Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года 6 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Кандидат физико-математических наук Абрамов Н. В.

Кандидат наук Ткаченко С. П.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Задачи изучения дисциплины:

- составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации;
- анализ изменения угроз безопасности информации , возникающих в ходе ее эксплуатации.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-1.1 Разрабатывает прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-1.1/Зн1 Знать особенности разработки прототипов ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС

Уметь:

ПК-1.1/Ум1 Уметь разрабатывать прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС

Владеть:

ПК-1.1/Нв1 Навыками разработки прототипов ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС

ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Знать:

ПК-1.2/Зн1 Программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Уметь:

ПК-1.2/Ум1 Создавать программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Владеть:

ПК-1.2/Нв1 Навыками создания программного кода ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС

ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.2/Зн1 Необходимые меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Уметь:

ПК-2.2/Ум1 Оценивать меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Владеть:

ПК-2.2/Нв1 Навыками обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

ПК-3 Способен управлять инициацией, разработкой и реализацией проектов в области информационных технологий, внедрять продукт проекта в деятельность организаций

ПК-3.1 Инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием

Знать:

ПК-3.1/Зн1 Как планируется проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием

Уметь:

ПК-3.1/Ум1 Планировать проект в области ИТ, организовывать исполнение работ проекта в соответствии с трудовым заданием

Владеть:

ПК-3.1/Нв1 Навыками планирования проекта в области ИТ, организации и исполнения работ в соответствии с трудовым заданием

ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС

Знать:

ПК-4.1/Зн1 Особенностей требований к Системе и концептуально-логически проектирует ИС

Уметь:

ПК-4.1/Ум1 Анализировать требования к Системе и концептуально-логически проектирует ИС

Владеть:

ПК-4.1/Нв1 Навыками формирования требований к Системе и концептуально-логически проектировать ИС

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Теория информационной безопасности и методология защиты информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 5.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-1 - Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы		

ПК-1.1 Разрабатывает прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС	Вычислительные системы, сети и телекоммуникации, Информационно-коммуникационные технологии в профессиональной деятельности, Нейросетевые технологии в социальных медиа, Основы проектной деятельности, Системы искусственного интеллекта, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Встроенные языки программирования, Выполнение и защита выпускной квалификационной работы, Вычислительные системы, сети и телекоммуникации, Моделирование процессов и систем, Организация вычислительных процессов, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, Системы искусственного интеллекта, Управление информационной безопасностью, Учебная практика: технологическая (проектно-технологическая) практика
ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	Основы алгоритмизации и программирования, Системы искусственного интеллекта, Современные технологии и языки программирования, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Методы и средства защиты информации, Организация вычислительных процессов, Программно-аппаратная защита информации, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, Системы искусственного интеллекта, Современные технологии и языки программирования, Современные цифровые технологии управления предприятием, Управление информационными проектами реализации комплексной безопасности, Учебная практика: технологическая (проектно-технологическая) практика

ПК-2 - Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС		
ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Криптографическая защита информации, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации, Учебная практика: технологическая (проектно-технологическая) практика
ПК-3 - Способен управлять инициацией, разработкой и реализацией проектов в области информационных технологий, внедрять продукт проекта в деятельность организаций		
ПК-3.1 Инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием	Основы проектной деятельности, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Учебная практика: технологическая (проектно-технологическая) практика
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС	Основы проектной деятельности, Системы искусственного интеллекта, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Компьютерная экспертиза, Методы и средства защиты информации, Моделирование процессов и систем, Организационная защита информации, Организация вычислительных процессов, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Современные цифровые технологии управления предприятием, Специализированные ИТ в правоохранительной деятельности, Учебная практика: технологическая (проектно-технологическая) практика, Цифровая культура в профессиональной деятельности

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Пятый семестр	108	3	4	2	2	2	0,3	67,7	Экзамен
Всего	108	3	4	2	2	2	0,3	67,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы		ные занятия	ые занятия	ельная работа

	Всего	Лаборатор	Лекционн	Самостоят
Раздел 1. Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей ИС	**33,3**	**1**	**1**	**30**
Тема 1.1. Понятие информации и информационной безопасности. ГОСТы на ИС. Типовые виды структуры ИС. Угрозы безопасности ИС и их классификация	33,3	1	1	30
Раздел 2. Способы защиты ИС от угроз информационной безопасности	**40,7**	**1**	**1**	**37,7**
Тема 2.1. Пассивная и активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика технических каналов утечки информации.(ТКУИ). Понятие контролируемой зоны и методы определения ее размеров.	40,7	1	1	37,7

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	тестирование
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей ИС	тестирование	Экзамен
2	Способы защиты ИС от угроз информационной безопасности	тестирование	Экзамен

6. Оценочные материалы текущего контроля

1. Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей ИС тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Разработка и конкретизация правовых нормативных актов обеспечения безопасности - Хищение жестких дисков, подключение к сети, инсайдерство - Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы		ПК-1

	Ответ:	Перехват данных, хищение данных, изменение архитектуры системы	
2	Виды информационной безопасности - Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная		ПК-1
	Ответ:	Персональная, корпоративная, государственная	
3	Как называется умышленно искаженная информация - Дезинформация - Информативный поток - Достоверная информация - Перестает быть информацией		ПК-1
	Ответ:	Дезинформация	
4	Как называется информация, к которой ограничен доступ - Конфиденциальная - Противозаконная - Открытая - Недоступная		ПК-1
	Ответ:	Конфиденциальная	
5	Какими путями может быть получена информация - проведением, покупкой и противоправным добыванием информации научных исследований - захватом и взломом ПК информации научных исследований - добыванием информации из внешних источников и скремблированием информации научных исследовании - захватом и взломом защитной системы для информации научных исследований		ПК-2
	Ответ:	проведением, покупкой и противоправным добыванием информации научных исследований	
6	Как называются компьютерные системы, в которых обеспечивается безопасность информации - защищенные КС - небезопасные КС - самодостаточные КС - саморегулирующиеся КС		ПК-2
	Ответ:	защищенные КС	
7	Основной документ, на основе которого проводится политика информационной безопасности - программа информационной безопасности - регламент информационной безопасности - политическая информационная безопасность - протекторат		ПК-2
	Ответ:	программа информационной безопасности	
8	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности 1. Сотрудники 2. Хакеры 3. Атакующие 4. Контрагенты (лица, работающие по договору)		ПК-1
	Ответ:	Сотрудники	
9	Кто является основным ответственным за определение уровня классификации информации? 1. Руководитель среднего звена 2. Высшее руководство 3. Владелец 4. Пользователь		ПК-1
	Ответ:	Владелец	
10	Что самое главное должно продумать руководство при классификации данных 1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным 2. Необходимый уровень доступности, целостности и конфиденциальности 3. Оценить уровень риска и отменить контрмеры 4. Управление доступом, которое должно защищать данные		ПК-2
	Ответ:	Необходимый уровень доступности, целостности и конфиденциальности	
11	Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены 1. Владельцы данных 2. Пользователи 3. Администраторы 4. Руководство		ПК-1
	Ответ:	Руководство	
12	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков 1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски 2. Когда риски не могут быть приняты во внимание по политическим соображениям 3. Когда необходимые защитные меры слишком сложны 4. Когда стоимость контрмер превышает ценность актива и потенциальные потери		ПК-2

	Ответ:	Когда стоимость контрмер превышает ценность актива и потенциальные потери	
13	Что такое политики безопасности 1. Пошаговые инструкции по выполнению задач безопасности 2. Общие руководящие требования по достижению определенного уровня безопасности 3. Широкие, высокоуровневые заявления руководства 4. Детализированные документы по обработке инцидентов безопасности		ПК-2
	Ответ:	Общие руководящие требования по достижению определенного уровня безопасности	
14	Эффективная программа безопасности требует сбалансированного применения 1. Технических и не технических методов 2. Контрмер и защитных механизмов 3. Физической безопасности и технических средств защиты 4. Процедур безопасности и шифрования		ПК-2
	Ответ:	Технических и не технических методов	

2. Способы защиты ИС от угроз информационной безопасности тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Что называют защитой информации - Все ответы верны - Называют деятельность по предотвращению утечки защищаемой информации - Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию - Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию		ПК-3
	Ответ:	Все ответы верны	
2	Под непреднамеренным воздействием на защищаемую информацию понимают - Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений - Процесс ее преобразования, при котором содержание информации изменяется на ложную - Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию - Не ограничения доступа в отдельные отрасли экономики или на конкретные производства		ПК-4
	Ответ:	Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений	
3	Основные предметные направления Защиты Информации - Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности - Охрана золотого фонда страны - Определение ценности информации - Усовершенствование скорости передачи информации		ПК-3
	Ответ:	Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности	
4	Государственная тайна это - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны - ограничения доступа в отдельные отрасли экономики или на конкретные производства - защищаемые банками и иными кредитными организациями сведения о банковских операциях - защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей		ПК-2
	Ответ:	защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны	

5	Коммерческая тайна это - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны - ограничения доступа в отдельные отрасли экономики или на конкретные производства - защищаемые банками и иными кредитными организациями сведения о банковских операциях - защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей Банковская тайна это…. - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны - ограничения доступа в отдельные отрасли экономики или на конкретные производства + защищаемые банками и иными кредитными организациями сведения о банковских операциях - защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей Профессиональная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны - ограничения доступа в отдельные отрасли экономики или на конкретные производства - защищаемые банками и иными кредитными организациями сведения о банковских операциях + защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей Ответ: ограничения доступа в отдельные отрасли экономики или на конкретные производства	ПК-2
6	Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право - управление доступом - конфиденциальность - аутентичность - целостность - доступность Ответ: конфиденциальность	ПК-3
7	Какая из перечисленных атак на поток информации является пассивной - перехват. - имитация. - модификация. - фальсификация. - прерывание. Ответ: перехват.	ПК-4
8	Можно выделить следующие направления мер информационной безопасности - Правовые - Организационные - Все ответы верны - Технические Ответ: Все ответы верны	ПК-4
9	Потенциальные угрозы, против которых направлены технические меры защиты информации - Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей - Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения - Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками. - Потери информации из-за не достаточной установки сигнализации в помещении. - Процессы преобразования, при котором информация удаляется Ответ: Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей	ПК-2
10	Шифрование информации это - Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов - Процесс преобразования, при котором информация удаляется - Процесс ее преобразования, при котором содержание информации изменяется на ложную - Процесс преобразования информации в машинный код Ответ: Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов	ПК-3
11	Какие сбои оборудования бывают? - сбои работы серверов, рабочих станций, сетевых карт и т.д. - потери при заражении системы компьютерными вирусами - несанкционированное копирование, уничтожение или подделка информации - ознакомление с конфиденциальной информацией Ответ: сбои работы серверов, рабочих станций, сетевых карт и т.д.	ПК-3

12	Какие потери информации бывают из-за некорректной работы программ? - сбои работы серверов, рабочих станций, сетевых карт и т.д. - перебои электропитания - потеря или изменение данных при ошибках ПО - ознакомление с конфиденциальной информацией		ПК-3
	Ответ:	потеря или изменение данных при ошибках ПО	
13	Какие потери информации, связанные с несанкционированным доступом, бывают - несанкционированное копирование, уничтожение или подделка информации - потери при заражении системы компьютерными вирусами - случайное уничтожение или изменение данных - сбои дисковых систем		ПК-4
	Ответ:	несанкционированное копирование, уничтожение или подделка информации	
14	Потери из-за ошибки персонала и пользователей бывают - несанкционированное копирование, уничтожение или подделка информации - потери при заражении системы компьютерными вирусами - случайное уничтожение или изменение данных - сбои дисковых систем		ПК-1
	Ответ:	случайное уничтожение или изменение данных	
15	Средства защиты данных, функционирующие в составе программного обеспечения. - Программные средства защиты информации - Технические средства защиты информации - Источники бесперебойного питания (UPS) - Смешанные средства защиты информации		ПК-1
	Ответ:	Программные средства защиты информации	

7. Оценочные материалы промежуточной аттестации

Экзамен пятый семестр

№ п/п	Содержание вопроса		Компетенция
	Правильный ответ (ключ ответа)		
1	Программное средство защиты информации. - криптография - программный источник бесперебойного питания - программа резервного копирования - дублирование данных		ПК-1
	Ответ:	криптография	
2	Обеспечение доступа к информации только авторизованным пользователям? - Конфиденциальность - Секретность - Доступность - Целесообразность		ПК-3
	Ответ:	Конфиденциальность	
3	Наибольшую угрозу для безопасности сети представляют. - несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение - вскрытие стандартной учётной записи пользователя - вскрытие стандартной учётной группы администратора - копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании		ПК-4
	Ответ:	несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение	
4	Защита через права доступа заключается. - присвоении каждому пользователю определенного набора прав -запереть серверы в специальном помещении с ограниченным доступом -присвоить пароль каждому общедоступному ресурсу - в наличии преобразователя для микрофона		ПК-2
	Ответ:	присвоении каждому пользователю определенного набора прав	

5	Дифференцированное резервное копирование это -Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании -Копирование всех выбранных файлов без отметки о резервном копировании -Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования -Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании	ПК-4
	Ответ: Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании	
6	Полное копирование данных это -Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования -Копирование всех выбранных файлов без отметки о резервном копировании -Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании -Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования	ПК-3
	Ответ: Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени	
7	Наиболее простой и недорогой метод предотвратить катастрофическую потерю данных -Резервное копирование на магнитную ленту -Шифрование данных -Бездисковые компьютеры -Все ответы верны	ПК-4
	Ответ: Резервное копирование на магнитную ленту	
8	Право Read дает вам возможность -Удаление файлов в каталоге -Запуск (выполнение) программ из каталога -Запрещение на доступ к каталогу, файлу, ресурсу -Чтение и копирование файлов из совместно используемого каталога	ПК-2
	Ответ: Чтение и копирование файлов из совместно используемого каталога	
9	Право Write дает вам возможность -Удаление файлов в каталоге -Запрещение на доступ к каталогу, файлу, ресурсу -Создание новых файлов в каталоге -Чтение и копирование файлов из совместно используемого каталога	ПК-4
	Ответ: Создание новых файлов в каталоге	
10	Ежедневное копирование данных это -Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании -Копирование всех выбранных файлов без отметки о резервном копировании -Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования -Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании	ПК-3
	Ответ: Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копирован	

7.1. Уровни овладения

Компетенция: ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.

Индикатор достижения компетенции: ПК-1.1 Разрабатывает прототипы ИС на базе типовой ИС в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика	Оценка в баллах

Повышенный	Прфессиональные навыки при разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	81-100
Базовый	Самостоятельно определять круг задач при разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	61-80
Пороговый	В общих чертах ориентируется в разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	41-60
Ниже порогового	Материал не освоен в достаточном объеме	0-40

Индикатор достижения компетенции: ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления.

Уровень	Характеристика	Оценка в баллах
Повышенный	Создает оптимальный программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	81-100
Базовый	Уверенно создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	61-80
Пороговый	С не критичными ошибками создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	41-60
Ниже порогового	Материал не освоен в достаточном объеме	0-40

Компетенция: ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС.

Индикатор достижения компетенции: ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика	Оценка в баллах
Повышенный	Принимает врвентивные меры в случае обнаружения известных инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	81-100
Базовый	Принимает меры в случае обнаружения известных инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	61-80

Пороговый	Принимает меры в случае обнаружения явных инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	41-60
Ниже порогового	Материал не освоен в достаточном объеме	0-40

Компетенция: ПК-3 Способен управлять инициацией, разработкой и реализацией проектов в области информационных технологий, внедрять продукт проекта в деятельность организаций.

Индикатор достижения компетенции: ПК-3.1 Инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием.

Уровень	Характеристика	Оценка в баллах
Повышенный	Творчески инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием	81-100
Базовый	Уверенно инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием	61-80
Пороговый	Повехстно инициирует и планирует проект в области ИТ, организует исполнение работ проекта в соответствии с трудовым заданием	41-60
Ниже порогового	Материал не освоен в достаточном объеме	0-40

Компетенция: ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений.

Индикатор достижения компетенции: ПК-4.1 Выявляет требования к Системе и концептуально-логически проектирует ИС.

Уровень	Характеристика	Оценка в баллах
Повышенный	Выявляет оптимальные требования к Системе и концептуально-логически проектирует ИС	81-100
Базовый	Уверенно выявляет требования к Системе и концептуально-логически проектирует ИС	61-80
Пороговый	Выявляет не все требования к Системе и концептуально-логически проектирует ИС	41-60
Ниже порогового	Материал не освоен в достаточном объеме	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. - 2-е изд. - Москва: Юрайт, 2026. - 107 с - 978-5-534-16388-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588741 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва: Юрайт, 2026. - 349 с - 978-5-534-19762-4. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583858 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Внуков, А. А. Защита информации: учебник для вузов / А. А. Внуков. - 3-е изд. - Москва: Юрайт, 2026. - 161 с - 978-5-534-07248-8. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584050 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://edu.gov.ru/ - Министерство просвещения Российской Федерации (Минпросвещения России)
2. https://lms2.sseu.ru - БРСО
3. https://digital.gov.ru - Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. LibreOffice;
2. 7-Zip;
3. «Альт Образование» и/или «Альт Рабочая станция»;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Справочно-правовая система "Гарант-Максимум";

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ

Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения