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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ПРОЕКТАМИ РЕАЛИЗАЦИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ»

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: 4 з.е.
в академических часах: 144 ак.ч.

г. Самара, 2026

Разработчики:
Не имеет Колотилина М. А.

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 теоретических знаний и практических навыков по управлению информационными проектами в области комплексной безопасности, включая планирование, организацию, контроль и оценку эффективности проектов по защите информации.

Задачи изучения дисциплины:

- Изучить методологии управления ИТ-проектами (Waterfall, Agile, Scrum, PMBOK), этапы жизненного цикла проектов в области комплексной безопасности и нормативно-правовые требования к проектам защиты информации.;
- Освоить методы планирования, бюджетирования, управления рисками и ресурсами проектов по созданию систем защиты информации, включая оценку эффективности и контроль качества реализации.;
- Сформировать навыки управления проектами по внедрению и сопровождению комплексной системы защиты информации, документального оформления проектных решений, мониторинга хода работ и применения корректирующих воздействий..

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

Знать:

ПК-1.2/Зн1 Методы и технологии управления информационными проектами в области комплексной безопасности (Waterfall, Agile, Scrum, PMBOK), требования к созданию программного кода с учетом требований информационной безопасности, принципы интеграции средств защиты информации в прототипы ИС на этапе разработки.

Уметь:

ПК-1.2/Ум1 Создавать программный код ИС с учетом требований безопасности на этапе разработки прототипов, применять методы управления проектами для планирования и контроля создания защищенных ИС, интегрировать средства защиты информации (аутентификация, шифрование, контроль доступа) в разрабатываемые прототипы, обеспечивать соответствие кода требованиям комплексной безопасности.

Владеть:

ПК-1.2/Нв1 Навыками разработки защищенного программного кода с учетом требований проектов комплексной безопасности, методами управления проектами создания ИС, приемами интеграции средств защиты информации в прототипы, навыками документирования и сопровождения проектных решений в области комплексной безопасности.

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-2.1 Верифицирует ИС в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.1/Зн1 Методы и технологии верификации ИС с учетом требований комплексной безопасности, подходы к интеграционному тестированию и проверке работоспособности средств защиты информации, критерии оценки соответствия ИС требованиям безопасности на этапе тестирования, регламенты проведения верификации в рамках управления проектами.

Уметь:

ПК-2.1/Ум1 Применять методы верификации ИС для проверки соответствия реализованных механизмов защиты требованиям проектной документации, проводить интеграционное тестирование средств защиты информации (СКУД, антивирусы, шифрование), выявлять и документировать отклонения и несоответствия требованиям безопасности.

Владеть:

ПК-2.1/Нв1 Навыками разработки планов и сценариев верификации для проектов комплексной безопасности, методами интеграционного тестирования защищенных ИС, приемами анализа результатов верификации и подготовки отчетной документации для управления проектом, навыками взаимодействия с разработчиками для устранения выявленных отклонений.

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

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС

Знать:

ПК-4.2/Зн1 Методологии выявления требований к комплексной безопасности в рамках ИТ-проектов (системный анализ, моделирование угроз, управление рисками), принципы концептуально-логического проектирования систем защиты информации, нормативно-правовые требования к проектам в области ИБ (152-ФЗ, приказы ФСТЭК/ФСБ, ГОСТы), методы оценки эффективности и критерии выбора проектных решений для сопровождения.

Уметь:

ПК-4.2/Ум1 Применять методы системного анализа для выявления требований к комплексной безопасности, разрабатывать концептуальные и логические модели систем защиты информации (модели угроз, архитектура СЗИ, схемы управления доступом), актуализировать проектные решения при изменении нормативных требований, угроз или состава объектов защиты, обосновывать выбор организационных и технических решений для сопровождения проектов.

Владеть:

ПК-4.2/Нв1 Навыками формирования технического задания с разделом требований к комплексной безопасности, методами проектирования и сопровождения систем защиты информации в рамках проектов, приемами верификации проектных решений на соответствие требованиям безопасности, методиками согласования требований к комплексной безопасности с заинтересованными сторонами и документирования результатов проектирования и сопровождения.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Управление информационными проектами реализации комплексной безопасности» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 8.

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-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Интеллектуальные информационные системы, Методы и средства защиты информации, Организация вычислительных процессов, Основы алгоритмизации и программирования, Программно-аппаратная защита информации, Проектирование информационных систем, Проектный практикум, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Современные технологии и языки программирования, Современные цифровые технологии управления предприятием, Теория информационной безопасности и методология защиты информации, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Разработка профессиональных приложений, Современные цифровые технологии управления предприятием
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-2.1 Верифицирует ИС в рамках выполнения работ по созданию и сопровождению ИС	Вычислительные системы, сети и телекоммуникации, Компьютерная экспертиза, Моделирование процессов и систем, Правовая защита информации, Проектирование информационных систем, Производственная практика: технологическая (проектно-технологическая) практика, Специализированные ИТ в правоохранительной деятельности, Управление информационной безопасностью, Учебная практика: технологическая (проектно-технологическая) практика, Цифровая культура в профессиональной деятельности	Выполнение и защита выпускной квалификационной работы, Проектирование информационных систем, Производственная практика: преддипломная практика, Специализированные ИТ в правоохранительной деятельности, Управление информационной безопасностью, Цифровая культура в профессиональной деятельности
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС	Информационно-коммуникационные технологии в профессиональной деятельности, Криптографическая защита информации, Нейросетевые технологии в социальных медиа, Облачные технологии и услуги, Основы проектной деятельности, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации, Технологии защищенного документооборота, Учебная практика: технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика

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
Восьмой семестр	144	4	4	2	2	2	0,3	103,7	Экзамен
Всего	144	4	4	2	2	2	0,3	103,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Лекционные занятия	Самостоятельная работа
Раздел 1. Управление информационными проектами реализации комплексной безопасности	**110**	**2**	**2**	**103,7**

Тема 1.1. Введение в управление информационными проектами в области комплексной безопасности: основные понятия и определения (проект, управление проектом, комплексная безопасность, информационная безопасность, жизненный цикл проекта); классификация проектов в области ИБ (внедрение СЗИ, аттестация объектов, разработка защищенных ИС); методологии управления проектами (Waterfall, Agile, Scrum, PMBOK, ГОСТ Р 54869-2011, ГОСТ Р ИСО 21500); нормативно-правовые требования к проектам в области защиты информации (152-ФЗ, 187-ФЗ, приказы ФСТЭК и ФСБ); роль руководителя проекта и команды; основные этапы управления проектами комплексной безопасности.	110	2	2	103,7

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестовое задание
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Управление информационными проектами реализации комплексной безопасности	Тестовое задание	Экзамен

6. Оценочные материалы текущего контроля

1. Управление информационными проектами реализации комплексной безопасности Тестовое задание

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	

1	Для автоматизации бизнес-процесса принятия кредитных решений в банке проектируется архитектура экспертной системы. Какая архитектурная модель обеспечивает наилучшую сопровождаемость и возможность модификации механизма вывода без изменения базы знаний и интерфейса пользователя? 1. Монолитная, где все компоненты выполняются в одном процессе 2. Двухзвенная клиент-серверная с хранением правил на клиенте 3. Компонентная (слабо связанные модули БЗ, механизма вывода и подсистемы объяснения) 4. Архитектура «тонкий клиент» с удалённым рабочим столом 5. Файл-серверная с общим сетевым хранилищем Ответ: 3	ПК-1
2	При разработке прототипа ИС для диагностики оборудования предприятия вы проводите интервью с экспертом. Какой метод инженерии знаний предполагает построение модели организации, задач и агента, что позволяет увязать логику ЭС с целевыми бизнес-процессами управления ремонтами? 1. Анализ протоколов «мыслей вслух» 2. CommonKADS (модель организации – задачи – аген) 3. Метод сортировки карточек (Repertory Grid) 4. Метод DELTA 5. Мозговой штурм без структурирования Ответ: 2	ПК-1
3	При проектировании базы знаний для системы управления персоналом (автоматизация подбора кадров) требуется описать иерархию должностей с наследованием атрибутов (требования к стажу, навыкам). Какой способ представления знаний следует выбрать для реализации такого прототипа? 1. Продукционная модель 2. Логическая модель (исчисление предикатов первого порядка) 3. Фреймовая модель со слотами и наследованием 4. Семантическая сеть без иерархии 5.Нейросетевая модель «чёрный ящик» Ответ: 3	ПК-1
4	В прототипе ЭС для оценки инвестиционных рисков используется коэффициент уверенности (CF). Согласно модели MYCIN, какое числовое значение CF соответствует полной уверенности в ложности утверждения? 1. +1.0 2. 0.0 3. -1.0 4. 0.5 5. 0.75 Ответ: 3	ПК-1
5	После завершения концептуализации предметной области для ЭС поддержки логистических бизнес-процессов вы переходите к созданию работающего прототипа. На каком этапе производится кодирование правил на языке инструментальной среды (например, CLIPS) с последующей отладкой синтаксиса? 11. Идентификация 2. Формализация (реализация / кодирование знаний) 3. Тестирование на тестовых примерах 4. Промышленное внедрение 5. Сопровождение и модификация Ответ: 2	ПК-1
6	Установите соответствие между этапом создания (или модификации) ИС для организационного управления и содержанием работ при разработке архитектуры и прототипа ЭС. **Этап** — **Содержание работ** 1. Идентификация — А. Кодирование продукционных правил в среде CLIPS с проверкой синтаксиса 2. [illegible] — Б. Сбор требований от заказчика, определение границ	ПК-1

	2. Концептуализация — Б. Сбор требований от заказчика, определение границ автоматизации бизнес-процесса 3. Формализация — В. Построение графа целей и задач, выделение сущностей и отношений предметной области 4. Валидация — Г. Сравнение результатов работы прототипа с эталонными решениями эксперта	
	Ответ: 1-Б, 2-В, 3-А, 4-Г	
7	Установите соответствие между типовой задачей, решаемой экспертной системой, и примером бизнес-процесса организационного управления, который она автоматизирует. **Тип задачи ЭС** — **Пример бизнес-процесса** 1. Диагностика — А. Формирование штатного расписания и графика отпусков 2. Интерпретация данных — Б. Определение причины отклонения параметров работы оборудования от нормы 3. Планирование — В. Расшифровка показаний датчиков склада для инвентаризации 4. Принятие решений — Г. Одобрение или отклонение заявки на командировку по заданным критериям	ПК-1
	Ответ: 1-Б, 2-В, 3-А, 4-Г	
8	Установите соответствие между компонентом архитектуры прототипа ИС и его функциональным назначением в процессе сопровождения и модификации системы. **Компонент архитектуры** — **Функция** 1. Подсистема объяснения — А. Обеспечивает прослеживаемость логики вывода для пользователя и эксперта 2. Механизм вывода — Б. Хранит правила и факты, которые могут быть изменены без перекомпиляции всей системы 3. База знаний — В. Реализует стратегию разрешения конфликтов и управления цепочкой правил 4. Интерфейс ввода/вывода — Г. Обеспечивает интеграцию с корпоративными источниками данных и UI для бизнес-пользователей	ПК-1
	Ответ: 1-А, 2-В, 3-Б, 4-Г	
9	Расположите в правильной последовательности этапы разработки прототипа ИС на базе типовой конфигурации 1С: 1 Демонстрация прототипа заказчику и согласование 2 Сбор требований и анализ бизнес-процессов 3 Доработка типовой конфигурации (настройка, расширения) 4 Выбор типовой конфигурации (например, Управление торговлей) 5 Разработка макетов интерфейсов и отчетов 6 Утверждение прототипа и переход к разработке	ПК-1
	Ответ: 2 → 4 → 5 → 3 → 1 → 6	
10	Расположите в правильной последовательности шаги создания программного кода для разработки отчета в СКД 1С: 1 Создание объекта метаданных «Отчет» 2 Написание и настройка запроса в СКД 3 Настройка макета отчета (группировки, поля, параметры) 4 Тестирование и отладка отчета 5 Сохранение и включение отчета в конфигурацию	ПК-1
	Ответ: 1 → 2 → 3 → 4 → 5	
11	Дайте развернутый ответ В рамках разработки прототипа ИС на базе типовой для автоматизации управления заказами опишите, как вы проведете анализ требований и выберете типовую конфигурацию 1С.	ПК-1
	Ответ: 1. Интервью с заказчиком; 2. Анализ бизнес-процессов (BPMN); 3. Сравнение типовых конфигураций (1С:УНФ, 1С:УТ, 1С:ERP); 4. Выбор по критериям: функциональность, стоимость, масштабируемость; 5. Формирование ТЗ на доработку прототипа.	
12	Дайте развернутый ответ Опишите процесс создания программного кода для документа «Поступление товаров» в 1С: проведение документа должно формировать движения по регистру накопления «Товары на складах».	ПК-1

	Ответ:	1. Создать документ «Поступление товаров» с реквизитами (Организация, Склад, Контрагент) и табличной частью (Номенклатура, Количество, Цена, Сумма); 2. В модуле документа в обработчике проведения написать алгоритм формирования движений по регистру накопления «Товары на складах» (приход); 3. Использовать запросы для контроля остатков; 4. Отладить и протестировать.	
13	Дайте развернутый ответ В рамках выполнения работ по созданию и сопровождению ИС опишите, как вы организуете процесс модификации типовой конфигурации 1С с использованием расширений.		ПК-1
	Ответ:	1. Создать расширение в 1С:Конфигуратор; 2. Определить объекты для изменения (справочники, документы, отчеты); 3. В расширении выполнить необходимые доработки (добавление реквизитов, изменение модулей); 4. Провести тестирование; 5. Установить расширение для пользователей; 6. Обновить документацию.	
14	Дайте развернутый ответ В рамках разработки прототипа рассчитайте ориентировочное время (в часах) на разработку документа «Заказ клиента» и отчета по заказам, если на проектирование требуется 4 часа, на написание кода – 16 часов, на тестирование – 4 часа, на отладку – 2 часа. Ответ дайте числом.		ПК-1
	Ответ:	4 + 16 + 4 + 2 = 26 часов.	
15	Дайте развернутый ответ Опишите план разработки прототипа ИС для автоматизации учета времени сотрудников на базе типовой конфигурации 1С. Какие объекты и отчеты вы будете разрабатывать?		ПК-1
	Ответ:	Объекты: справочник «Сотрудники», документ «Табель учета рабочего времени», регистр накопления «Отработанное время». Отчеты: «Сводка по отработанным часам», «Табель за период». Прототип включает макеты документов, отчетов и настройку прав доступа.	
16	В рамках разработки прототипа ИС на базе типовой ИС для учета товаров вы должны выбрать типовую конфигурацию 1С. Какая конфигурация подходит для автоматизации торгового предприятия? a) 1С:Управление торговлей b) 1С:Бухгалтерия c) 1С:Зарплата и управление персоналом d) 1С:Управление строительной организацией		ПК-1
	Ответ:	a	
17	При создании программного кода ИС на платформе 1С для автоматизации бизнес-процесса закупок вы должны реализовать контроль остатков при проведении документа. Какой язык используется для написания алгоритмов бизнес-логики? a) Python b) Java c) Встроенный язык 1С d) C++		ПК-1
	Ответ:	c	
18	В рамках разработки прототипа ИС на базе типовой вы должны создать макет отчета по продажам. Какой инструмент 1С позволяет разрабатывать отчеты с визуальным конструктором? a) СКД (Система компоновки данных) b) Конфигуратор c) Конструктор запросов d) Отладчик		ПК-1
	Ответ:	a	
19	При создании программного кода в 1С вам нужно выбрать объект метаданных для хранения справочной информации о сотрудниках. Какой объект используется? a) Документ b) Регистр накопления c) Справочник d) План счетов		ПК-1
	Ответ:	c)	
20	В рамках разработки прототипа ИС вы должны согласовать требования с заказчиком. Какой документ фиксирует результаты согласования прототипа? a) Техническое задание (ТЗ) b) Руководство пользователя c) Программа испытаний d) Акт выполненных работ		ПК-1
	Ответ:	a	
21	Соотнесите этап разработки прототипа ИС на базе типовой с его содержанием:		ПК-1

Этап	Содержание
1. Анализ требований	А. Создание работающих макетов интерфейсов и отчетов
2. Прототипирование	Б. Сбор и формализация потребностей заказчика, обследование бизнес-процессов
3. Согласование прототипа	В. Представление прототипа заказчику, сбор замечаний, утверждение

	Ответ: 1–Б, 2–А, 3–В	
22	Соотнесите объект метаданных 1С с его назначением при создании программного кода: **Объект** — **Назначение** 1. Справочник — А. Хранение хозяйственных операций с проведением по регистрам 2. Документ — Б. Отображение сводной информации по данным, с возможностью формирования в печатный вид 3. Отчет — В. Хранение условно-постоянной информации (номенклатура, контрагенты) Ответ: 1–В, 2–А, 3–Б	ПК-1
23	Соотнесите вид доработки типовой ИС с его целью при создании (модификации) ИС на базе типовой: **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей Ответ: 1–А, 2–В, 3–Б	ПК-1
24	Расположите в правильной последовательности этапы разработки прототипа ИС на базе типовой конфигурации 1С: 1 Демонстрация прототипа заказчику и согласование 2 Сбор требований и анализ бизнес-процессов 3 Доработка типовой конфигурации (настройка, расширения) 4 Выбор типовой конфигурации (например, Управление торговлей) 5 Разработка макетов интерфейсов и отчетов 6 Утверждение прототипа и переход к разработке **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей Ответ: 2 → 4 → 5 → 3 → 1 → 6	ПК-1
25	Расположите в правильной последовательности шаги создания программного кода для разработки отчета в СКД 1С: 1 Создание объекта метаданных «Отчет» 2 Написание и настройка запроса в СКД 3 Настройка макета отчета (группировки, поля, параметры) 4 Тестирование и отладка отчета 5 Сохранение и включение отчета в конфигурацию **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей	ПК-1

	Ответ:	1 → 2 → 3 → 4 → 5
26	Дайте развернутый ответ В рамках разработки прототипа ИС на базе типовой для автоматизации управления заказами опишите, как вы проведете анализ требований и выберете типовую конфигурацию 1С. **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей	ПК-1
	Ответ:	1. Интервью с заказчиком; 2. Анализ бизнес-процессов (BPMN); 3. Сравнение типовых конфигураций (1С:УНФ, 1С:УТ, 1С:ERP); 4. Выбор по критериям: функциональность, стоимость, масштабируемость; 5. Формирование ТЗ на доработку прототипа.
27	Дайте развернутый ответ Опишите процесс создания программного кода для документа «Поступление товаров» в 1С: проведение документа должно формировать движения по регистру накопления «Товары на складах». **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей	ПК-1
	Ответ:	1. Создать документ «Поступление товаров» с реквизитами (Организация, Склад, Контрагент) и табличной частью (Номенклатура, Количество, Цена, Сумма); 2. В модуле документа в обработчике проведения написать алгоритм формирования движений по регистру накопления «Товары на складах» (приход); 3. Использовать запросы для контроля остатков; 4. Отладить и протестировать.
28	Дайте развернутый ответ В рамках выполнения работ по созданию и сопровождению ИС опишите, как вы организуете процесс модификации типовой конфигурации 1С с использованием расширений. **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей	ПК-1
	Ответ:	1. Создать расширение в 1С:Конфигуратор; 2. Определить объекты для изменения (справочники, документы, отчеты); 3. В расширении выполнить необходимые доработки (добавление реквизитов, изменение модулей); 4. Провести тестирование; 5. Установить расширение для пользователей; 6. Обновить документацию.
29	Дайте развернутый ответ В рамках разработки прототипа рассчитайте ориентировочное время (в часах) на разработку документа «Заказ клиента» и отчета по заказам, если на проектирование требуется 4 часа, на написание кода – 16 часов, на тестирование – 4 часа, на отладку – 2 часа. Ответ дайте числом. **Вид доработки** — **Цель** 1. Создание расширения — А. Добавление новых отчетов и обработок без изменения типовой конфигурации 2. Настройка прав доступа — Б. Обеспечение соответствия бизнес-логики требованиям заказчика 3. Изменение алгоритмов проведения документов — В. Ограничение доступа к данным в соответствии с ролями пользователей	ПК-1
	Ответ:	4 + 16 + 4 + 2 = 26 часов.
30	Дайте развернутый ответ Опишите план разработки прототипа ИС для автоматизации учета времени сотрудников на базе типовой конфигурации 1С. Какие объекты и отчеты вы будете разрабатывать?	ПК-1

Вид доработки	Цель
1. Создание расширения	А. Добавление новых отчетов и обработок без изменения типовой конфигурации
2. Настройка прав доступа	Б. Обеспечение соответствия бизнес-логики требованиям заказчика
3. Изменение алгоритмов проведения документов	В. Ограничение доступа к данным в соответствии с ролями пользователей

Ответ: Объекты: справочник «Сотрудники», документ «Табель учета рабочего времени», регистр накопления «Отработанное время». Отчеты: «Сводка по отработанным часам», «Табель за период». Прототип включает макеты документов, отчетов и настройку прав доступа.

31 При верификации ИС в рамках проекта комплексной безопасности, какой метод тестирования позволяет проверить взаимодействие всех компонентов системы с учетом требований защиты информации?
a) модульное тестирование
b) интеграционное тестирование
c) нагрузочное тестирование
d) тестирование пользовательского интерфейса
ПК-2

Ответ: b

32 При обнаружении инцидента ИБ в ходе сопровождения ИС, какой документ должен быть оформлен для фиксации нарушения?
a) техническое задание
b) акт об инциденте ИБ
c) бизнес-план
d) маркетинговый план
ПК-2

Ответ: b

33 При тестировании ИС на соответствие требованиям комплексной безопасности, какой вид анализа позволяет выявить уязвимости в программном коде без его запуска?
a) статический анализ (SAST)
b) динамический анализ (DAST)
c) нагрузочное тестирование
d) тестирование на проникновение
ПК-2

Ответ: a

34 При верификации ИС, какие показатели позволяют оценить степень защищенности системы от несанкционированного доступа?
a) количество строк кода
b) уровень покрытия кода тестами и результаты пентеста
c) объем базы данных
d) количество пользователей
ПК-2

Ответ: b

35 При обнаружении инцидента ИБ в рамках сопровождения ИС, какое действие должно быть выполнено в первую очередь?
a) увольнение сотрудника
b) изоляция затронутого компонента и сохранение доказательств
c) перезагрузка системы
d) удаление логов
ПК-2

Ответ: b

36 Установите соответствие между видом тестирования (1–3) и его целью (A–C) при верификации ИС в рамках проекта комплексной безопасности. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C).
ПК-2

Вид тестирования	Цель тестирования
1. Модульное тестирование	A. Проверка системы на наличие уязвимостей и защищенность от атак
2. Интеграционное тестирование	B. Проверка корректности работы отдельных компонентов и модулей
3. Тестирование безопасности	C. Проверка взаимодействия компонентов системы с учетом СЗИ

Ответ: 1-B, 2-C, 3-A

37 Установите соответствие между инструментом обнаружения (1–3) и его назначением (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C).
ПК-2

Инструмент	Назначение

	1. SIEM-система — A. Обнаружение уязвимостей в веб-приложениях 2. Burp Suite — B. Централизованный сбор и корреляция событий безопасности 3. OWASP ZAP — C. Сканирование и пентест веб-приложений Ответ: 1-B, 2-C, 3-A	
38	Установите соответствие между стадией реагирования на инцидент ИБ (1–3) и её содержанием (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Стадия реагирования — Содержание стадии 1. Обнаружение и локализация — A. Устранение уязвимости, обновление СЗИ 2. Устранение — B. Мониторинг аномалий, идентификация затронутых компонентов 3. Анализ и предотвращение — C. Документирование, анализ причин, разработка мер предотвращения Ответ: 1-B, 2-A, 3-C	ПК-2
39	Установите правильную последовательность действий при обнаружении инцидента ИБ в ИС в рамках сопровождения ИС. Расположите буквы (A–D) в верном порядке. A) Изоляция затронутого компонента и сохранение доказательств B) Обнаружение аномалии (сигнал от SIEM, сообщение от пользователя) C) Устранение инцидента (исправление, обновление СЗИ) D) Документирование инцидента и анализ причин Ответ: B → A → C → D	ПК-2
40	Установите правильную последовательность этапов верификации ИС при проверке соответствия требованиям комплексной безопасности. Расположите буквы (A–D) в верном порядке. A) Проверка соответствия СЗИ требованиям проектной документации B) Интеграционное тестирование компонентов системы C) Составление акта верификации и передача результатов заказчику D) Анализ результатов и документирование отклонений Ответ: A → B → D → C	ПК-2
41	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух признаков инцидента ИБ, которые могут быть выявлены при тестировании ИС в рамках проекта комплексной безопасности. Ответ: необычные исходящие соединения, появление неизвестных файлов, аномалии в логах доступа, ошибки аутентификации, сбои в работе СЗИ, нехарактерная активность пользователей.	ПК-2
42	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в ИС, какие меры должны быть приняты для обеспечения сохранности доказательств? Ответ: изоляция затронутого компонента, создание резервных копий логов и данных, сохранение дампов памяти, фотофиксация состояния системы, документирование времени и характера инцидента, привлечение экспертов для расследования.	ПК-2
43	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов тестирования, используемых при верификации ИС для проверки защищенности от атак. Ответ: тестирование на проникновение (пентест), статический анализ кода (SAST), динамический анализ (DAST), сканирование уязвимостей, анализ конфигурации безопасности.	ПК-2
44	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ, связанного с утечкой данных, какие меры должны быть приняты в рамках сопровождения ИС? Ответ: изоляция уязвимого компонента, проверка журналов доступа, смена паролей и ключей, уведомление заинтересованных сторон и регулятора (при необходимости), усиление контроля доступа, проведение расследования.	ПК-2
45	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов мониторинга, используемых для обнаружения инцидентов ИБ в процессе сопровождения ИС. Ответ: SIEM-системы (Splunk, QRadar, ArcSight), системы обнаружения вторжений (IDS/IPS), WAF (Web Application Firewall), системы мониторинга логов, DLP-системы.	ПК-2
46	При выявлении требований к Системе для проекта комплексной безопасности, какие требования учитывают необходимость защиты информации от утечки по техническим каналам? a) функциональные требования b) требования к технической защите информации c) требования к интерфейсу d) требования к производительности	ПК-4

	Ответ: b	
47	На этапе концептуально-логического проектирования ИС, какая модель используется для описания угроз и определения мер защиты? a) ER-диаграмма b) модель угроз (моделирование угроз) c) UML-диаграмма классов d) BPMN-диаграмма Ответ: b	ПК-4
48	При выявлении требований к Системе для проекта комплексной безопасности, какой нормативный документ является основным для определения требований к защите персональных данных? a) 152-ФЗ «О персональных данных» b) 63-ФЗ «Об электронной подписи» c) ISO 9001 d) ITIL Ответ: a	ПК-4
49	Что является результатом этапа выявления требований к комплексной безопасности для ИС? a) исходный код приложения b) техническое задание с разделом требований к безопасности и защите c) маркетинговый план d) бизнес-план Ответ: b	ПК-4
50	При сопровождении разработанных проектных решений по комплексной безопасности, какие действия необходимо выполнять при изменении требований регуляторов? a) игнорирование изменений b) актуализация требований, пересмотр проектных решений и документации c) переустановка системы d) замена оборудования Ответ: b	ПК-4
51	Установите соответствие между этапом проектирования ИС (1–3) и его содержанием (A–C) в области комплексной безопасности. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап проектирования | Содержание в области комплексной безопасности 1. Выявление требований | A. Разработка модели угроз и архитектуры СЗИ 2. Концептуально-логическое проектирование | B. Определение требований к защите от утечек, НСД, шифрованию 3. Сопровождение проектных решений | C. Актуализация документации при изменении угроз и требований Ответ: 1-B, 2-A, 3-C	ПК-4
52	Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при выявлении требований к Системе в области комплексной безопасности. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Нормативный документ | Содержание требований 1. 152-ФЗ «О персональных данных» | A. Требования к обеспечению безопасности объектов КИИ 2. 187-ФЗ «О безопасности КИИ» | B. Требования к защите персональных данных в ИС 3. Приказы ФСТЭК России | C. Требования к технической защите информации Ответ: 1-B, 2-A, 3-C	ПК-4
53	Установите соответствие между методом защиты информации (1–3) и его назначением (A–C) при выявлении требований к Системе для проекта комплексной безопасности. В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Метод защиты | Назначение 1. Шифрование | A. Ограничение доступа к информации по ролям 2. Разграничение доступа | B. Подтверждение подлинности пользователя 3. Аутентификация | C. Обеспечение конфиденциальности данных Ответ: 1-C, 2-A, 3-B	ПК-4

54	Установите правильную последовательность этапов выявления требований к комплексной безопасности для ИС. Расположите буквы (A–D) в верном порядке. A) Анализ нормативно-правовых требований (152-ФЗ, 187-ФЗ, приказы ФСТЭК) B) Определение перечня защищаемых объектов и угроз C) Определение требований к СЗИ (шифрование, контроль доступа, аудит) D) Формирование раздела требований к безопасности в ТЗ		ПК-4
	Ответ:	A → B → C → D	
55	Установите правильную последовательность действий при сопровождении проектных решений по комплексной безопасности при изменении требований. Расположите буквы (A–D) в верном порядке. A) Оценка влияния изменений на систему безопасности B) Получение запроса на изменение (изменение законодательства, угроз) C) Актуализация проектной документации и повторное согласование D) Внесение изменений в систему безопасности и тестирование		ПК-4
	Ответ:	B → A → D → C	
56	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов выявления требований к комплексной безопасности для ИС.		ПК-4
	Ответ:	анализ нормативно-правовых документов (152-ФЗ, 187-ФЗ), проведение моделирования угроз, аудит существующей системы безопасности, интервьюирование заинтересованных сторон, анализ рисков.	
57	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой артефакт разрабатывается на этапе концептуально-логического проектирования в области комплексной безопасности?		ПК-4
	Ответ:	модель угроз, архитектура системы защиты информации, схема разграничения доступа (RBAC), перечень технических средств защиты, план мероприятий по обеспечению безопасности.	
58	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Для чего используется модель угроз при выявлении требований к Системе в проектах комплексной безопасности?		ПК-4
	Ответ:	для идентификации всех возможных угроз, уязвимостей и каналов атак, а также для обоснования выбора мер защиты и определения необходимого уровня защищенности системы.	
59	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании системы комплексной безопасности для ИС, обрабатывающей персональные данные.		ПК-4
	Ответ:	152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ», Приказы ФСТЭК России, 63-ФЗ «Об электронной подписи».	
60	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для проекта комплексной безопасности?		ПК-4
	Ответ:	раздел «Требования к комплексной безопасности и защите информации» (включая требования к защите от утечек, НСД, шифрованию, аутентификации, аудиту, резервному копированию и восстановлению).	

7. Оценочные материалы промежуточной аттестации

Экзамен восьмой семестр

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При создании программного кода для автоматизации бизнес-процессов с учетом комплексной безопасности, какие средства защиты информации должны быть интегрированы в код на этапе разработки прототипа?		ПК-1
	Ответ:	аутентификация (OAuth, JWT), разграничение доступа (RBAC), шифрование данных (AES, TLS), логирование событий (аудит), защита от инъекций и XSS.	
2	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух подходов к разработке прототипов ИС в проектах комплексной безопасности, которые позволяют минимизировать риски безопасности на ранних этапах.		ПК-1
	Ответ:	прототипирование с использованием моделей угроз, применение безопасных библиотек и фреймворков, проведение статического анализа кода на этапе прототипирования, использование принципа наименьших привилегий.	
3	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При создании программного кода в проекте комплексной безопасности, какие требования к коду должны быть соблюдены для обеспечения возможности его дальнейшего сопровождения?		ПК-1
	Ответ:	документирование кода (комментарии, Readme), использование системы контроля версий (Git), модульная структура, покрытие тестами, соответствие корпоративным стандартам кодирования.	
4	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух инструментов, используемых для управления проектами и создания программного кода в проектах комплексной безопасности.		ПК-1
	Ответ:	Jira (управление задачами), Git (контроль версий), Jenkins/GitLab CI (непрерывная интеграция), SonarQube (анализ качества кода и безопасности), Docker (контейнеризация).	

5	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При верификации ИС в проекте комплексной безопасности, какие виды тестирования должны быть выполнены для проверки работоспособности средств защиты информации (СЗИ)?		ПК-2
	Ответ:	интеграционное тестирование СЗИ с компонентами ИС, тестирование безопасности (пентест, сканирование уязвимостей), функциональное тестирование механизмов аутентификации и авторизации, нагрузочное тестирование.	
6	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При обнаружении инцидента ИБ в ходе сопровождения ИС, какие действия должен выполнить руководитель проекта для минимизации последствий?		ПК-2
	Ответ:	оперативная изоляция затронутого компонента, активация плана реагирования на инциденты, уведомление заинтересованных сторон, привлечение экспертов для расследования, документирование инцидента, анализ причин и разработка мер предотвращения.	
7	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух метрик, используемых для оценки эффективности верификации ИС в проектах комплексной безопасности.		ПК-2
	Ответ:	количество выявленных критических уязвимостей, процент покрытия кода тестами (код-ревью), время устранения дефектов, количество успешно завершенных тест-кейсов.	
8	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При выявлении требований к Системе для проекта комплексной безопасности, какие требования необходимо собрать для обеспечения защиты объекта критической информационной инфраструктуры (КИИ)?		ПК-4
	Ответ:	требования к категорированию объекта КИИ, требования к обеспечению непрерывности работы (отказоустойчивость, резервирование), требования к защите от внешних и внутренних угроз, требования к мониторингу и реагированию на инциденты, требования к импортозамещению.	
9	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). При сопровождении разработанных проектных решений по комплексной безопасности, какие действия необходимо выполнить при выявлении новой уязвимости (например, в используемом ПО)?		ПК-4
	Ответ:	провести оценку рисков и критичности уязвимости, разработать план устранения (обновление ПО, установка патча, внесение изменений в конфигурацию), актуализировать документацию, провести повторное тестирование, согласовать изменения с заинтересованными сторонами.	
10	Дайте краткий письменный ответ (слово, словосочетание или 1–2 предложения). Назовите не менее двух методов, используемых для выявления требований к концептуально-логическому проектированию систем комплексной безопасности.		ПК-4
	Ответ:	моделирование угроз (STRIDE, OCTAVE), анализ рисков, проведение аудита существующих систем, интервью с экспертами, анализ нормативно-правовых требований, метод «мозгового штурма».	

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

Уровень	Характеристика
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.
Ниже порогового	Компетенция не освоена

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-2.1 Верифицирует ИС в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.
Ниже порогового	Компетенция не освоена

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

Индикатор достижения компетенции: ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС.

Уровень	Характеристика
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.
Ниже порогового	Компетенция не освоена

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Алексанов, Д. С. Управление проектами в АПК: учебник для вузов / Д. С. Алексанов, В. М. Кошелев, Н. В. Чекмарева. - Москва: Юрайт, 2026. - 193 с - 978-5-534-15176-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589040 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Зуб, А. Т. Управление изменениями: учебник и практикум для вузов / А. Т. Зуб. - Москва: Юрайт, 2026. - 284 с - 978-5-534-00490-8. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583130 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Зуб, А. Т. Управление проектами: учебник и практикум для вузов / А. Т. Зуб. - 2-е изд. - Москва: Юрайт, 2026. - 397 с - 978-5-534-17500-4. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583111 (дата обращения: 21.05.2026). - Режим доступа: по подписке

3. Козырь, Н. С. Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. - Москва: Юрайт, 2026. - 131 с - 978-5-534-17863-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589431 (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://stepik.org - Платформа с онлайн-курсами от авторов-практиков

2. : https://meganorm.ru/Index/51/51696.htm - ГОСТ Р 54869-2011 «Проектный менеджмент. Требования к управлению проектом»: страница стандарта на портале МЕГАНОРМ с возможностью скачать полный текст . Национальный стандарт РФ, описывающий процессы инициации, организации, контроля и завершения проекта, а также требования к управлению документами .

3. https://platformaofd.ru/articles/kak-nachat-rabotu-s-platforma-edo/ - Платформа ЭДО — как подключиться

Инструкция по подключению к сервису электронного документооборота. Описаны способы работы (веб-версия, мобильное приложение, интеграция с 1С через API), получение квалифицированной электронной подписи (КЭП) и регистрация в системе .

4. https://www.pmi.org/standards/pmbok - PMBoK (Project Management Body of Knowledge) Guide: официальная страница свода знаний от PMI (Project Management Institute) . Актуальное 8-е издание (2025 г.) включает 6 ключевых принципов, 7 областей производительности и обновлённые разделы по ИИ и управлению проектами . В отличие от ГОСТ Р 54869-2011, PMBoK выделяет 10 областей знаний (включая управление рисками и заинтересованными сторонами), что особенно актуально для проектов в сфере комплексной безопасности .

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)

Не используется.

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 СП
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения