

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

02.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.39 Организация защиты объектов критической инфраструктуры

(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	4
Семестр	8

Распределение учебного времени

Трудоемкость по учебному плану	180 / 5	часов/зачетных единиц
Лекции	32	часов
Лабораторные работы	32	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	64	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	80	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	8	семестр
Зачет	-	семестр
БРК, ДЗ	-	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.П. Александров
(должность)	(кафедра)		(И.О. Фамилия)
заведующая кафедрой	БД	СОГЛАСОВАНО	И.Г. Сидоркина
(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 07.02.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /М.Л. Бойкова/

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-17 Способен осуществлять внедрение и эксплуатацию систем защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	ОПК-17.1 знает программно-аппаратные средства обеспечения защиты информации автоматизированных систем	знания: знает программно-аппаратные средства обеспечения защиты информации автоматизированных систем умения: навыки:
	ОПК-17.2 умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	знания: умения: умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы навыки:
	ОПК-17.3 владеть навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах	знания: умения: навыки: владеть навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Сети ЭВМ и распределенная обработка информации (ОПК-17); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-17)

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, процедуры самообучения

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

8 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Аудиторная и самостоятельная работа	144	ОПК-17
<p>Лекция. Темы лекций:</p> <ol style="list-style-type: none"> 1. Понятие критической информационной инфраструктуры. 2. Субъекты и объекты КИИ, их права и обязанности. 3. Категории объектов критической информационной инфраструктуры 4. Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры 5. Технические и организационные меры безопасности значимых объектов 6. Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры. 7. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) 8. Аудит безопасности критической инфраструктуры. 	32	
<p>Лабораторная работа. Практические занятия:</p> <ol style="list-style-type: none"> 1. Основы обеспечения безопасности КИИ Российской Федерации. Термины и определения, понятие критической информационной инфраструктуры. 2. Категорирование объектов КИИ. Оформление и передача в ФСТЭК России результатов категорирования 3. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ. 4. Перечень показателей критериев ЗОКИИ и их значения. 5. Оценка в соответствии с перечнем показателей критериев ЗОКИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. 6. Требования по обеспечению безопасности значимых объектов КИИ РФ. 7. Система безопасности значимого объекта КИИ. 8. Организационные меры по обеспечению безопасности значимого объекта КИИ 9. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ 10. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ 11. Контроль за обеспечением безопасности значимого объекта КИИ 12. Перечень информации, представляемой в ГосСОПКА. Порядок представления информации в ГосСОПКА. 13. Этапы проведения аудита. Практические особенности проведения аудита КИИ. 14. Тестирование как один из основных типов аудита критической информационной инфраструктуры 15. Тестирование критической инфраструктуры специальными информационно-психологическими воздействиями. 16. Юридическая ответственность за преступления и 	32	

правонарушения в области защиты КИИ.		
Задания для самостоятельной работы, в том числе выполнение РГР		
Темы РГР:		
1. Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ		
2. Категорирование объектов КИИ, понятие, общий порядок. Комиссия по категорированию, порядок создания и деятельности комиссии.		
3. Субъекты и объекты КИИ, понятие, определение принадлежности, права и обязанности.		
4. Перечень критических процессов субъекта КИИ, порядок формирования перечня.		
5. Процедура категорирования объекта КИИ. Определение категории значимости объекта КИИ.		
6. Уязвимости объектов КИИ, классификация уязвимостей.		
7. Методы оценки возможных последствий реализации возникновения угроз безопасности информации значимого объекта КИИ.		
8. Основные требования по обеспечению безопасности значимого объекта КИИ. СОИБ значимого объекта КИИ.		
9. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.		
10. Требования к организационным и техническим мерам, направленным на блокирование (нейтрализацию) угроз безопасности информации значимого объекта КИИ.		
11. Основные документы системы безопасности значимых объектов КИИ и обеспечения их функционирования.		
12. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ.	80	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение 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 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.

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 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 **расчётно-графической работы**.

Подготовка расчётно-графических работ осуществляется в течение семестра в соответствии с перечнем рекомендуемых тем РГР. Успешное выполнение РГР достигается путем анализа теоретических и практических материалов по выбранной теме тщательной подготовке к защите РГР.

Подготовка к выполнению РГР

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.

Выполнение РГР

Используя лекционный материал, действующие в Российской Федерации нормативно-правовые документы, регламентирующие деятельность в сфере информационной безопасности, учебную и специальную литературу, информацию из современных периодических изданий подобрать материалы, необходимые для выполнения РГР. В работе могут приводиться примеры применения организационно-правовых и технических мер защиты информации по выбранной теме на российских предприятиях и в учреждениях, зарубежный опыт работы в данной области информационной безопасности, мнения о дальнейшем совершенствовании защиты информации в рассматриваемой области.

Целью выполнения РГР является формирование и развитие профессиональных компетенций, приобретение практических навыков реализации требований по организации защиты информации, изучение современного опыта построения систем информационной безопасности, подготовка к БКР по результатам изучения дисциплины.

Оформление РГР

Составление отчета о проведенных исследованиях является заключительным этапом выполнения РГР. 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 РГР;
- РГР должна содержать оглавление, введение с постановкой задачи, аналитическую часть, практическое использование/применение рассматриваемой темы, заключение, перечень используемой литературы. Допускается введение в РГР других разделов и приложений по усмотрению студента. Объем РГР как правило должен составлять 15-30 листов формата А-4;
- к защите РГР готовиться презентация, состоящая из 10-15 слайдов.

Защита РГР проводится индивидуально.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по модулю является экзамен.

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

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющихся в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	https://e.lanbook.com/book/293009
2.	Галатенко, В. А. Стандарты информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 307 с. ISBN 5-9556-0053-1.	https://e.lanbook.com/book/100511
3.	Смирнов, Владимир Иванович. Защита информации [Текст] : лабораторный практикум : [по направлению 09.03.01] / В. И. Смирнов; М-во образования и науки Рос. Федерации, ФГБОУ ВО "Поволж. гос. технол. ун-т". Йошкар-Ола: ПГТУ, 2017. - 65 с. ISBN 978-5-8158-1866-8. Экземпляры: всего 24.	24 / https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf
4.	Чекулаева, Елена Николаевна. Управление информационной безопасностью [Текст] : учебное пособие : для студентов и магистрантов направлений подготовки 10.05.03 "Информационная безопасность автоматизированных систем", 10.04.01 "Информационная безопасность" / Е. Н. Чекулаева, Е. С. Кубашева; Министерство науки и высшего образования Российской Федерации, ФГБОУ ВО "Поволжский государственный технологический университет". Йошкар-Ола: ПГТУ, 2020. - 153 с. ISBN 978-5-8158-2165-1. Экземпляры: всего 15.	15 / https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf
5.	Тумбинская, М. В. Защита информации на предприятии [Электронный ресурс] : учебное пособие / Тумбинская М. В., Петровский М. В. Санкт-Петербург: Лань, 2020. - 184 с. ISBN 978-5-8114-4291-1.	https://e.lanbook.com/book/130184
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.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.	535 (III)	Мультимедийный комплект 4 (1), Ноутбук Acer (1), Персональный компьютер в сборе PowerCool(Core i3-8100/H310/16GbDDR4/HDD 0.5Tb/23"6 АОС/кл.мышь/пач-корд 3м) (20), 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 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	отлично

	<p>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</p>	
--	--	--

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.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ № 1

По модулю: «Организация защиты объектов критической информационной структуры»

1. Объекты и субъекты КИИ.

2. Структура системы безопасности значимых объектов КИИ.

Зав. кафедрой ИБ _____ И.Г. Сидоркина

«___» _____ 20__ г.

Перечень вопросов для проведения промежуточной аттестации

Перечень
вопросов к экзамену

1. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.
2. Объекты и субъекты КИИ.
3. Определение принадлежности к субъектам КИИ, их права и обязанности.
4. Правила категорирования объектов КИИ. Общий порядок работ, сроки категорирования.
5. Критерии значимости объектов КИИ.
6. Формирование перечня критических процессов, перечня объектов КИИ, подлежащих категорированию.
7. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.
8. Особенности обеспечения безопасности объектов КИИ.
9. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
10. Государственный контроль в области обеспечения безопасности объектов КИИ. Цели государственного контроля в области обеспечения безопасности объектов КИИ.
11. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.
12. Оценка в соответствии с перечнем показателей критериев значимых объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов.
13. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ.
14. Основные требования по обеспечению безопасности значимых объектов КИИ.
15. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимых объектов КИИ. Цели и задачи планирования.
16. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ.
17. Цели и задачи системы безопасности значимого объекта КИИ.
18. Требования к силам обеспечения безопасности значимых объектов КИИ.
19. Структура системы безопасности значимых объектов КИИ.
20. Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ и эффективности, принимаемых организационных и технических мер.