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

Кафедра Информационные технологии, электроэнергетики и систем управления



УТВЕРЖДАЮ
Директор филиала
_____ А.В. Агафонов
«23» апреля 2021 г.

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	**заочная**
Год начала обучения	**2021**

Чебоксары, 2021

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Рабочая программа дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (п.8 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, электроэнергетики и систем управления,

Скипина Людмила Николаевна, кандидат технических наук, доцент кафедры информационных технологий, электроэнергетики и систем управления

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

Программа одобрена на заседании кафедры Информационных технологий, электроэнергетики и систем управления (протокол № 10 от 10.04.2021).

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 теоретических знаний и об основных принципах, методов и средств защиты информации; развитие умений и навыков защиты информации в процессе ее обработки, передачи и хранения компьютерных средств в информационных системах.

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:

Наименование профессиональных стандартов (ПС)	Код, наименование и уровень квалификации ОТФ, на которые ориентирована дисциплина	Код и наименование трудовых функций, на которые ориентирована дисциплина
06.017 «Руководитель разработки программного обеспечения»	Управление программно-техническими, технологическими и человеческими ресурсами	C/01.7 Управление инфраструктурой коллективной среды разработки
		C/02.7 Управление рисками разработки программного обеспечения
		C/03.7 Управление процессами оценки сложности, трудоемкости, сроков выполнения работ
06.027 Специалист по администрированию сетевых устройств информационно-коммуникационных систем	Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения	F/02.7 Документирование ошибок в работе сетевых устройств и программного обеспечения

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,	ОПК-7. Способен адаптировать зарубежные	ОПК-7.1. Знать: функциональные требования к	Знать: международные стандарты информационного

Наименование категории (группы) компетенций	Код и наименование компетенций	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения
модификация программного обеспечения	комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования	обмена; основные положения теории информационной безопасности. Уметь: применять международные стандарты информационного обмена; основные положения теории информационной безопасности. Владеть: навыками применения международных стандартов информационного обмена; основных положений теории информационной безопасности.
		ОПК-7.2. Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами	Знать: информационные системы безопасности Уметь: разрабатывать информационные системы безопасности Владеть: навыками разработки информационных систем безопасности
		ОПК-7.3. Владеть: методами настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций	Знать: методы настройки интерфейса. Уметь: настраивать пользовательские шаблоны. Владеть: методами настройки информационных систем безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.Д(М).Б.9 «Информационные системы специального назначения» реализуется в рамках обязательной части Блока 1 учебного плана обучающихся заочной формы обучения.

Дисциплина «Информационные системы специального назначения» выступает в качестве первого этапа формирования знаний, умений, навыков. Знания, умения и навыки, сформированные при изучении дисциплины «Информационные системы специального назначения», является предшествующей для изучения дисциплин: производственная практика: преддипломная практика, итоговая аттестация: выполнение и защита выпускной квалификационной работы.

3. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 академических часов), в том числе

заочная форма обучения:

Семестр	4
лекции	4
лабораторные занятия	4
семинары и практические занятия	-
контроль: контактная работа	0,2
контроль: самостоятельная работа	8,8
расчетно-графические работы, курсовые работы (проекты): контактная работа	-
расчетно-графические работы, курсовые работы (проекты): самостоятельная работа	-
консультации	-
Контактная работа	*8,2*
Самостоятельная работа	*99,8*

Вид промежуточной аттестации (форма контроля): зачет

4. Содержание дисциплины, структурированное по темам (разделам)

Заочная форма обучения

Тема (раздел)	Количество часов				Код индикатора достижений компетенции
	контактная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Международные стандарты информационного обмена. Основные положения теории информационной безопасности.	2	2		46	ОПК-7.1, ОПК-7.2, ОПК-7.3
Информационные системы безопасности	2	2		45	ОПК-7.1, ОПК-7.2, ОПК-7.3

Расчетно-графические работы, курсовые работы (проекты)	-	-	-
Консультации	-		
Контроль (зачет)	0,2	8,8	
ИТОГО	**8,2**	**99,8**	

5. Образовательные технологии, применяемые при освоении дисциплины

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся: лекционные, практические и лабораторные занятия.

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств, включая интерактивные лекции, групповые дискуссии, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курсов, составленных на основе результатов научных исследований, проводимых институтом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей.

Примеры интерактивных форм и методов проведения занятий:

- подготовка к выполнению практических и лабораторных занятий;
- проведение мастер-классов экспертов и специалистов по методам и средствам испытаний.

6. Практическая подготовка

Практическая подготовка реализуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью. Объем занятий в форме практической подготовки составляет 2 часа.

Вид занятия	Тема занятия	Количество часов	Форма проведения	Код индикатора достижений компетенции
Практическое занятие	Разработка защищенных систем в предприятии	2	Индивидуальная работа	ОПК-7.1, ОПК-7.2, ОПК-7.3

7. Учебно-методическое обеспечение самостоятельной работы студентов

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 99,8 часов. Самостоятельная работа реализуется в рамках программы освоения дисциплины в следующих формах:

- подготовка к занятиям лекционного и семинарского типа;
- проработка тем вынесенных на самостоятельное изучение.
- подготовка к зачету (изучение конспектов лекций, изучение конспектов практических занятий, дистанционное тестирование по темам)

8. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

8.1. Паспорт фонда оценочных средств

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
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	Опрос, тест., зачет

			библиотек, добавления новых функций	
2.	Информационные системы 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

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 промежуточным этапом комплекса дисциплин, в ходе изучения которых у студентов формируются компетенции ОПК-7.

Итоговая оценка сформированности компетенций ОПК-7 определяется в период итоговой аттестации: выполнение и защита выпускной квалификационной работы.

В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования ОПК-7 при изучении дисциплины «Информационные системы специального назначения» является последовательное изучение содержательно связанных между собой тем учебных занятий. Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет.

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

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

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

8.2.2. Темы докладов

1. Разработка системы мер защиты банка
2. Разработка системы мер защиты магазина
3. Разработка системы мер защиты отеля
4. Разработка системы мер защиты розничного продовольственного магазина
5. Разработка системы мер защиты образовательного учреждения
6. Разработка системы мер защиты организаций системы здравоохранения
7. Разработка системы мер защиты учреждений социальной защиты
8. Разработка системы мер защиты предприятий сельскохозяйственного назначения
9. Разработка системы мер защиты малого предприятия связи
10. Разработка системы мер защиты страховой фирмы
11. Разработка системы мер защиты магазина напольных покрытий
12. Разработка системы мер защиты автотранспортного предприятия
13. Разработка системы мер защиты промышленного предприятия
14. Разработка системы мер защиты склада косметики и парфюмерии
15. Разработка системы мер защиты государственной службы социальной поддержки безработных

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

8.2.3. Оценочные средства остаточных знаний (тест)

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется

a. Компилятор
b. Интернет-черви
c. Вирус
d. Стелс.

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется
a. Воздействием (влиянием)
b. Потерей
c. Силой
d. Убытком

3. Уровень риска, который считается доступным для достижения желаемого результата, называется
a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью
d. Сингулярностью.

4. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:
a. Каталоги
b. Символьные файлы
c. Регулярные файлы
d. Текстовые файлы

5. Требования к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:
Выберите один ответ.
a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности
d. Структурой безопасности

6. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:
a. Управление риском
b. Предупреждением рисков
c. Анализом рисков
d. Синтезом рисков.

7. Выберите характеристики электронной цифровой подписи (несколько ответов).

a. Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи.

b. Позволяет проверить отсутствие искажения информации в электронном документе с момента формирования подписи, принадлежность подписи владельцу сертификата ключа подписи.

c. Может быть подделана с помощью обычного копирования

d. В случае успешной проверки принадлежности подписи владельцу подтвердить факт подписания электронного документа.

8. Выберите основные направления использования криптографических методов (несколько ответов).

a. Очистка компьютера от вирусов

b. Передача конфиденциальной информации по каналам связи (например, электронная почта)

c. Установление подлинности передаваемых сообщений

d. Хранение информации (документов, баз данных) на носителях в зашифрованном виде.

9. Выберите программы для криптографии

a. CryptoExpert

b. КриптоПро CSP

c. VeraCrypt

d. AccessCrypt

10. Модель угроз – это..

a. Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

b. Пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

c. Перечень возможных угроз информации.

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

11. Дайте характеристику правового режима персональных данных.

12.Опишите международные стандарты электронного обмена данными

13. Нормативно-правовые акты в области информационной безопасности в Российской Федерации

14. Опишите более подробно каждый уровень секретности документов

15. Особенности обеспечения информационной безопасности РФ в сфере экономики.

16. Классификация моделей безопасности.
17. Основные средства, используемые для создания механизма защиты.
18. Программные средства защиты информации
19. Основные положения теории защиты информации
20. Методология анализа защищенности информационной системы

Ключ к тесту

№ вопроса	Ответ
1	c
2	a
3	b
4	a
5	b
6	c
7	a, b, d
8	b, c, d
9	a, b, c
10	a
11	Правовой режим персональных данных - нормативно установленные правила, определяющие условия доступа, хранения, уточнения, передачи, блокирования, обезличивания и уничтожения персональных данных. Персональные данные, находящиеся в ведении держателя, относятся к конфиденциальной информации, кроме случаев, определенных настоящим Законом. Режим конфиденциальности персональных данных снимается в случаях обезличивания персональных данных; требований субъекта в отношении своих персональных данных, не противоречащих национальному законодательству; включения персональных данных в общедоступные базы данных. По желанию субъекта для его персональных данных может быть установлен режим общедоступной информации (био-, библиографические справочники, телефонные книги, адресные книги, частные объявления и т.д.). Правовой режим для персональных данных, полученных в результате деятельности правоохранительных органов, устанавливается в соответствии с национальным законодательством.
12	При интенсивном электронном обмене данными существенное значение имеет общий объем передаваемого сообщения. Существующие национальные и международные стандарты ЭОД основаны на гибких форматах электронных

	сообщений, по каналам связи передаются только значения информационных полей исходного документа, отделенные друг от друга специальными синтаксическими разделителями. Наименования самих информационных полей в электронное сообщение не помещаются. Поля идентифицируются по их позиции в известной структуре стандартного сообщения, за счет чего объем сообщения значительно сокращается. Это дает заметный выигрыш в стоимости услуг связи при интенсивном электронном обмене данными. Другим способом сокращения объема электронного сообщения ЭОД является кодирование полей документа. Наиболее предпочтительными для пользователя являются те стандарты ЭОД, справочники элементов и кодов которых имеют более широкое распространение.
13	В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся: - Доктрина информационной безопасности РФ; - руководящие документы ФСТЭК (Гостехкомиссии России); - приказы ФСБ; - стандарты информационной безопасности, из которых выделяют: международные стандарты; государственные (национальные) стандарты РФ; рекомендации по стандартизации; методические указания.
14	Уровни секретности документов 1. Уровень секретности «Особой важности». К нему принадлежат бумаги наивысшей степени секретности. Данный гриф присваивают, так как данные при их раскрытии таят в себе большую опасность для страны и интересов государства. Вот почему документация с грифом «Особой важности» охраняется от разглашения. 2. Уровень секретности «Совершенно секретно». Его получают те бумаги, в которых содержится государственная тайна. Порядок работы с информацией в таких документах четко определяется действующим законодательством. 3. Уровень секретности «Для служебного пользования». Нельзя назвать такой гриф статусом секретности, однако в данном случае доступ к

	служебной информации разрешается исключительно сотрудникам компании. Использовать ее бесконтрольно запрещено.
15	Согласно доктрине, обеспечение информационной безопасности РФ в сфере экономики играет ключевую роль в обеспечении национальной безопасности РФ. Недостаточный контроль деятельности отечественных и зарубежных структур, занимающихся созданием и защитой систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает угрозу безопасности России в экономической сфере. Бесконтрольное привлечение иностранных фирм к созданию подобных систем создает благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации со стороны иностранных спецслужб. Широкое использование импортных средств информатизации создает угрозу возникновения технологической зависимости России от иностранных государств. Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением в компьютерные системы и сети банков и иных кредитных организаций.
16	Классические модели безопасности (для моделирования защиты от угроз АВС используется математическая логика): 1.Модели, предотвращающие угрозу раскрытия информации. 2.Модели контроля целостности информации. 3.Модели, предотвращающие угрозу отказа служб.
17	К основным средствам защиты, используемым для создания механизма защиты, относятся следующие. Технические средства представляют электрические, электромеханические и электронные устройства. Физическими средствами являются автономные устройства и системы (замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации и др.). Программные средства — это программное

	обеспечение, специально предназначенное для выполнения функций защиты информации. Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций. Законодательные средства защиты определяются законодательными актами страны, регламентирующими правила пользования, обработки и передачи информации ограниченного доступа и устанавливающими меры ответственности за нарушение этих правил. Для реализации мер безопасности используются различные механизмы шифрования (криптографии).
18	Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие: средства архивации данных; антивирусные программы; криптографические средства; средства идентификации и аутентификации пользователей; средства управления доступом; протоколирование и аудит. Как примеры комбинаций вышеперечисленных мер можно привести: защиту баз данных; защиту операционных систем; защиту информации при работе в компьютерных сетях.
19	Основные теоретические положения, отражающие принципиальные подходы в решении вопросов защиты информации: Защита информации в современных системах ее обработки должна быть комплексной как по целям защиты, так и по используемым средствам; Организация защиты должна осуществляться в соответствии с четкой стратегической установкой; Защита информации в любой обстановке, в любых условиях должна строиться на основе единого концептуально-методологического базиса, причем в этом базисе должен содержаться механизм,

	гарантирующий достижение необходимого уровня защиты; Концептуально-методологический базис должен обеспечивать наличие методологии и порядок применения инструментальных средств по достижению требуемого уровня защищенности, рациональным путем и на регулярной основе; Защита информации в рамках единого концептуально-методологического базиса может быть эффективной лишь при высоком уровне организации и достаточной обеспеченности всех работ.
20	При разработке архитектуры и создании инфраструктуры корпоративной информационных систем неизбежно встает вопрос о ее защищенности от угроз. Решение вопроса состоит в подробном анализе таких взаимно пересекающихся видов работ, как реализация информационных систем и аттестация, аудит и обследование безопасности информационных систем. Основой формального описания систем защиты традиционно считается модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие области угроз, защищаемой области и системы защиты. Модель может быть представлена в виде трех множеств: T= {ti} — множество угроз безопасности, O = {oj} — множество объектов (ресурсов) защищенной системы, M= {mk} — множество механизмов безопасности. Элементы этих множеств находятся между собой в определенных отношениях, собственно и представляющих систему защиты. Для системы с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе защиты для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность ИС, второй фактор — «прочность» и надежность механизмов защиты.

Шкала оценивания результатов тестирования

% верных решений (ответов)	Шкала оценивания
85 - 100	отлично
70 - 84	хорошо
50- 69	удовлетворительно
0 - 49	неудовлетворительно

8.2.4. Оценочные средства промежуточного контроля

Вопросы (задания) для зачета:

1. Понятие угрозы, атаки.
2. Глобальные сети и информационная безопасность.
3. Понятие государственной, коммерческой, личной тайны.
4. Основные нормативные документы в области информационной безопасности.
5. Стандарты в области информационной безопасности.
6. Международные стандарты информационного обмена.
7. Рассекречивание документов. Уровень тайны.
8. Назначение и задачи в сфере обеспечения безопасности.
9. Основные положения теории информационной безопасности.
10. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании.
11. Модели безопасности для государственной информационной системы.
12. Модели безопасности для промышленных предприятий
13. Основные технологии построения защищенных систем.
14. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.
15. Антивирусные программы
16. Электронная цифровая подпись.
17. Криптография, Криптоанализ. Основные понятия криптологии.
18. Программы для криптографии.

8.3. 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»

8.3.1. 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	Обучающийся свободно применяет полученные навыки, в полном объеме владеет выбором инструментальных средств разработки

			разработки программного обеспечения	программного обеспечения

8.3.2. 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 предприятий	методологии разработки программного обеспечения	применять методологии разработки программного обеспечения	выбор инструментальных средств разработки программного обеспечения	
Оценка по дисциплине (среднее арифметическое)				

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, навыки).

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 зачет 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 приведенным в таблицах показателей, 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.

9. 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.

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) официальный сайт института в сети Интернет, расположенный по адресу www.polytech21.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», «Библиотека», «Студенту», «Абитуриенту», «ДПО»);

- информирование обучающихся обо всех изменениях учебного процесса (разделы сайта «Студенту», «Кафедры», новостная лента сайта, лента анонсов);

- взаимодействие между участниками образовательного процесса (подразделы сайта «Вопрос кафедре», «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) http://students.polytech21.ru/login.php (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» http://library.polytech21.ru

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

- «ЛАНЬ» - www.e.lanbook.com

- Znanium.com - www.znanium.com

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

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

Основная литература

1.Андрейчиков, А. В. Интеллектуальные информационные системы и методы искусственного интеллекта : учебник / А.В. Андрейчиков, О.Н. Андрейчикова. — Москва : ИНФРА-М, 2022. — 530 с. — (Высшее образование: Магистратура). — ISBN 978-5-16-014883-0. - URL: https://znanium.com/catalog/product/1864091 - Текст : электронный.

2. Голицына, О. Л. Информационные системы : учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2022. — 448 с. : ил. — (Высшее образование). - ISBN 978-5-91134-833-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1832410

Дополнительная литература

1. Беспалов, Д. А. Операционные системы реального времени и технологии разработки кроссплатформенного программного обеспечения. Часть 1 : учебное пособие / Д. А. Беспалов, С. М. Гушанский, Н. М. Коробейникова ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 139 с. - ISBN 978-5-9275-3367-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088203

2. Беспалов, Д. А. Операционные системы реального времени и технологии разработки кроссплатформенного программного обеспечения. Часть 2 : учебное пособие / Д. А. Беспалов, С. М. Гушанский, Н. М. Коробейникова ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 168 с. - ISBN 978-5-9275-3368-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088205

4. Гридчин, А. В. Информационные технологии. Программирование на C++ : учебно-методическое пособие / А. В. Гридчин. - Новосибирск : Изд-во НГТУ,

2020. - 68 с. - ISBN 978-5-7782-4174-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866900

5. Гридчин, А. В. Информационные технологии. Специальные информационные технологии : учебно-методическое пособие / А. В. Гридчин. - Новосибирск : Изд-во НГТУ, 2020. - 56 с. - ISBN 978-5-7782-4173-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1866901

Периодика

1. Программные продукты и системы : международный научно-практический журнал / НИИ Центрпрограммсистем. - URL: https://znanium.com/catalog/magazines/issues?ref=f9bfbd0e-239e-11e4-99c7-90b11c31de4c. - Текст : электронный

11. Профессиональные базы данных и информационно-справочные системы

Профессиональная база данных и информационно-справочные системы	Информация о праве собственности (реквизиты договора)
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, включая нефтегазовую отрасль, трансфера технологий, оказания широкого спектра образовательных услуг, обеспечения связей с общественностью, производством, наукой и интеграции в международное научно-образовательное пространство. свободный доступ
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.
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

12. 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.)
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Компьютерный класс Кабинет информационных систем и технологий ЭЛАРА (211б)	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года.	Band S: 150-249 Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.ЗК/21 от 24.12.2021 до 31.12.2023
	MS Windows 10 Pro	договор № 392_469.223.ЗК/19 от 17.12.19 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант	Договор № 735_480.2233К/20 от 15.12.2020
	Yandex браузер	отечественное 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)
	Zoom	свободно распространяемое программное обеспечение (бессрочная лицензия)
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)
Помещение для самостоятельной работы (103а)	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года.	Band S: 150-249 Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.ЗК/21 от 24.12.2021 до 31.12.2023
	MS Windows 10 Pro	договор № 392_469.223.ЗК/19 от 17.12.19 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант	Договор № 735_480.223.3К/20
	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

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
		обеспечение (бессрочная лицензия)

13. 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 магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) **Компьютерный класс** **Кабинет информационных систем и технологий** **ЭЛАРА** 428000, Чебоксары, ул. К.Маркса, д.60 2 этаж, №211б	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: компьютерная техника; мультимедийное оборудование (проектор, экран)
Помещение для самостоятельной работы 428000, Чебоксары, ул. К.Маркса, д.54 1 этаж, №103а	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

14. 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 семинарского (практического) типа.

Практические 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.

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор основной и дополнительной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку к занятию, которая начинается с изучения основной и дополнительной литературы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. Далее следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие или по теме, вынесенной на дискуссию (круглый стол), продумать примеры с целью обеспечения тесной связи изучаемой темы с реальной жизнью.

Готовясь к докладу или выступлению в рамках интерактивной формы (дискуссия, круглый стол), 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.

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

Обучение по дисциплине «Информационные системы специального назначения» 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 дисциплине «Информационные системы специального назначения» 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 2022-2023 учебном году на заседании кафедры, протокол № 10 от «14» мая 2022 г.

Внесены дополнения и изменения в части актуализации лицензионного программного обеспечение, используемое при осуществлении образовательного процесса по данной дисциплины, а так же современных профессиональных баз данных и информационных справочных системах, актуализации тем для самостоятельной работы, актуализации вопросов для подготовки к промежуточной аттестации, актуализации перечня основной и дополнительной учебной литературы.

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 _____