. — URL: https://digital.gov.ru/ (дата обращения: 19.05.2026).

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). — URL: https://rkn.gov.ru/ (дата обращения: 19.05.2026).

3. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). — URL: https://fstec.ru/ (дата обращения: 19.05.2026).

4. Портал проектного управления Правительства Российской Федерации. — URL: https://pm.expert/ (дата обращения: 19.05.2026).

5. ГИИС «Электронный бюджет». — URL: https://budget.gov.ru/ (дата обращения: 19.05.2026).

6. Единая информационная система в сфере закупок (ЕИС). — URL: https://zakupki.gov.ru/ (дата обращения: 19.05.2026).

7. Справочная правовая система «КонсультантПлюс». — URL: https://www.consultant.ru/ (дата обращения: 19.05.2026).

8. Научная электронная библиотека eLIBRARY.RU. — URL: https://elibrary.ru/ (дата обращения: 19.05.2026).

9. Образовательная платформа «Юрайт». — URL: https://urait.ru/ (дата обращения: 19.05.2026).

10. Электронно-библиотечная система Znanium. — URL: https://znanium.ru/ (дата обращения: 19.05.2026).

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

Технические средства – компьютерная техника, проектор, флипчарт

Методы обучения с использованием информационных технологий:

- демонстрация лекционных материалов с использованием мультимедийной технологии.

Информационно-справочные системы и Интернет-ресурсы:

- www.consultant.ru – Справочная правовая система «Консультант Плюс»;
- www.garant-park.ru – Справочная правовая система «Гарант».
- https:/lms.ranepa.ru/ - СДО Академии.

Материально-техническое и программное обеспечение дисциплины

Для проведения лекций требуются аудитории, оснащенные мультимедийной техникой. Для проведения практических занятий требуются аудитории, оборудованные мобильными столами, стульями, доской.

Самостоятельная работа по дисциплине проводится с частичным применением ДОТ.

Для подключения к СДО требуется наличие компьютерной техники с выходом в Интернет.