

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

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

14.02.2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б.1.2.11 Компьютерная вирусология

(код и наименование дисциплины по учебному плану)

Направление подготовки  
(специальность)

09.03.04 Программная инженерия

Квалификация выпускника

Бакалавр

(бакалавр/магистр/специалист)

Направленность

Разработка программных систем

Курс 4  
Семестр 8

**Распределение учебного времени**

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	16	часов
Лабораторные работы	24	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	40	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	104	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	8	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.03.04 Программная инженерия

Программу составили:

ИиСП	СОГЛАСОВАНО	А.В. Бородин
заведующий кафедрой с ученой		
степенью кандидата наук		
(должность)	(кафедра)	(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина  
Кафедра информатики и системного программирования

(наименование кафедры)		
05.02.2024	протокол №	7
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

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

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	А.В. Бородин
		(И.О. Фамилия)

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

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

Эксперт(ы): Егошин Алексей Борисович, ген. директор ООО "Цитрус"

Рабочая программа проверена и зарегистрирована в УМЦ 12.03.2024 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. ПК-12 Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных	ПК-12.1 Знает методы формальных спецификаций и системы управления базами данных	<b>знания:</b> Знает методы формальных спецификаций, включая используемые в задачах информационной безопасности, и системы управления базами данных <b>умения:</b> <b>навыки:</b>
	ПК-12.2 Умеет применять современные средства и языки программирования	<b>знания:</b> <b>умения:</b> Умеет применять современные средства и языки программирования <b>навыки:</b>
	ПК-12.3 Имеет навыки использования операционных систем	<b>знания:</b> <b>умения:</b> <b>навыки:</b> Имеет навыки использования операционных систем, в том числе при решении задач информационной безопасности

## Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Проектный практикум (ПК-12)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ПК-12)

## Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

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

Основными стратегическими технологиями являются: исследовательские, лекционные занятия, практические и лабораторные занятия, процедуры самообучения

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

## Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

**8 семестр**

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Компьютерная вирусология</b>	<b>144</b>	ПК-12
Лекция. Лекция №1. Вводная лекция. История становления курса. Понятие модели угроз. Классификация моделей угроз.	2	
Лекция. Лекция №2. Вредоносная программа: правовая квалификация. Основные термины и определения. Признаки вредоносности. Ситуационное моделирование.	2	
Лекция. Лекция №3. Классификация вредоносных программ и программных компонент. Алгоритмическая модель типового компьютерного вируса.	2	
Лекция. Лекция №4. Технологии обнаружения признаков вредоносности программ и программных компонент: случай скриптовых языков программирования, общий случай.	2	
Лекция. Лекция №5. Проблемы формального определения компьютерного вируса. Классификационные признаки компьютерных вирусов и особенности поведения инфицированных программ и программных систем. Основной классификационный признак в контексте теоретико-множественного формализма. Современное параопределение компьютерного вируса. ГОСТы и жизненный цикл вредоносных программ.	2	
Лекция. Лекция №6. Теоретико-алгоритмические проблемы обнаружения компьютерных вирусов: основные теоремы.	2	
Лекция. Лекция №7. Обнаружение вредоносных программ на практике.	2	
Лекция. Лекция №8. Существование компьютерных вирусов в контексте базовых архитектур вычислительных систем. Субъектно-объектный формализм при анализе проблемы существования компьютерных вирусов.	1	
Лекция. Лекция №9. Понятие политики безопасности. Основные политики безопасности противодействия угрозе существования компьютерных вирусов.	1	
Лабораторная работа. Лабораторная работа №1. Анализ кода на вредоносность. Случай скриптовых языков программирования.	8	
Лабораторная работа. Лабораторная работа №2. Анализ кода на вредоносность. Общий случай.	8	
Лабораторная работа. Лабораторная работа №3. Выделение оптимальных сигнатур РПВ.	8	
Задания для самостоятельной работы, в том числе выполнение История вредоносных программ и программных компонент: Червь Морриса, KB в MS DOS, KB в MS Windows, Android как среда обитания вредоносных программ.  Результаты Ф. Козна.  Понятие сигнатуры вредоносного кода.  Подходы IBM к выделению оптимальных сигнатур.		
Экономика компьютерных вирусов.	104	
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 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.

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 лабораторных работ. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине является БРК.

## 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.	Бородин, Андрей Викторович. Феномен компьютерных вирусов: элементы теории и экономика существования [Текст] : учеб. пособие для студентов вузов по специальности 351400 "Прикладная информатика (по областям)" и др. междисциплинар. специальностям / А. В. Бородин. Йошкар-Ола: МарГТУ, 2004. - 144 с. ISBN 5-8158-0347-2. Экземпляры: всего 42.	42
2.	Грушо, Александр Александрович. Теоретические основы компьютерной безопасности [Текст] : [учеб. пособие для вузов по специальностям группы 090100 "Информ. безопасность"] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. М.: Академия, 2009. - 267, [1] с. ISBN 978-5-7695-4242-8. Экземпляры: всего 10.	10
3.	Дейтел, Харви М. Операционные системы [Текст] : [учебник]. Ч. 2 : Распределенные системы, сети и	15

	безопасность, 2013. - 704 с. ISBN 978-5-9518-0432-7. Экземпляры: всего 15.	
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.	<a href="https://e.lanbook.com/book/293009">https://e.lanbook.com/book/293009</a>
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
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>
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
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.	429 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S ATA3/монит.LCD PHILIPS 23,6"клав.,м (8), Принтер HP LaserJet Professional P1102 (1), Проектор VIEWSONIC PJD6550LW белый (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
2.	430 (III)	ПК RAMEC GALE/i7-3770/B75M2x4DDR3/GTX650/500S ATA3/монит.LCD PHILIPS 23,6"клав.,м (8), Проектор VIEWSONIC PJD6550LW белый (1), Шкаф телекоммуникационный напольный ЦМО ШТК-М (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
3.	521 (I)	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
4.	522 (I)	Анализатор спектра NS-30A (1), Антенна M102 в компл. с кабелем ВЧ TNCm-SMAm (1), Блок питания лаборат. НУ 3003 D-3 (1), Внешний HDD WD 2TB 3.0 , 3.5"USB (1), Внешний накопитель 1 Seagate Original USB 3.0 4 Tb (1), Внешний накопитель флешка USB TRANSCEND Jetflash 780 64 Gb (1), Гигабитный управляемый коммутатор на 16 портов (1), Измеритель CN -801 HP (1), Кондиционер AEG ACS-09HR (1), Многофункциональный измерительный прибор (1), Монитор 20 "Beng FP 202W (2), Монитор LCD Samsung 17" SM 713N (1), МФУ Canon i-SENSYS MF 4018 (1), МФУ 1 Лазерный Canon i-Sensys MF226 (1), Набор ВЧ переходников (1), Ноутбук Dell Latitude E6520 Intel Core I5 Processor 2520M 15,6" (2), Ноутбук TOSHIBA Satellite L655-1H2-RU (1), Паяльная станция AOYUE 968 (1), Переключатель ZX80-DR230 (1), Персональный компьютер 3 Atlant A2X4/4G(3)/512Mb/монитор Pyama 2209/3Y (1), ПК RAMEC GALE LCD LG 23"/Intel i5 4590/MSI B85M- E45/2x4DDR3/GT740 2Gb/500Gb/клав (28), Преобразователь SP-200-24-AC-DC в кожухе 199x99x50мм (1), Приемо- передающая программно- конфигурируемая радиоплатформа G32 (1), Принтер Canon LBP 2900 лазерный с кабелем (1), Проектор	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

	мультимедийный Hitachi CP-EX250 (1), Проектор мультимедийный Hitachi CP-EX251N (1), Сист. блок Pen D 945 3.4 DDR 2 1024*2/FDD 3.5/250 Gb/DVD-RW/кл+мышь+коврик (1), Систем.блок CPU Intel Core i7-6700/ASRod Z-170/32Gb/GTX 1070/200Gb/Wi-Fi +клав, (1), Станок сверлильный 350 Вт (1), Универсальная приёмо-передающая платформа для проектирования СВЧ-систем компл.мг (1), Усилитель LZY-22 (1), Усилитель ZHL-3A-S (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 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	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. **Заражение компьютерными вирусами может произойти в процессе ...**

работы с файлами  
форматирования дискеты  
выключения компьютера  
печати на принтере

#### 1. **Что необходимо иметь для проверки на вирус жесткого диска?**

защищенную программу  
загрузочную программу  
файл с антивирусной программой  
дискету с антивирусной программой, защищенную от записи

#### 1. **Какая программа не является антивирусной?**

AVP  
Defrag  
Norton Antivirus  
Dr Web

#### 1. **Какие программы не относятся к антивирусным?**

программы-фаги  
программы сканирования  
программы-ревизоры  
программы-детекторы

#### 1. **Как вирус может появиться в компьютере?**

переместиться с гибкого диска  
при решении математической задачи  
при подключении к компьютеру модема

самопроизвольно

1. **Как происходит заражение "почтовым" вирусом?**

при открытии зараженного файла, присланного с письмом по e-mail  
при подключении к почтовому серверу  
при подключении к web-серверу, зараженному "почтовым" вирусом  
при получении с письмом, присланном по e-mail, зараженного файла

1. **Как обнаруживает вирус программа-ревизор?**

контролирует важные функции компьютера и пути возможного заражения  
отслеживает изменения загрузочных секторов дисков  
при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных  
периодически проверяет все имеющиеся на дисках файлы

1. **Компьютерным вирусом является...**

программа проверки и лечения дисков  
любая программа, созданная на языках низкого уровня  
программа, скопированная с плохо отформатированной дискеты  
специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"

1. **Заражению компьютерными вирусами могут подвергнуться...**

графические файлы  
программы и документы  
звуковые файлы  
видеофайлы

1. **Какие из перечисленных типов не относятся к категории вирусов?**

загрузочные вирусы  
type - вирусы  
сетевые вирусы  
файловые вирусы

Перечень вопросов для проведения промежуточной аттестации

1. Понятие модели угроз. Классификация моделей угроз.

2. Вредоносная программа: правовая квалификация.

3. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?

4. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.

5. Какие вирусы называются резидентными и в чем особенность таких вирусов?
6. Каковы отличия вирусов-репликаторов, стелс-вирусов, мутантов и «троянских» программ?
7. Опишите схему функционирования загрузочного вируса.
8. Опишите схему функционирования файлового вируса.
9. Опишите схему функционирования загрузочно-файловых вирусов.
10. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?
11. Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов.
12. Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?
13. Каковы пути проникновения вирусов в компьютер и признаки заражения компьютера вирусом?
14. Каковы способы обнаружения вирусов и антивирусной профилактики?
15. Перечислите основные меры по защите от компьютерных вирусов.
16. Опишите назначение антивирусных программ различных типов.
17. Назовите примеры современных антивирусных программ и опишите их особенности.