МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ЧЕБОКСАРСКИЙ ИНСТИТУТ (ФИЛИАЛ) МОСКОВСКОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Кафедра Информационных технологий и систем управления

УТВЕРЖДАЮ
Директор филиала
_____А.В. Агафонов
"27" мая 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационные системы специального назначения»
(наименование дисциплины)

Направление подготовки	**09.04.01 «Информатика и вычислительная техника»**
	(код и наименование направления подготовки)
Направленность (профиль) подготовки	**«Информационное и программное обеспечение вычислительной техники и автоматизированных систем»**
	(наименование профиля подготовки)
Квалификация выпускника	**магистр**
Форма обучения	**очная, заочная**
Год начала обучения	**2026**

Чебоксары, 2026

Рабочая программа дисциплины разработана в соответствии с:

- Федеральный государственный образовательный стандарт высшего образования – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 918 от 19 сентября 2017 года, зарегистрированный в Минюсте 9 октября 2017 года, рег. номер N 48478;
- учебным планом (очной, заочной форм обучения) по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Рабочая программ дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (п.6 Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины)

Автор Пикина Наталия Евгеньевна, кандидат педагогических наук, доцент кафедры информационных технологий и систем управления

(указать ФИО, ученую степень, ученое звание или должность)

Программа одобрена на заседании кафедры Информационных технологий и систем управления (протокол № 9 от 22.05.2026 г.).

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

1.1. *Целями* освоения дисциплины «Информационные системы специального назначения» являются:

формирование у обучающихся системного понимания принципов построения, архитектурных решений, математического, программного и технического обеспечения информационных систем, предназначенных для решения задач в условиях особых требований к информационной безопасности, отказоустойчивости, оперативности и достоверности обработки данных.

Для достижения целей дисциплины необходимо решить следующую *основную задачу* – сформировать у обучающихся теоретические знания и практические навыки, необходимые для:

изучения методологий проектирования и верификации ИС специального назначения;

формирование компетенций по анализу угроз и выбору методов защиты информации;

обучение оценке надежности и живучести ИС СН в условиях кибератак и деструктивных воздействий.

1.2. Области профессиональной деятельности и(или) сферы профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере проектирования, разработки, модернизации средств вычислительной техники и информационных систем).

1.3. К основным задачам изучения дисциплины относится подготовка обучающихся к выполнению трудовых функций в соответствии с профессиональными стандартами:

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.017 Руководитель разработки программного обеспечения	C	Управление программно-техническими, технологическими и человеческими ресурсами для разработки компьютерного программного обеспечения	7	Управление инфраструктурой коллективной среды разработки компьютерного программного обеспечения	C/01.7	7
			7	Управление рисками разработки компьютерного программного обеспечения	C/02.7	
			7	Управление процессами оценки сложности, трудоемкости, сроков выполнения работ	C/03.7	

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.027 Специалист по администрированию сетевых устройств информационно-коммуникационных систем	F	Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения	7	Документирование ошибок в работе сетевых устройств и программного обеспечения	F/02.7	7

1.4. Компетенции обучающегося, формируемые в результате освоения дисциплины

Наименование категории (группы) компетенций	**Код и наименование компетенций**	**Код и наименование индикатора достижения компетенции**	**Перечень планируемых результатов обучения**
Разработка, отладка, проверка работоспособности, модификация программного обеспечения	ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	ОПК-7.1. Знать: функциональные требования к прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования	*на уровне знаний:* знать международные стандарты информационного обмена; основные положения теории информационной безопасности. *на уровне умений:* уметь применять международные стандарты информационного обмена; основные положения теории информационной безопасности. *на уровне навыков:* навыками применения международных стандартов информационного обмена; основных положений теории информационной безопасности.
		ОПК-7.2. Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными	*на уровне знаний:* знать информационные системы безопасности, национальные стандарты. *на уровне умений:* уметь разрабатывать

Наименование категории (группы) компетенций	Код и наименование компетенций	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения
		стандартами, интегрировать с отраслевыми информационными системами	информационные системы безопасности *на уровне навыков:* навыками разработки информационных систем безопасности
		ОПК-7.3. Владеть: методами настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций	*на уровне знаний:* знать интерфейс, шаблоны. подключение библиотек. *на уровне умений:* уметь выбирать методы настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций. *на уровне навыков:* навыками настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.Д(М).Б.9 «Информационные системы специального назначения» реализуется в рамках обязательной части Блока 1 «Дисциплины (модули)» программы магистратуры.

Дисциплина «Информационные системы специального назначения» преподается обучающимся по очной форме обучения – в 3-м семестре, по заочной форме – в 4-м семестре.

Дисциплина «Информационные системы специального назначения» является начальным этапом формирования компетенций ОПК-7 в процессе освоения ОПОП.

Дисциплина «Информационные системы специального назначения» является предшествующей для изучения дисциплин Производственная практика: преддипломная практика, Государственная итоговая аттестация: выполнение и защита выпускной квалификационной работы.

Формой промежуточной аттестации знаний обучаемых по очной форме обучения является зачет в 3-м семестре, по заочной форме зачет в 4-м семестре.

3. Объем дисциплины

очная форма обучения:

Вид учебной работы по дисциплине	**Всего в з.е. и часах**	**Семестр 3 в часах**
Общая трудоёмкость дисциплины	**2 з.е. - 72 ак.час**	**72 ак.час**
Контактная работа - Аудиторные занятия	**24**	**24**
Лекции	12	12
Лабораторные занятия	12	12
Семинары, практические занятия	-	-
Консультация	-	-
Самостоятельная работа	**48**	**48**
Курсовая работа (курсовой проект)	-	-
Вид промежуточной аттестации	Зачет	Зачет

заочная форма обучения:

Вид учебной работы по дисциплине	**Всего в з.е. и часах**	**Семестр 4 в часах**
Общая трудоёмкость дисциплины	**2 з.е. - 72 ак.час**	**72 ак.час**
Контактная работа - Аудиторные занятия	**8**	**8**
Лекции	4	4
Лабораторные занятия	4	4
Семинары, практические занятия	-	-
Консультация	-	-
Самостоятельная работа	**60**	**60**
Курсовая работа (курсовой проект)	-	-
Вид промежуточной аттестации	Зачет – 4 часа	Зачет – 4 часа

4. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

4.1. Учебно-тематический план

Очная форма обучения

Тема (раздел)	Количество часов				Код индикатора достижений компетенции
	контактная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Международные стандарты информационного	6	6	-	24	ОПК-7.1, ОПК-7.2,

обмена. Основные положения теории информационной безопасности.					ОПК-7.3
Тема 2. Информационные системы безопасности	6	6	-	24	ОПК-7.1, ОПК-7.2, ОПК-7.3
Консультации	-			-	ОПК-7.1, ОПК-7.2, ОПК-7.3
Курсовая работа (курсовой проект)	-				ОПК-7.1, ОПК-7.2, ОПК-7.3
Контроль (зачет)	-				ОПК-7.1, ОПК-7.2, ОПК-7.3
ИТОГО	**24**			**48**	

Заочная форма обучения

Тема (раздел)	Количество часов				Код индикатора достижений компетенции
	контактная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Международные стандарты информационного обмена. Основные положения теории информационной безопасности.	2	2	-	30	ОПК-7.1, ОПК-7.2, ОПК-7.3
Тема 2. Информационные системы безопасности	2	2	-	30	ОПК-7.1, ОПК-7.2, ОПК-7.3
Консультации	-			-	ОПК-7.1, ОПК-7.2, ОПК-7.3
Курсовая работа (курсовой проект)	-				ОПК-7.1, ОПК-7.2, ОПК-7.3
Контроль (зачет)	4				ОПК-7.1, ОПК-7.2, ОПК-7.3
ИТОГО	**8**			**60**	

4.2. Содержание дисциплины

Тема 1. Международные стандарты информационного обмена. Основные положения теории информационной безопасности.

Понятие и классификация информационных систем специального назначения. Области применения: оборонная, государственная, медицинская, промышленная сферы.

Международные и отечественные стандарты информационного обмена: ISO/IEC 27000, ISO 10303 (STEP), HL7, X.500, ASN.1 и др.

Роль стандартов в обеспечении совместимости, надежности и безопасности информационного взаимодействия.

Протоколы обмена данными в ИССН: SNMP, MQTT, Modbus, OPC UA, SOAP, REST.

Основы теории информационной безопасности: понятия "угроза", "уязвимость", "атака", "безопасность информации".

Классификация угроз информационной безопасности. Типовые сценарии атак на ИС специального назначения.

Триада информационной безопасности: конфиденциальность, целостность, доступность (CIA).

Криптографические методы защиты: шифрование, цифровая подпись, хэш-функции. Международные стандарты криптографии (AES, RSA, ГОСТ).

Принципы построения защищенных информационных систем: многоуровневая защита, модель доверенных вычислений, контроль доступа.

Законодательные и нормативные аспекты: ФЗ-152, ФЗ-187, ГОСТ Р 56939, требования ФСТЭК и ФСБ России.

Тема 2. Информационные системы безопасности

Понятие информационной системы безопасности (ИСБ) и ее роль в защите ИССН.

Архитектура ИСБ: подсистемы аутентификации, контроля доступа, мониторинга, анализа событий безопасности.

Средства обеспечения ИБ: антивирусы, фаерволы, IDS/IPS, SIEM-системы, DLP-системы, системы управления ключами.

Управление инцидентами информационной безопасности. Реакция, восстановление, расследование.

Организация защищенного информационного обмена в системах специального назначения.

Информационная безопасность в условиях критической инфраструктуры. Пример: автоматизированные системы управления технологическими процессами (АСУ ТП).

Системы управления информационной безопасностью (СУИБ): принципы построения, цикл PDCA, стандарт ISO/IEC 27001.

Роль человеческого фактора в обеспечении ИБ: социальная инженерия, политика безопасности, обучение персонала.

Интеграция ИСБ в структуру ИССН: проектирование безопасной архитектуры, контроль на всех этапах жизненного цикла.

Практические кейсы: построение ИСБ в системах госуправления, здравоохранения, промышленной автоматизации.

5. Учебно-методическое обеспечение самостоятельной работы студентов

Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний студентов; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций; развитию исследовательских умений студентов.

Формы и виды самостоятельной работы студентов: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, курсовой работе, экзамену); самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, задачи, тесты).

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, компьютерные классы с возможностью работы в Интернет; аудитории (классы) для консультационной деятельности.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации.

Контроль самостоятельной работы студентов предусматривает: соотнесение содержания контроля с целями обучения; объективность контроля; валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы: просмотр и проверка выполнения самостоятельной работы преподавателем; организация самопроверки, взаимопроверки выполненного задания в группе; обсуждение результатов выполненной работы на занятии; проведение письменного опроса; проведение устного опроса; организация и проведение индивидуального собеседования; организация и проведение собеседования с группой.

Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	**Перечень вопросов, отводимых на самостоятельное освоение**	**Формы внеаудиторной самостоятельной работы**
Тема 1. Международные стандарты информационного обмена. Основные положения теории информационной безопасности.	Изучение международных стандартов в области информационного обмена (ISO/IEC 27001, ISO 10303, X.500 и др.). Особенности межгосударственного информационного взаимодействия и вопросы интероперабельности. Базовые принципы информационной безопасности: конфиденциальность, целостность, доступность. Модели угроз и механизмов защиты в специальных информационных системах.	Составление таблицы с кратким описанием международных стандартов обмена данными. Анализ конкретного стандарта (например, ISO/IEC 27001) с точки зрения применения в информационных систем специального назначения.
Тема 2. Информационные системы безопасности	Обзор архитектуры информационных систем безопасности (IDS/IPS, SIEM, DLP и др.). Программные и аппаратные средства защиты информации в специальных условиях. Методы контроля доступа и аутентификации в защищённых системах. Анализ примеров реализации информационных систем безопасности в госструктурах и промышленности.	Выполнение сравнительного анализа нескольких IDS/IPS-систем. Разработка схемы модели контроля доступа для гипотетической защищённой ИС.

Шкала оценивания

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает тему самостоятельной работы, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер
«Хорошо»	Обучающийся в целом раскрывает тему самостоятельной работы, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера
«Удовлетворительно»	Обучающийся в целом раскрывает тему самостоятельной работы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.

«Неудовлетворительно»	Обучающийся не владеет выбранной темой самостоятельной работы

6. Оценочные материалы (фонд оценочных средств) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. Паспорт фонда оценочных средств

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
1.	Тема 1. Международные стандарты информационного обмена. Основные положения теории информационной безопасности.	ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	ОПК-7.1. Знать: функциональные требования к прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования ОПК-7.2. Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами ОПК-7.3. Владеть: методами настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций	Опрос, тест, зачет
2.	Тема 2. Информационные системы безопасности	ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного	ОПК-7.1. Знать: функциональные требования к прикладному программному обеспечению для решения актуальных	Опрос, тест, зачет

		проектирования к нуждам отечественных предприятий	задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования ОПК-7.2. Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами ОПК-7.3. Владеть: методами настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций	

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенции, характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе итоговой аттестации: выполнение и защита выпускной квалификационной работы.

Дисциплина «Информационные системы специального назначения» является начальным этапом комплекса дисциплин, в ходе изучения которых у студентов формируются компетенции ОПК-7.

Завершается работа по формированию у студентов указанных компетенций в ходе изучения дисциплин Производственная практика: преддипломная практика.

Итоговая оценка сформированности компетенций ОПК-7 определяется в период Государственная итоговая аттестация: выполнение и защита выпускной квалификационной работы.

В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования ОПК-7 при изучении дисциплины Б1.Д(М).Б.9 «Информационные системы специального назначения» является последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение студентами необходимыми дескрипторами (составляющими) компетенций. Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет.

6.2. Контрольные задания и материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

6.2.1. Контрольные вопросы по темам (разделам) для опроса на занятиях

Тема (раздел)	Вопросы
Тема 1. Международные стандарты информационного обмена. Основные положения теории информационной безопасности.	ОПК-7 1. Международные стандарты информационного обмена. 2. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. 3. Основные положения теории защиты информации 4. Модели безопасности и их применение.
Тема 2. Информационные системы безопасности	ОПК-7 1. Методология анализа защищенности информационной системы. 2. Основные технологии построения защищенных систем. 3. Антивирусные программы. 4. ЭЦП и КриптоПро.

Шкала оценивания ответов на вопросы

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает ответ на каждый теоретический вопрос, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«Хорошо»	Обучающийся в целом раскрывает теоретические вопросы, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает теоретические вопросы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«Неудовлетворительно»	Обучающийся не знает ответов на поставленные теоретические вопросы.

6.2.2. Оценочные средства остаточных знаний (тест)
ОПК-7.

1. Опишите правовой режим персональных данных.
2. Опишите международные стандарты электронного обмена данными.
3. Опишите нормативно-правовые акты в области информационной безопасности в Российской Федерации.
4. Опишите каждый уровень секретности документов.
5. Перечислите особенности обеспечения информационной безопасности РФ в сфере экономики.
6. Дайте определение понятию стандарт информационного обмена.
7. Дайте определение понятию стандартизация информационного обмена.
8. Перечислите виды стандартов информационной безопасности.
9. Дайте определение понятию теория защиты информации.
10. Дайте классификацию моделей безопасности.
11. Перечислите основные средства, используемые для создания механизма защиты.
12. Охарактеризуйте программные средства защиты информации.
13. Перечислите основные положения теории защиты информации.
14. Опишите методологию анализа защищенности информационной системы.
15. Дайте определение понятию угрозы.
16. Дайте определение понятию атаки.
17. Дайте определение понятию глобальные сети.
18. Дайте определение понятию информационная безопасность.
19. Дайте определение понятию государственной тайны.
20. Дайте определение понятию коммерческой тайны.
21. Дайте определение понятию личной тайны.
22. Дайте определение понятию антивирусные программы.
23. Перечислите назначение электронной цифровой подписи.
24. Приведите примеры использования электронной цифровой подписи.
25. Дайте определение понятию электронная цифровая подпись.
26. Перечислите процесс создания электронной цифровой подписи.
27. Опишите этап генерации ключевой пары.
28. Опишите этап формирования подписи.
29. Опишите этап верификации подписи.
30. Перечислите устройства хранения закрытого ключа.
31. Дайте определение понятию криптография.
32. Опишите сущность криптографических методов.
33. Дайте определение понятию криптопровайдер.
34. Перечислите функции КриптоПро ЭЦП.
35. Перечислите деструктивные действия вирусов.
36. Опишите принцип действия компаньон-вируса.
37. Опишите принцип действия стелс-вируса.
38. Опишите принцип действия резидентного вируса.

39. Опишите принцип действия вирусов типа «Троянский конь».
40. Опишите принцип действия полиморфиков.
41. Опишите принцип действия макровирусов.
42. Назовите вирусы, разрушающие «компьютерное железо».
43. Перечислите виды антивирусных программ.
44. Перечислите стадии жизненного цикла вируса.
45. Перечислите методы борьбы с компьютерными вирусами.

Тестовые задания

46. **Программа, которая может размножаться, присоединяя свой код к другой программе, называется**
1) Компилятор
2) Интернет-черви
3) Вирус

47. **Какого типа вирусов не бывает?**
1) Компаньон-вирус
2) Интернет-черви
3) Полиморфики
4) Вирус-змея

48. **Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется**
1) Воздействием (влиянием)
2) Потерей
3) Силой

49. **Уровень риска, который считается доступным для достижения желаемого результата, называется**
1) Устойчивостью
2) Терпимостью по отношению к риску
3) Независимостью

50. **Системные файлы, обеспечивающие поддержку структур файловой системы, называются:**
1) Каталоги
2) Символьные файлы
3) Регулярные файлы

51. **Требования к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:**
1) Правилами безопасности

2) Требованием безопасности
3) Мерами безопасности

52. **Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:**
1) Управление риском
2) Предупреждением рисков
3) Анализом рисков

53. **Выберите характеристики электронной цифровой подписи (несколько ответов).**
1) Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи.
2) Позволяет проверить отсутствие искажения информации в электронном документе с момента формирования подписи, принадлежность подписи владельцу сертификата ключа подписи.
3) Может быть подделана с помощью обычного копирования
4) В случае успешной проверки принадлежности подписи владельцу подтвердить факт подписания электронного документа.

54. **Выберите основные направления использования криптографических методов (несколько ответов).**
1) Очистка компьютера от вирусов
2) Передача конфиденциальной информации по каналам связи (например, электронная почта)
3) Установление подлинности передаваемых сообщений
4) Хранение информации (документов, баз данных) на носителях в зашифрованном виде.

55. **Выберите программы для криптографии**
1) CryptoExpert
2) КриптоПро CSP
3) VeraCrypt
4) AccessCrypt

56. **Модель угроз – это..**
1) Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.
2) Пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

3) Перечень возможных угроз информации.

4) Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

57. **Какие антивирусные программы рассчитаны на обнаружение конкретных, заранее известных программе вирусов и основаны на сравнении характерной последовательности байтов (сигнатур), содержащихся в теле вируса, с байтами проверяемых программ?**

1) Программы-детекторы
2) Программы-дезинфекторы
3) Программы-ревизоры
4) Программы-фильтры

58. **Какие антивирусные программы не только находят зараженные файлы, но и лечат их, удаляя из файла тело программы-вируса?**

1) Программы-детекторы
2) Программы-дезинфекторы
3) Программы-ревизоры
4) Программы-фильтры

59. **Какие антивирусные программы анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора?**

1) Программы-детекторы
2) Программы-дезинфекторы
3) Программы-ревизоры
4) Программы-фильтры

60. **Какие антивирусные программы оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия?**

1) Программы-детекторы
2) Программы-дезинфекторы
3) Программы-ревизоры
4) Программы-фильтры

Ключи к тесту

46.3	**47.4**	**48.1**	**49.2**	**50.1**	**51.2**	**52.3**	**53.1,2,4**	**54.2,3,4**
55.1,2,3	**56.1**	**57.1**	**58.2**	**59.3**	**60.4**			

Шкала оценивания результатов тестирования

% верных решений (ответов)	Шкала оценивания
85 - 100	отлично

70 - 84	хорошо
50- 69	удовлетворительно
0 - 49	неудовлетворительно

6.2.3. Индивидуальные задания для курсовой работы (проекта)

КР и КП по дисциплине «Информационные системы специального назначения» рабочей программой и учебным планом не предусмотрены.

6.3. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Вопросы для подготовки к промежуточной аттестации по итогам освоения дисциплины Информационные системы специального назначения:

ОПК-7.

1. Понятие угрозы, атаки.
2. Глобальные сети и информационная безопасность.
3. Стандарты в области информационной безопасности.
4. Международные стандарты информационного обмена.
5. Рассекречивание документов. Уровень тайны.
6. Назначение и задачи в сфере обеспечения безопасности.
7. Основные положения теории информационной безопасности.
8. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании.
9. Модели безопасности для промышленных предприятий
10. Основные технологии построения защищенных систем.
11. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.
12. Электронная цифровая подпись.
13. Программы для криптографии.
14. Классификация угроз информационной безопасности по источнику возникновения.
15. Внутренние и внешние угрозы для информационных систем специального назначения.
16. Умышленные и неумышленные угрозы: различия и примеры.
17. Каналы утечки информации и методы их выявления.
18. Понятие уязвимости и соотношение с угрозами и атаками.
19. Модель нарушителя информационной безопасности и её основные типы.
20. Атаки на уровне сети: сниффинг, спуфинг, DoS и DDoS.
21. Атаки на уровне приложений: SQL-инъекции, межсайтовый скриптинг.
22. Методы фишинга и противодействие им в специальных информационных системах.

23. Понятие защищённой информационной системы и критерии защищённости.

24. Принципы построения систем защиты информации: эшелонированность, избыточность, простота.

25. Методология управления рисками информационной безопасности.

26. Оценка рисков: идентификация активов, угроз, уязвимостей.

27. Понятие остаточного риска и допустимого уровня риска.

28. Мандатная и дискреционная модели управления доступом.

29. Мандатная модель безопасности Белла — Лападулы.

30. Модель Кларка — Уилсона для целостности данных.

31. Модель Китаева — Лефевра.

32. Ролевая модель управления доступом в крупных информационных системах.

33. Модель безопасности многоуровневых систем.

34. Автоматизированные системы в защищённом исполнении: классы защищённости.

35. Защита информации от утечки по техническим каналам.

36. Организация защищённого документооборота в органах государственной власти.

37. Механизмы контроля целостности информации: хеширование и контрольные суммы.

38. Аутентификация пользователей в информационных системах специального назначения.

39. Биометрические методы аутентификации: достоинства и недостатки.

40. Многофакторная аутентификация как обязательное требование для специальных систем.

41. Межсетевые экраны и их классификация.

42. Системы обнаружения и предотвращения вторжений.

43. Анализаторы защищённости и их применение.

44. DLP-системы для контроля утечек конфиденциальной информации.

45. SIEM-системы как инструмент централизованного сбора и корреляции событий безопасности.

46. Классификация вредоносного программного обеспечения: вирусы, черви, трояны, руткиты.

47. Сравнительный анализ антивирусных движков: сигнатурный, эвристический, поведенческий анализ.

48. Понятие криптостойкости и факторы, её определяющие.

49. Инфраструктура открытых ключей и удостоверяющие центры.

50. Криптографические хеш-функции.

51. Квантовая криптография и перспективы её применения в специальных системах.

52. Понятие стеганографии и методы скрытой передачи информации.

53. Требования к аппаратному обеспечению информационных систем специального назначения.

54. Аттестация объектов информатизации по требованиям безопасности.

55. Сертификация средств защиты информации и лицензирование деятельности в области ИБ.

56. Организация резервного копирования и восстановления данных в критических системах.

57. Защита информации в облачных инфраструктурах специального назначения.

58. Инциденты информационной безопасности: порядок обнаружения, регистрации и расследования.

59. Понятие Security Operation Center для мониторинга и реагирования.

60. План непрерывности бизнес-процессов и восстановления после сбоев для специальных информационных систем.

61. Классификация информационных систем специального назначения по степени критичности.

62. Принципы построения защищённых автоматизированных систем управления технологическими процессами (АСУ ТП).

63. Методы противодействия атакам на критическую информационную инфраструктуру.

64. Организация безопасного удалённого доступа к информационным системам специального назначения.

65. Методы защиты информации при передаче по открытым каналам связи.

66. Архитектура типового защищённого сегмента локальной вычислительной сети.

67. Принципы изоляции информационных систем специального назначения от публичных сетей.

68. Методы контроля съёмных носителей информации в защищённых системах.

69. Организация аудита событий информационной безопасности в специальных системах.

70. Методы очистки памяти носителей от конфиденциальной информации.

71. Принципы физической защиты серверного и сетевого оборудования.

72. Методы предотвращения несанкционированного доступа к вычислительным ресурсам.

73. Организация контроля действий привилегированных пользователей.

74. Методы защиты информации в беспроводных сетях специального назначения.

75. Принципы построения защищённых систем видеоконференцсвязи.

76. Методы борьбы с закладными устройствами съёма информации.

77. Организация безопасного межсетевого взаимодействия разнородных информационных систем.

78. Методы мониторинга целостности системных файлов и конфигураций.

79. Принципы реагирования на инциденты в информационных системах специального назначения.

80. Методы восстановления работоспособности информационной системы после успешной атаки.

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Основной целью проведения промежуточной аттестации является определение степени достижения целей по учебной дисциплине или ее разделам. Осуществляется это проверкой и оценкой уровня теоретической знаний, полученных обучающимися, умения применять их в решении практических задач, степени овладения обучающимися практическими навыками и умениями в объеме требований рабочей программы по дисциплине, а также их умение самостоятельно работать с учебной литературой.

Организация проведения промежуточной аттестации регламентирована «Положением об организации образовательного процесса в федеральном государственном автономном образовательном учреждении «Московский политехнический университет»

6.4.1. Показатели оценивания компетенций на различных этапах их формирования, достижение обучающимися планируемых результатов обучения по дисциплине

Код и наименование компетенции ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: методологии разработки программного обеспечения	Обучающийся демонстрирует неполное соответствие следующих знаний: методологии разработки программного обеспечения	Обучающийся демонстрирует частичное соответствие следующих знаний: методологии разработки программного обеспечения	Обучающийся демонстрирует полное соответствие следующих знаний: методологии разработки программного обеспечения

уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять: методологии разработки программного обеспечения	Обучающийся демонстрирует неполное соответствие следующих умений: применять методологии разработки программного обеспечения	Обучающийся демонстрирует частичное соответствие следующих умений: применять методологии разработки программного обеспечения	Обучающийся демонстрирует полное соответствие следующих умений: применять методологии разработки программного обеспечения
владеть	Обучающийся не владеет или в недостаточной степени владеет: выбором инструментальных средств разработки программного обеспечения	Обучающийся владеет в неполном объеме и проявляет недостаточность владения выбором инструментальных средств разработки программного обеспечения	Обучающимся допускаются незначительные ошибки, неточности, затруднения, частично владеет выбором инструментальных средств разработки программного обеспечения	Обучающийся свободно применяет полученные навыки, в полном объеме владеет выбором инструментальных средств разработки программного обеспечения

6.4.2. Методика оценивания результатов промежуточной аттестации

Показателями оценивания компетенций на этапе промежуточной аттестации по дисциплине «Информационные системы специального назначения» являются результаты обучения по дисциплине.

Оценочный лист результатов обучения по дисциплине

Код компетенции	Знания	Умения	Навыки	Уровень сформированности компетенции на данном этапе / оценка
ПК-7 Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных	на уровне знаний: знать методологии разработки программного обеспечения	на уровне умений: уметь применять методологии разработки программного обеспечения	на уровне навыков: выбор инструментальных средств разработки программного обеспечения	

предприятий				
Оценка по дисциплине (среднее арифметическое)				

Оценка «зачтено» выставляется, если среднее арифметическое находится в интервале от 2,4 до 5,0. Оценка «не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

Промежуточная аттестация обучающихся в форме зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по дисциплине «Информационные системы специального назначения», при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «зачтено», или «не зачтено».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков по этапам (уровням) сформированности компетенций, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7. Электронная информационно-образовательная среда

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде Чебоксарского института (филиала) Московского политехнического университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории филиала, так и вне ее.

Электронная информационно-образовательная среда – совокупность информационных и телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися

образовательных программ в полном объёме независимо от места нахождения обучающихся.

Электронная информационно-образовательная среда обеспечивает:

а) доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

б) формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы;

в) фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы магистратуры;

г) проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

д) взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет».

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих.

Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

Основными составляющими ЭИОС филиала являются:

а) сайт института в сети Интернет, расположенный по адресу www.polytech21.ru, https://chebpolytech.ru/ который обеспечивает:

- доступ обучающихся к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем, электронным информационным и образовательным ресурсам, указанных в рабочих программах (разделы сайта «Сведения об образовательной организации»);

- информирование обучающихся обо всех изменениях учебного процесса (новостная лента сайта, лента анонсов);

- взаимодействие между участниками образовательного процесса (подразделы сайта «Задать вопрос директору»);

б) официальные электронные адреса подразделений и сотрудников института с Яндекс-доменом @polytech21.ru (список контактных данных подразделений Филиала размещен на официальном сайте Филиала в разделе «Контакты», списки контактных официальных электронных данных преподавателей размещены в подразделах «Кафедры») обеспечивают взаимодействие между участниками образовательного процесса;

в) личный кабинет обучающегося (портфолио) (вход в личный кабинет размещен на официальном сайте Филиала в разделе «Студенту» подразделе «Электронная информационно-образовательная среда») включает в себя портфолио студента, электронные ведомости, рейтинг студентов и обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися,

- формирование электронного портфолио обучающегося, в том числе с сохранение работ обучающегося, рецензий и оценок на эти работы,

г) электронные библиотеки, включающие электронные каталоги, полнотекстовые документы и обеспечивающие доступ к учебно-методическим материалам, выпускным квалификационным работам и т.д.:

Чебоксарского института (филиала) - «ИРБИС»

д) электронно-библиотечные системы (ЭБС), включающие электронный каталог и полнотекстовые документы:

- ЭБС «ЛАНЬ» -https://e.lanbook.com/

- Образовательная платформа Юрайт - https://urait.ru

- IPR SMART -https://www.iprbookshop.ru/

е) платформа цифрового образования Политеха - https://lms.mospolytech.ru/

ж) система «Антиплагиат» -https://www.antiplagiat.ru/

з) система электронного документооборота DIRECTUM Standard — обеспечивает документооборот между Филиалом и Университетом;

и) система «1С Управление ВУЗом Электронный деканат» (Московский политехнический университет) обеспечивает фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися;

к) система «POLYTECH systems» обеспечивает информационное, документальное автоматизированное сопровождение образовательного процесса;

л) система «Абитуриент» обеспечивает документальное автоматизированное сопровождение работы приемной комиссии.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Информационные системы управления производственной компанией : учебник и практикум для вузов / под редакцией Н. Н. Лычкиной. — Москва : Издательство Юрайт, 2025. — 241 с. — (Высшее образование). — ISBN 978-5-534-00764-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560080.

2. Жмудь, В. А. Системы автоматического управления высшей точности : учебник для вузов / В. А. Жмудь, А. В. Тайченачев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 206 с. — (Высшее образование). — ISBN 978-5-534-05143-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557574.

3. Антимиров, В. М. Системы автоматического управления: бортовые цифровые вычислительные системы : учебник для вузов / В. М. Антимиров ; под научной редакцией В. В. Телицина. — Москва : Издательство Юрайт, 2025. — 71 с. — (Высшее образование). — ISBN 978-5-9916-9907-5. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562926.

4. Бородин, И. Ф. Автоматизация технологических процессов и системы автоматического управления : учебник для вузов / И. Ф. Бородин, С. А. Андреев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2026. — 377 с. — (Высшее образование). — ISBN 978-5-534-19501-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/585154.

Дополнительная литература

1. Рыжко, А. Л. Информационные системы управления производственной компанией : учебник для вузов / А. Л. Рыжко, А. И. Рыбников, Н. А. Рыжко. — Москва : Издательство Юрайт, 2025. — 354 с. — (Высшее образование). — ISBN 978-5-534-00623-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560486.

2. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для вузов / Л. А. Станкевич. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 478 с. — (Высшее образование). — ISBN 978-5-534-20363-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560754.

Периодика:

1. Известия Тульского государственного университета. Технические науки: Научный рецензируемый журнал. https://tidings.tsu.tula.ru/tidings/index.php?id=technical&lang=ru&year=1. - Текст : электронный.

2. Научный периодический журнал «Вестник Южно-Уральского государственного университета. Серия «Вычислительная математика и информатика» : Научный рецензируемый журнал. https://vestnik.susu.ru/cmi - Текст : электронный.

3. Научный периодический журнал «Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника»: Научный рецензируемый журнал. https://vestnik.susu.ru/ctcr - Текст : электронный.

9. Профессиональные базы данных и информационно-справочные системы

Профессиональная база данных и информационно-справочные системы	Информация о праве собственности (реквизиты договора)
Университетская информационная система РОССИЯ https://uisrussia.msu.ru/	Тематическая электронная библиотека и база для прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права. свободный доступ

научная электронная библиотека Elibrary http://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научно-технических журналов, из которых более 4800 журналов в открытом доступе свободный доступ
сайт Института научной информации по общественным наукам РАН. http://www.inion.ru	Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объём массивов составляет более 3 млн. 500 тыс. записей (данные на 1 января 2012 г.). Ежегодный прирост — около 100 тыс. записей. В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языках, поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифром хранения и ссылками на полные тексты источников из Научной электронной библиотеки.
Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru	Федеральный портал «Российское образование» – уникальный интернет-ресурс в сфере образования и науки. Ежедневно публикует самые актуальные новости, анонсы событий, информационные материалы для широкого круга читателей. Еженедельно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными, репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.
computerra.ru-Компьютерра : Новости про компьютеры, железо, новые технологии, информационные технологии	Компьютерра — это ресурс о современных технологиях, которые пришли в потребительский сегмент из научных сфер. Задача — понятным языком рассказать читателям о том будущем, которое уже наступило и стало доступным рядовым потребителям. Ресурс помогает разобраться в таких сложных на первый взгляд вещах, как блокчейн, облачные технологии, дополненная и виртуальная реальности, искусственный интеллект, робототехника и других, а также знакомит с новыми продуктами и устройствами, которые делают жизнь проще, безопаснее и интереснее.
Информационные технологии – периодическое научно-техническое издание в области информационных технологий, автоматизированных систем	Издательство выпускает теоретические и прикладные научно-технические журналы, обеспечивающие научной, производственной, обзорно-аналитической и образовательной информацией руководящих работников и специалистов промышленных предприятий, научных академических и отраслевых организаций, а также учебных

и использования информатики в различных приложениях novtex.ru	заведений в области приоритетных направлений развития науки и технологий.
iXBT.com - актуальные новости из сферы IT, обзоры смартфонов, планшетов, персональных компьютеров, компьютерных комплектующих, программного обеспечения и периферийных устройств ixbt.com	iXBT.com — специализированный российский информационно-аналитический сайт с самыми актуальными новостями из сферы IT, науки, техники, космоса и автомобильной отрасли. Детальными обзорами смартфонов, планшетов, персональных компьютеров, компьютерных комплектующих, бытовой техники и устройств для ремонта, сада и огорода, программного обеспечения и периферийных устройств. На сайте ежедневно освещаются вопросы цифровых технологий и современных решений на их базе.
Ассоциация инженерного образования России http://www.ac-raee.ru/	Совершенствование образования и инженерной деятельности во всех их проявлениях, относящихся к учебному, научному и технологическому направлениям, включая процессы преподавания, консультирования, исследования, разработки инженерных решений, оказания широкого спектра образовательных услуг, обеспечения связей с общественностью, производством, наукой и интеграции в международное научно-образовательное пространство. свободный доступ

10. Программное обеспечение (лицензионное и свободно распространяемое), используемое при осуществлении образовательного процесса

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
№ 211б Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	Microsoft Visual Studio 2019	свободно распространяемое программное обеспечение (бессрочная лицензия)
	КОМПАС-3D v20 и v21	Сублицензионный договор № Нп-22-00044 от 21.03.2022 (бессрочная лицензия)
	PaitNet	свободно распространяемое программное обеспечение

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
программах дисциплин (модулей) Лаборатория «Программного обеспечения и сопровождения компьютерных систем» Кабинет информационных систем и технологий АО «НПК «ЭЛАРА»		(бессрочная лицензия)
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)
№ 103а Помещение для самостоятельной работы обучающихся	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	MS Windows 10 Pro	договор № 392_469.223.ЗК/19 от 17.12.19 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант- справочно-правовая система	Договор №С-002-2025 от 09.01.2025
	Yandex браузер	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic (Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)

11. Материально-техническое обеспечение дисциплины

Тип и номер помещения	Перечень основного оборудования и технических средств обучения
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Лаборатория «Программного обеспечения и сопровождения компьютерных систем» Кабинет информационных систем и технологий АО «НПК «ЭЛАРА»	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды, автоматизированные рабочие места на 15 обучающихся, автоматизированное рабочее место преподавателя, Технические средства обучения: компьютерная техника; мультимедийное оборудование (проектор, экран), маркерная доска, программное обеспечение общего и профессионального назначения

№ 211б (г. Чебоксары, ул. К.Маркса, 60)	
Помещение для самостоятельной работы обучающихся **№ 103а** (г. Чебоксары, ул. К.Маркса, 54)	Оборудование: комплект мебели для учебного процесса; Технические средства обучения: компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Филиала

12. Методические указания для обучающегося по освоению дисциплины

Методические указания для занятий лекционного типа

В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из основной и дополнительной литературы, рекомендованной преподавателем и предусмотренной учебной программой дисциплины.

Методические указания для занятий лабораторного типа.

Выполнению лабораторных работ предшествует проверка знаний студентов – их теоретической готовности к выполнению задания. Проверка знаний проводится в форме, которую определяет преподаватель дисциплины (тестирование, опрос).

При проведении лабораторных занятий выделяют следующие разделы:

- общие положения (перечень лабораторных или практических
- занятий);
- ообщие требования к выполнению работ;
- инструкция по каждой работе;
- справочные материалы и т. д.

Лабораторные занятия позволяют развивать у обучающегося творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Готовясь к докладу или выступлению в рамках интерактивной формы, при необходимости, следует обратиться за помощью к преподавателю.

Методические указания к самостоятельной работе.

Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала по учебной дисциплине может выполняться в библиотеке университета, учебных кабинетах, компьютерных классах, а также в домашних условиях. Содержание и количество самостоятельной работы обучающегося

определяется учебной программой дисциплины, методическими материалами, практическими заданиями и указаниями преподавателя.

***Самостоятельная работа в аудиторное время может включать**:*

1) конспектирование (составление тезисов) лекций;
2) выполнение контрольных работ;
3) решение задач;
4) работу со справочной и методической литературой;
5) работу с нормативными правовыми актами;
6) выступления с докладами, сообщениями на семинарских занятиях;
7) защиту выполненных работ;
8) участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;
9) участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;
10) участие в тестировании и др.

Самостоятельная работа во внеаудиторное время может состоять из:

1) повторения лекционного материала;
2) подготовки к практическим занятиям;
3) изучения учебной и научной литературы;
4) изучения нормативных правовых актов (в т.ч. в электронных базах данных);
5) решения задач, и иных практических заданий
6) подготовки к контрольным работам, тестированию и т.д.;
7) подготовки к практическим занятиям устных докладов (сообщений);
8) подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
9) выполнения курсовых работ, предусмотренных учебным планом;
10) выполнения выпускных квалификационных работ и др.
11) выделения наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на консультациях.
12) проведения самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

Текущий контроль осуществляется в форме устных, тестовых опросов, докладов, творческих заданий.

В случае пропусков занятий, наличия индивидуального графика обучения и для закрепления практических навыков студентам могут быть выданы типовые индивидуальные задания, которые должны быть сданы в установленный преподавателем срок.

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение по данной дисциплине инвалидов и лиц с ограниченными возможностями здоровья (далее ОВЗ) осуществляется преподавателем с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Для студентов с нарушениями опорно-двигательной функции и с ОВЗ по слуху предусматривается сопровождение лекций и практических занятий мультимедийными средствами, раздаточным материалом.

Для студентов с ОВЗ по зрению предусматривается применение технических средств усиления остаточного зрения, а также предусмотрена возможность разработки аудиоматериалов.

По данной дисциплине обучение инвалидов и лиц с ограниченными возможностями здоровья может осуществляться как в аудитории, так и с использованием электронной информационно-образовательной среды, образовательного портала и электронной почты.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ

рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____
____