

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

25.01.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.41 Комплексное обеспечение информационной безопасности автоматизированных систем

(код и наименование дисциплины по учебному плану)

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем
(специальность)

Квалификация выпускника Специалист

(бакалавр/магистр/специалист)

Специализация Анализ безопасности информационных систем

Курс 5
Семестр 9

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	36	часов
Лабораторные работы	-	часов
Практические занятия	36	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	72	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	72	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	9	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

доцент	ИБ	СОГЛАСОВАНО	А.В. Михайлов
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

(наименование кафедры)		
31.01.2023	протокол №	10/1
(дата)		
Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими) кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 22.02.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /И.Р. Валиева/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-18 Способен разрабатывать методики и тесты для анализа степени защищенности информационн ой системы и её соответствия нормативным требованиям по защите информации	ОПК-18.1.1 знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем	знания: знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем умения: навыки:
	ОПК-18.2 умеет проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защи-щенности	знания: умения: умеет проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защи-щенности навыки:
	ОПК-18.3 владеет методами расчета и измерения основных параметров устройств СВЧ, антенн и линий передачи сверхвысокочастотного диапазона	знания: умения: навыки: владеет методами расчета и измерения основных параметров устройств СВЧ, антенн и линий передачи сверхвысокочастотного диапазона
	ОПК-18.1.2 знает программно-аппаратные средства обеспечения за-щиты информации в программном обеспечении автома-	знания: знает программно-аппаратные средства обеспечения за-щиты информации в программном обеспечении автома-тизированных систем умения: навыки:
2. ПК-4 Способен применять инструментарий анализа безопасности программного обеспечения	ПК-4.4.1 знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем	знания: знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем умения: навыки:

ПК-4.4.2 знает программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем	знания: знает программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем умения: навыки:
ПК-4.4.2 умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами	знания: умения: умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами навыки:
ПК-4.4.3 Владеть инструментами оценки эффективности реализуемых технических решений	знания: умения: навыки: Владеть инструментами оценки эффективности реализуемых технических решений

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Защита информации от утечки по техническим каналам (ОПК-18)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к сдаче и сдача государственного экзамена (ОПК-18), Подготовка к сдаче и сдача государственного экзамена (ПК-4), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ПК-4)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические занятия

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

9 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Раздел 1	34	ОПК-18, ПК-4

Лекция. Постановка проблемы комплексного обеспечения информационной безопасности АС	2	ОПК-18, ПК-4
Лекция. Состав компонентов комплексной системы обеспечения ИБ	2	
Лекция. Методология формирования задач защиты	2	
Лекция. Интеграция средств информационной безопасности в технологическую среду	2	
Практическое занятие. Постановка проблемы комплексного обеспечения информационной безопасности АС. Состав компонентов КСИБ. Методология формирования задач защиты	4	
Практическое занятие. Интеграция средств информационной безопасности в технологическую среду. Этапы и особенности проектирования КСИБ на современном уровне и требования к ним	4	
Задания для самостоятельной работы, в том числе выполнение Подготовка к лекции Подготовка к защите лабораторные работы Подготовка к устному опросу	18	
Раздел 2	40	
Лекция. Этапы и особенности проектирования КСИБ на современном уровне и требования к ним	2	
Лекция. Типовая структура комплексной системы защиты информации от НСД	6	
Лекция. Методы и методики проектирования	2	
Практическое занятие. Этапы и особенности проектирования КСИБ на современном уровне и требования к ним. Типовая структура комплексной СЗИ от НСД	4	
Практическое занятие. Методы и методики проектирования	8	
Задания для самостоятельной работы, в том числе выполнение Подготовка к лекции Подготовка к защите лабораторные работы Подготовка к устному опросу	18	ОПК-18, ПК-4
Раздел 3	26	
Лекция. Методы и методики оценки качества КСИБ	4	
Практическое занятие. Методы и методики оценки качества КСИБ	4	
Задания для самостоятельной работы, в том числе выполнение Подготовка к лекции Подготовка к защите лабораторные работы Подготовка к устному опросу	18	ОПК-18, ПК-4
Раздел 4	44	
Лекция. Требования к эксплуатационной документации КСИБ	2	
Лекция. Аттестация по требованиям безопасности	4	
Лекция. Особенности эксплуатации КСИБ на объекте защиты	2	
Лекция. Ведение специальной информационной базы данных КСИБ	2	
Лекция. Система типовых документов по защите информации	4	
Практическое занятие. Требования к эксплуатационной документации КСИБ. Аттестация по требованиям безопасности	4	
Практическое занятие. Особенности эксплуатации КСИБ на	4	

объекте защиты. Ведение специальной информационной базы данных КСИБ		
Практическое занятие. Мониторинг и контроль состояния окружающей среды	4	
Задания для самостоятельной работы, в том числе выполнение реферата		
Подготовка к лекции		
Подготовка к защите лабораторные работы		
Подготовка к устному опросу	18	
Иная контактная работа:	0	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины (модуля) рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

Занятия лекционного типа дают систематизированные знания по дисциплине (модулю), концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. (при наличии)

Подготовка к **занятиям семинарского типа** включает ознакомление с планом практического (лабораторного) занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины (модуля).

Содержание **самостоятельной работы** определяется рабочей программой дисциплины (модуля), оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины (модуля), к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины (модуля) включает выполнение практической работы, подготовку реферата

Подготовка реферата осуществляется в течение семестра в соответствии индивидуальным планом работы преподавателя и перечнем рекомендуемых тем. Успешное написание реферата достигается путем анализа теоретических и практических материалов по выбранной теме. Подготовка к выполнению Подготовка заключается в: - внимательном изучении выбранной темы, уяснении цели и задачи работы; - изучении и анализе относящихся к данной теме организационно- правовых документов и материалов их практического применения. Написание реферата Используя лекционный материал, учебную и специальную литературу, информацию из современных периодических изданий подобрать материалы, необходимые для выполнения работы. Целью написания реферата является формирование и развитие профессиональных компетенций, приобретение практических навыков реализации требований по организации защиты информации, изучение современного опыта построения систем информационной безопасности, подготовка к зачету и экзамену по результатам дисциплины изучения дисциплины. Оформление реферата Составление отчета о проведенных исследованиях является заключительным этапом написания реферата. Отчет выполняется в электронном (машинописном) виде,

руководствуясь следующими положениями: - титульный лист оформляется в соответствии с требованиями по оформлению практических заданий и курсовых работ с указанием дисциплины и темы реферата; - Реферат должен содержать оглавление, введение, практическое использование/применение рассматриваемой темы, заключение, перечень используемой литературы. Допускается введение других разделов и приложений по усмотрению студента. Объем реферата, как правило, должен составлять 10-20 листов формата А-4.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине (модулю) является балльно-рейтинговый контроль

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Барабанов, А. В. Семь безопасных информационных технологий [Электронный ресурс] : монография / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов: ДМК Пресс, 2017. - 224 с. ISBN 978-5-97060-494-6.	https://e.lanbook.com/book/97352
2.	Технология построения защищенных автоматизированных систем [Текст] : метод. указания к выполнению практ. работ для студентов специальности 075500 "Комплексное обеспечение информ. безопасности автоматизир. систем" / [сост. Е. В. Зверева]. Йошкар-Ола: МарГТУ, 2005. - 42 с. Экземпляры: всего 60.	60
3.	Зегжда, Дмитрий Петрович. Основы безопасности информационных систем [Текст] : Учеб. пособие для вузов по спец. "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизир.систем" / Д. П. Зегжда, А. М. Ивашко. М.: Горячая линия - Телеком, 2000. - 449 с. ISBN 5-93517-018-3. Экземпляры: всего 9.	9
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.ru

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	107 (III)	Генератор шума Соната -P2 (1), Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Коммутатор D-Link DES-3200-28 (8), Коммутатор D-Link DES-3810-28 (2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Ноутбук Acer Aspire 3 A315-42 (1), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Система виброакустической защиты "Соната-AB" (1), Система виброакустической.защиты "Соната-PC2" (1), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый	Обучающийся твердо знает программный материал,	хорошо

уровень	излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

1. Понятие и сущность КСЗИ. 2. Назначение КСЗИ. 3. Задачи КСЗИ. 4. КСЗИ как средство выражения концептуальных основ защиты информации. 5. Методология защиты информации как теоретический базис построения КСЗИ. 6. Методологические основы организации КСЗИ. 7. КСЗИ как сложная человеко-машинная система. 8. Основные положения теории систем. 9. Принципы организации КСЗИ. 10. Основные требования, предъявляемые к КСЗИ. Содержательная характеристика этапов разработки КСЗИ. 11. Основные факторы, влияющие на организацию КСЗИ. 12. Методика определения состава защищаемой информации. 13. Этапы работы по выявлению состава защищаемой информации. 14. Функции руководства и подразделений организации, экспертной комиссии, службы защиты информации. 15. Классификация информации по видам тайны и степеням конфиденциальности. 16. Нормативное закрепление состава защищаемой информации. 17. Значение носителей защищаемой информации как объектов защиты. 18. Хранилища носителей информации как объект защиты. 19. Особенности помещений для работы с защищаемой информацией как объектов защиты. 20. Состав технических средств обработки, передачи, транспортировки информации, являющихся объектами защиты. 21. Факторы, определяющие необходимость защиты периметра и здания организации.

22. Каналы утечки информации. Физические основы возникновения каналов утечки

информации.

24. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию. 25. Определение возможных методов несанкционированного доступа к защищаемой информации. 26. Оценка степени опасности применения различных методов. Анализ потенциальных последствий реализации несанкционированного доступа. 27. Определение направлений и возможностей доступа нарушителей к защищаемой информации.

Перечень вопросов для проведения промежуточной аттестации

1. Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам. 2. Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования. 3. Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз. 4. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам. 5. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ. 6. Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности. 7. Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности организации». 8. Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию. 11. Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа. 12. Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией. 13. Контролируемая зона организации. Требования к введению внутриобъектового режима. 14. Организация пропускного режима. Типы пропусков. Учёт пропускных документов. 15. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки. 16. Возможные каналы утечки информации из помещений, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. 17. Требования СТР-К по защите помещений. Организация борьбы с утечкой информации из помещений. 18. Эксплуатационная документация объектов информатизации. Технический паспорт. 19. Аттестация объектов информатизации. Этапы проведения аттестации. 20. Порядок организации работ по созданию и эксплуатации объектов информатизации в соответствии с действующими нормативными документами ФСТЭК России. 21. Стадии жизненного цикла объектов информатизации. 22. Порядок организации эксплуатации автоматизированных систем и их средств защиты информации.