

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)

ФТД.2.1 Интеллектуальные системы 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	3
Семестр	6

Распределение учебного времени

Трудоемкость по учебному плану	108 / 3	часов/зачетных единиц
Лекции	18	часов
Лабораторные работы	36	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	54	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	6	семестр
БРК, ДЗ	-	семестр

(год)

Оборотная сторона титульного листа

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)

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-19 Способен разрабатывать системы защиты информации, функционирующие на критически важных объектах и в автоматизированных системах критически важных объектов	ОПК-19.1 знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	знания: знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах умения: навыки:
	ОПК-19.2 умеет оценивать информационные риски в автоматизированных системах	знания: умения: умеет оценивать информационные риски в автоматизированных системах навыки:
	ОПК-19.3 Владеть методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем	знания: умения: навыки: Владеть методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем
2. ПК-4 Способен применять инструментарий анализа безопасности программного обеспечения	ПК- 4.1.1 знает принципы организации и структуру систем защиты информации и программного обеспечения автоматизированных систем	знания: знает принципы организации и структуру систем защиты информации и программного обеспечения автоматизированных систем умения: навыки:
	ПК- 4.2.1 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- 4.2.2 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- 4.2.3 владеет инструментами анализа эффективности реализуемых технических решений	знания: умения: навыки: владеет инструментами анализа эффективности реализуемых технических решений
---	--

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к элективным дисциплинам (модулям) ОПОП.

Дисциплина является факультативной

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Методы прогнозирования возможных угроз информационной безопасности (ПК-4), Системы обнаружения и предотвращения компьютерных атак (ОПК-19), Защита АСУТП объектов КИИ (ОПК-19), Создание и модернизация системы безопасности значимых объектов КИИ (ОПК-19); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ПК-4), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-19)

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, информационные, классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Защита информации в интеллектуальных системах	108	ОПК-19
Лекция. Основные понятия и определения. Задачи информационной безопасности.	3	
Лабораторная работа. Проблемы создания защищенных информационных систем.	9	
Лекция. Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. Понятие и виды защищаемой информации.	5	
Лабораторная работа. Обзор и сравнительный анализ стандартов информационной безопасности	9	
Лекция. Общая характеристика способов и средств защиты информации. Криптографические методы защиты информации.	5	
Лабораторная работа. Методология анализа защищенности интеллектуальной информационной системы	9	
Лекция. Электронная цифровая подпись и цифровые	5	

сертификаты. Программно-аппаратные средства защиты информации.		
Лабораторная работа. Обеспечение интегральной безопасности интеллектуальной системы.	9	
Задания для самостоятельной работы, в том числе выполнение Подготовка к лекции.		
Подготовка к устному опросу	54	
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 **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 **лабораторной работы**. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине **(модулю)** является **зачёт**.

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.	Малюк, Анатолий Александрович. Информационная безопасность [Текст] : концептуальные и методологические основы защиты информации : [учеб. пособие для студентов вузов по специальности 075400 "Комплексная защита объектов информ."] / А. А. Малюк.	10

	М.: Горячая линия - Телеком, 2004. - 280 с. ISBN 5-93517-197-X. Экземпляры: всего 10.	
2.	Хохлов, Геннадий Иванович. Основы теории информации [Текст] : [учеб. пособие для вузов по специальности "Комплекс. обеспечение информ. безопасности автоматизир. систем"] / Г. И. Хохлов. М.: Академия, 2008. - 170, [1] с. ISBN 978-5-7695-4576-4. Экземпляры: всего 10.	10
3.	Богомолова, М. А. Экспертные системы (техника и технология проектирования) [Текст] : Методические указания к лабораторным работам / М. А. Богомолова. Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. - 47 с.	http://www.iprbookshop.ru/71908
4.	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
5.	Мельников, Виталий Викторович. Безопасность информации в автоматизированных системах [Текст] / В. В. Мельников. М.: Финансы и статистика, 2003. - 367 с. ISBN 5-279-02560-7. Экземпляры: всего 20.	20

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	Зачтено

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.

- Разработать экспертную систему учета посещаемости студентов группы ВУЗа.
- Построить нейронную сеть распознавания 2-х букв алфавита.
- Построить нейронную сеть принятия решения, что делать после 18-00 в выходные.
- Разработать нечетко-логическую схему распознавания уровня финансового показателя.

Перечень вопросов для проведения промежуточной аттестации

- 1 Определение информационной безопасности.
- 2 Критические данные.
- 3 Признаки компьютерных преступлений в интернет технологиях.
- 4 Основные технологии и методы компьютерных преступлений.
- 5 Уровня защиты компьютерных (интернет технологий) и информационных ресурсов.
- 6 Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
- 7 Концепция обеспечения безопасности информационных систем.
- 8 Избирательная политика управления доступом.
- 9 Организационные меры безопасности информационных систем.
- 10 Матрица доступа в АСОИ.
- 11 Полномочное управление доступом.
- 12 Избирательное управление доступом.

- 13 Оценочные стандарты и технические спецификации.
- 14 Угрозы безопасности данных
- 15 Источники нарушений безопасности
- 16 Аутентификация
- 17 Авторизация пользователей
- 18 Методы парольной аутентификации. Недостатки методов аутентификации с запоминаемым паролем.
- 19 Аутентификация с помощью биометрических характеристик.
- 20 Принципы работы биометрических систем.
- 21 Реализация биометрических систем.
- 22 Поведенческие биометрические характеристики.
- 23 Атаки на биометрические системы.
- 24 Концепция шифрования на открытом ключе.
- 25 Концепция шифрования на закрытом ключе
- 26 Понятие хэш-функции. Общая схема образования хэш-функции.
- 27 ЭЦП RSA
- 28 ЭЦП Эль-Гамаль
- 29 ЭЦП ГОСТ Р 34.10-2001
- 30 Базовая модель криптографии