

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

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

30.06.2021 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**С.1.1.39 Анализ рисков информационной безопасности**

*(код и наименование дисциплины по учебному плану)*

Направление подготовки (специальность)	10.05.03 Информационная безопасность автоматизированных систем
Квалификация выпускника	Специалист (бакалавр/магистр/специалист)
Специализация	Безопасность автоматизированных систем критически важных объектов

Курс	5
Семестр	9

**Распределение учебного времени**

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	36	часов
Лабораторные работы	-	часов
Практические занятия	54	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	90	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	54	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:

заведующий кафедрой с ученой степенью доктора наук и ученым званием "профессор"	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)
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)		
31.05.2021	протокол №	23	
(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 01.07.2021 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

## 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-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1 знает содержание и этапы проектной деятельности по созданию автоматизированных систем в защищенном исполнении	<b>знания:</b> знает содержание и этапы проектной деятельности по созданию автоматизированных систем в защищенном исполнении <b>умения:</b> <b>навыки:</b>
	ОПК-9.2 умеет анализировать и составлять нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами	<b>знания:</b> <b>умения:</b> умеет анализировать и составлять нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами <b>навыки:</b>
	ОПК-9.3 Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы	<b>знания:</b> Знает технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы <b>умения:</b> Умеет проводить технико-экономические оценки целесообразности создания системы защиты информации автоматизированной системы <b>навыки:</b> Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы
2. ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный	ОПК-15.1 знает программные средства, позволяющие вести автоматизированный аудит	<b>знания:</b> знает программные средства, позволяющие вести автоматизированный аудит <b>умения:</b> <b>навыки:</b>
	ОПК-15.2 умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	<b>знания:</b> <b>умения:</b> умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы <b>навыки:</b>

защищенности автоматизированных систем	ОПК-15.3 Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	<b>знания:</b> Знает как анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах <b>умения:</b> Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах <b>навыки:</b> Владеет навыком анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах
--	--	---

## 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: Методы прогнозирования возможных угроз информационной безопасности (ОПК-9), Сети и системы передачи информации (ОПК-9), Техническая защита информации (ОПК-15)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Техническая защита информации (ОПК-9), Программно-аппаратные средства защиты информации (ОПК-15), Техническая защита информации (ОПК-15); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-9), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-15)

## 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 и лабораторные 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
<b>Угрозы информационной безопасности</b>	<b>26</b>	ОПК-15, ОПК

		-9
Лекция. Введение. Основные понятия. Предмет и задачи дисциплины	2	
Лекция. Базовые вопросы управления информационной безопасностью	2	
Лекция. Стандартизация в области управления информационной безопасностью	2	
Лекция. Система управления информационной безопасностью. Область действия системы информационной безопасности	4	
Лекция. Аудит системы управления информационной безопасности	2	
Практическое занятие. Формирование перечней угроз информационной безопасности и мероприятий по их минимизации	4	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к защите практической работы Подготовка к устному опросу	10	ОПК-15, ОПК-9
<b>Оценка рисков информационной безопасности</b>	<b>34</b>	
Лекция. Основные процессы СУИБ. Обязательная документация СУИБ.	2	
Лекция. Управление рисками и инцидентами информационной безопасности. Методики анализа рисков информационной безопасности	4	
Лекция. Аудит системы управления информационной безопасности	2	
Практическое занятие. Анализ модели угроз и уязвимостей	8	
Практическое занятие. Построение программы и методик аудита информационной безопасности	8	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к защите практической работы Подготовка к устному опросу	10	ОПК-15, ОПК-9
<b>Методы управления рисками информационной безопасности</b>	<b>36</b>	
Лекция. Внедрение разработанных процессов	4	
Лекция. Управление инцидентами ИБ	6	
Лекция. Обеспечение соответствия требованиям законодательства РФ	4	
Практическое занятие. Разработка и управление политикой ИБ	8	
Практическое занятие. Документирование процесса внедрения разработанных процессов	4	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к защите практической работы Подготовка к устному опросу	10	ОПК-15, ОПК-9
<b>Технические методы управления ИБ</b>	<b>48</b>	
Лекция. Разработка частной модели угроз информационной безопасности	2	

Практическое занятие. Разработка модели угроз информационной безопасности	22	
Задания для самостоятельной работы, в том числе выполнение реферата		
Подготовка к защите практической работы	24	
Иная контактная работа:	0	

## Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины 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, 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.

Подготовка к **занятиям семинарского типа** включает ознакомление с планом практического 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.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины, 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, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины включает выполнение лабораторной 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.

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
<b>УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ</b>		
1.	Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учеб. пособие по специальностям в обл. информ. безопасности / С. Н. Семкин, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. М.: Гелиос АРВ, 2005. - 185 с. ISBN 5-85438-042-0. Экземпляры: всего 30.	30
2.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2023. - 324 с. ISBN 978-5-8114-6738-9.	<a href="https://e.lanbook.com/book/341267">https://e.lanbook.com/book/341267</a>
3.	Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 266 с. ISBN 978-5-94774-821-5.	<a href="https://e.lanbook.com/book/100295">https://e.lanbook.com/book/100295</a>
<b>ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ</b>		
1.	Научная электронная библиотека eLIBRARY.RU	<a href="http://elibrary.ru">http://elibrary.ru</a>
2.	Научная электронная библиотека «Киберленинка»	<a href="http://cyberleninka.ru">http://cyberleninka.ru</a>
<b>ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ</b>		
1.	Справочно-правовая система Консультант+	<a href="http://www.consultant.ru">http://www.consultant.ru</a>

### 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)	Доска маркерная 100*200см (1), 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	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,

	EAR003, Монитор 24" BenQ G2450HM, клавиатура, мышь (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	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 уровень	Обучающийся твердо знает программный материал, 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	хорошо
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. Место анализа рисков в общей схеме управления ИБ2. Количественный подход к оценке рисков. Достоинства, недостатки подхода.3. Качественный подход к оценке рисков. Достоинства, недостатки подхода.

4. ГОСТ Р ИСО 31000-2010: принципы и схема процесса риск менеджмента.

5. ГОСТ ИСО/МЭК 27001-2006. Мониторинг и анализ системы менеджмента информационной безопасности

6. Управление рисками и жизненный цикл информационной системы.7. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий.

Введение и общая модель». Основные понятия и их взаимосвязь.8. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий.

Введение и общая модель». Профиль защиты9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Общие положения.10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Порядок определения актуальных угроз.11. Базовая модель угроз информационной безопасности персональных данных при их обработке в информационных системах персональных данных. Классификация угроз безопасности.

12. Модель угроз информационной безопасности на основе методических документов ФСТЭК России.

## Перечень вопросов для проведения промежуточной аттестации

1. Понятие уязвимости, угрозы, атаки, риска, оценки риска.2. Экономическая модель оценки риска: основное содержание, достоинства, недостатки.3. Модель риска типа «узла»: основное содержание, пример.4. Вероятностная модель: основное содержание, достоинства, недостатки.5. Отличие вероятностной модели оценки рисков от экономической модели оценки рисков.6. Понятие уровня безопасности организации.7. Этапы проведения аудита информационной безопасности.

8. Виды аудита информационной безопасности.9. Актив, типы активов.10. Риск, угроза, уязвимость, механизмы контроля.11. Порядок определения актуальных угроз безопасности информации.12. Классификация угроз безопасности.13. Угрозы утечки информации по техническим каналам.14. Угрозы несанкционированного доступа к информации