Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:54
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании Ученого совета
Высшей школы интеллектуальных систем и кибертехнологий

Протокол от «23» _05_ 2025 № 10

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации
по дисциплине

Б1.В.ДВ.02.2 «Компьютерная вирусология»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**
бакалавриата, специалитета, магистратуры

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»
наименование образовательной программы

10.03.01 «Информационная безопасность»
шифр, наименование направления подготовки / специальности

Составитель Мунирова Ю.С.,
старший преподаватель Высшей школы интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2025

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа
ПК-4.	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах	ИПК-4.1. Применяет программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем

В результате изучения дисциплины обучающийся должен:

Знает:

– принципы функционирования и классификацию компьютерных вирусов и иного вредоносного программного обеспечения; требования нормативных и методических документов ФСТЭК России в области антивирусной защиты

– принципы работы и архитектуру антивирусных средств защиты автоматизированных систем; методы анализа вредоносного программного кода

Умеет:

– применять технологии, методы и средства защиты информации ограниченного доступа от воздействия вредоносного программного обеспечения

– осуществлять конфигурирование параметров антивирусных средств защиты автоматизированных систем

Владеет:

– навыками организации защиты информации ограниченного доступа от вредоносного программного обеспечения в соответствии с действующими нормативными требованиями

– навыками применения средств анализа и нейтрализации вредоносного программного обеспечения

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Тема 1. ИСТОРИЯ И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ	ОПК-6
	ТЕМА 2. ЖИЗНЕННЫЙ ЦИКЛ КОМПЬЮТЕРНОГО ВИРУСА	ОПК-6
	ТЕМА 3. ФАЙЛОВЫЕ И ЗАГРУЗОЧНЫЕ ВИРУСЫ	ОПК-6
	ТЕМА 4. МАКРОВИРУСЫ, СКРИПТОВЫЕ ВИРУСЫ И СЕТЕВЫЕ ЧЕРВИ	ПК-4
	ТЕМА 5. ТРОЯНСКИЕ ПРОГРАММЫ И ПРОГРАММЫ-ШИФРОВАЛЬЩИКИ	ПК-4
	ТЕМА 6. МЕТОДЫ АНАЛИЗА ВРЕДОНОСНОГО ПРОГРАММНОГО КОДА	ПК-4
	ТЕМА 7. ПОЛИМОРФНЫЕ И МЕТАМОРФНЫЕ ВИРУСЫ	ОПК-6
	ТЕМА 8. АРХИТЕКТУРА АНТИВИРУСНЫХ СРЕДСТВ И ОРГАНИЗАЦИЯ ЛАБОРАТОРНОГО АНАЛИЗА	ПК-4

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра
Форма промежуточной аттестации - зачет.

Шкала оценки уровня сформированности компетенций		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 балльная шкала, %	100 балльная шкала, %	недифференцированная оценка
Допороговый	ниже 61	ниже 61	не зачтено
Пороговый	61-85,9	61-69,9	зачтено
		70-85,9	зачтено
Повышенный	86-100	86-100	зачтено

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения зачета осуществляется итоговый контроль и оценка результатов освоения компетенций.

Перечень вопросов для подготовки к зачету

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1. История развития компьютерных вирусов и вредоносного программного обеспечения.
2. Классификация компьютерных вирусов по среде обитания, способу заражения, деструктивным возможностям.
3. Нормативные и методические документы, регламентирующие защиту от вредоносного программного обеспечения.
4. Жизненный цикл компьютерного вируса: фазы заражения, инкубации, активации, проявления.
5. Файловые вирусы: принципы функционирования и заражения исполняемых файлов.
6. Загрузочные вирусы и буткиты: принципы функционирования.
7. Макровирусы и скриптовые вирусы: особенности распространения.
8. Организация защиты информации ограниченного доступа от вредоносного программного обеспечения.
9. Полиморфные и метаморфные вирусы: методы противодействия обнаружению.
10. Отчетность и документирование инцидентов, связанных с вредоносным программным обеспечением.

ПК-4. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах

1. Сетевые черви: механизмы распространения и заражения.
2. Троянские программы и бэкдоры: назначение и принципы функционирования.
3. Программы-шифровальщики (ransomware): принципы функционирования и методы противодействия.
4. Методы статического анализа вредоносного программного кода.
5. Методы динамического анализа вредоносного программного кода (запуск в изолированной среде).
6. Архитектура и принципы работы антивирусных средств защиты.
7. Конфигурирование параметров антивирусных средств защиты автоматизированных систем.
8. Методы нейтрализации и удаления вредоносного программного обеспечения.
9. Технологии обнаружения неизвестных ранее образцов вредоносного ПО (эвристический, поведенческий анализ).
10. Организация лабораторного анализа образцов вредоносного программного обеспечения.