

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

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

07.02.2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

С.1.1.28 Безопасность операционных систем

(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	5, 6

**Распределение учебного времени**

Трудоемкость по учебному плану	324 / 9	часов/зачетных единиц
Лекции	72	часов
Лабораторные работы	108	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	180	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	108	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	6	семестр
Зачет	5	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 с ученой степенью кандидата наук	ИБ	СОГЛАСОВАНО	А.А. Кречетов
(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 13.02.2023 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-7 Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 знает язык программирования высокого уровня (объектно-ориентированное программирование)	<b>знания:</b> - язык(и) высокого уровня - требования предъявляемые к разрабатываемым системам <b>умения:</b> <b>навыки:</b>
	ОПК-7.2 умеет работать с интегрированной средой разработки программного обеспечения умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач	<b>знания:</b> <b>умения:</b> - разрабатывать программы на языках высокого уровня <b>навыки:</b>
	ОПК-7.3 Разработка программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	<b>знания:</b> - язык(и) высокого уровня - требования предъявляемые к разрабатываемым системам <b>умения:</b> - разрабатывать программы на языках высокого уровня <b>навыки:</b> - разработка программного обеспечения для обеспечения безопасности
2. ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1 знает принципы построения и функционирования, примеры реализаций современных операционных систем	<b>знания:</b> - защитные механизмы и средства обеспечения безопасности операционных систем; - основные требования к подсистеме аудита и политике аудита; - средства и методы хранения и передачи аутентификационной информации; - методы восстановления работоспособности прикладного и системного программного обеспечения; <b>умения:</b> <b>навыки:</b>
	ОПК-12.2 Основные информационные технологии, используемые в автоматизированных системах	<b>знания:</b> - защитные механизмы и средства обеспечения безопасности операционных систем; - основные требования к подсистеме аудита и политике аудита; - средства и методы хранения и передачи

		аутентификационной информации; - методы восстановления работоспособности прикладного и системного программного обеспечения; <b>умения:</b> - настраивать политики безопасности операционных систем. <b>навыки:</b> - тестирования программных и аппаратных средств
	ОПК-12.3 Проводить комплексное тестирование аппаратных и программных средств	<b>знания:</b> - защитные механизмы и средства обеспечения безопасности операционных систем; - основные требования к подсистеме аудита и политике аудита; - средства и методы хранения и передачи аутентификационной информации; - методы восстановления работоспособности прикладного и системного программного обеспечения; <b>умения:</b> - настраивать политики безопасности операционных систем. <b>навыки:</b> - тестирования программных и аппаратных средств

## 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: Объектно-ориентированное программирование (ОПК-7), Языки программирования (ОПК-7), Технология и методы программирования (ОПК-7)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Безопасность систем баз данных (ОПК-12); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-7), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-12)

## 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

### 5 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Архитектура ОС	144	ОПК-12, ОПК

		-7
Лекция. Архитектурные особенности современных ОС. Общая характеристика ОС; назначение и возможности систем семейства UNIX, систем семейства Windows. Интерфейс взаимодействия ОС с пользователями. Общие принципы управления ресурсами вычислительных систем. Понятия процесса (потока) в ОС. Средства межпроцессорного взаимодействия. Управление памятью в ОС. Виртуальная память.	12	
Лекция. Управление доступом. Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Подходы к организации защиты в операционной системе. Этапы построения защиты. Административные меры защиты.	12	
Лекция. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в Linux. Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов: олицетворение субъектов доступа.	12	
Лабораторная работа. Механизмы безопасности ОС Windows.	14	
Лабораторная работа. Подсистема контроля доступа в ОС Windows	14	
Лабораторная работа. Безопасность сетевых сервисов ОС Windows	14	
Лабораторная работа. Обеспечение безопасности веб-серверов ОС Windows	12	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к лабораторным работам	54	
Иная контактная работа:	0	

### 6 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Безопасность ОС</b>	<b>144</b>	ОПК-12, ОПК-7
Лекция. Идентификация, аутентификация и авторизация. Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи	12	

аутентификационной информации по каналам вычислительной сети. Криптографическое Обеспечение аутентификации пользователей. Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в Linux, библиотеки PAM. Парольная аутентификация в Windows, средства управления параметрами аутентификации. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы.	
Лекция. Аудит и регистрация событий. Политика аудита. Аудит в ОС семейства UNIX/Linux. Управление подсистемой аудита в ОС Linux. Аудит в ОС семейства Windows Управление подсистемой аудита в ОС Windows. Инструментальные средства анализа журналов аудита.	12
Лекция. Вспомогательные механизмы защиты информации. Критические компоненты операционных систем, требующие дополнительных средств для повышения защищенности. Стеганографические и криптографические возможности современных ОС.	12
Лабораторная работа. Механизмы безопасности ОС Linux	14
Лабораторная работа. Подсистема контроля доступа в ОС	14
Лабораторная работа. Безопасность сетевых сервисов ОС Linux	14
Лабораторная работа. Обеспечение безопасности веб-серверов ОС Linux	12
Задания для самостоятельной работы, в том числе выполнение Проработка лекций Подготовка к лабораторным работам	54
Иная контактная работа:	0
Подготовка к экзамену	30
Проведение экзамена	6

## 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**) 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, экзамен.

## 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.	Таненбаум, Эндрю. Современные операционные системы [Текст] : [12+] / Э. Таненбаум, Х. Бос. 4-е изд. Москва: Питер, 2015. - 1119 с. ISBN 978-5-496-01395-6. Экземпляры: всего 5.	5
2.	Дейтел, Харви М. Операционные системы [Текст] : [учебник]. Ч. 2 : Распределенные системы, сети и безопасность, 2013. - 704 с. ISBN 978-5-9518-0432-7. Экземпляры: всего 15.	15
3.	Операционные системы. Программное обеспечение [Электронный ресурс] : учебник. Санкт-Петербург: Лань, 2020. - 248 с. ISBN 978-5-8114-4290-4.	<a href="https://e.lanbook.com/book/131045">https://e.lanbook.com/book/131045</a>
4.	Староверова, Н. А. Операционные системы [Электронный ресурс] : учебник / Н. А. Староверова. Санкт-Петербург: Лань, 2022. - 308 с. ISBN 978-5-8114-4000-9.	<a href="https://e.lanbook.com/book/207089">https://e.lanbook.com/book/207089</a>
<b>ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ</b>		
1.	Научная электронная библиотека eLIBRARY.RU	<a href="http://elibrary.ru">http://elibrary.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)	Анализатор линейных коммуникаций УЛАН-2 (1), 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), Комплекс защиты информации Secret Disk 4.0 (1), Комплекс защиты информации Secret Net 5.0	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

	(2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/M "Катран" (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), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	
--	---	--

## 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



	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	
--	---	--

### 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.

Операционная система - комплекс взаимосвязанных программ, действующий как интерфейс между приложениями и пользователями с одной стороны, а с другой стороны - ...

- 1) + аппаратурой компьютера
- 2) - внешними устройствами
- 3) - оперативной памятью
- 4) - накопителями информации

В наибольшей степени подчеркивают роль ОС критерии эффективности вычислительной системы (выберите несколько ответов):

- 1) - качество графического интерфейса
- 2) + пропускная способность
- 3) + удобство работы пользователей
- 4) + реактивность

Важной причиной применения программных прерываний вместо обычных инструкций вызова подпрограмм является возможность смены пользовательского режима процессора на \_\_\_\_\_ одновременно с вызовом процедуры.

- 1) + привилегированный
- 2) - авторизованный
- 3) - пользовательский

4) - обычный

Перечень вопросов для проведения промежуточной аттестации

1.

Определение и назначение ОС

2.

Виды ОС

3.

Функции ОС

4.

Архитектура операционной системы

5.

Структура ОС

6.

Монолитная архитектура

7.

Микроядерная архитектура

8.

Понятия вычислительного процесса и ресурса

9.

Прерывания

10.

Системные вызовы

11.

Процесс, поток.

12.

Создание процессов и потоков

13.

Состояния потока

14.

Планирование и диспетчеризация потоков

15.

## Алгоритмы планирования

16.

## Управление памятью

17.

## Типы адресов

18.

## Методы распределения памяти без использования дискового пространства

19.

## Методы распределения памяти с использованием дискового пространства

20.

## Понятие виртуальной памяти

21.

## Страничное распределение виртуальной памяти

22.

## Сегментное распределение виртуальной памяти

23.

## Странично-сегментное распределение виртуальной памяти

24.

## Свопинг

25.

## Назначение и функции файловой системы

26.

## Логическая организация файловой системы

27.

## Файловая система FAT

28.

## Файловая система NTFS

29.

## Контроль доступа к файлам

30.

## Основные понятия безопасности ОС

31.

Системный подход к обеспечению безопасности

32.

Симметричные криптосистемы

33.

Асимметричные криптосистемы

34.

Аутентификация

35.

Аутентификация на основе многоразовых паролей

36.

Аутентификация на основе одноразовых паролей

37.

Цифровые сертификаты

38.

Цифровые подписи

39.

Авторизация доступа

40.

Аудит