Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:53
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

«Защита программного обеспечения»
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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знает основные характеристики, достоинства и недостатки средств криптографической и технической защиты информации в автоматизированных системах ИОПК-9.2. Применяет средства криптографической и технической защиты информации от «утечки»
ПК-1.	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации

В результате изучения дисциплины обучающийся должен:

Знает:

– основные характеристики, достоинства и недостатки средств криптографической и технической защиты программного обеспечения

– порядок установки, настройки и обслуживания средств защиты программного обеспечения в соответствии с технической документацией

Умеет:

– применять средства криптографической защиты программного обеспечения от несанкционированного доступа и модификации

– устанавливать и настраивать средства защиты программного обеспечения с соблюдением требований по защите информации

Владеет:

– навыками применения средств криптографической и технической защиты программного обеспечения

– навыками обслуживания программных и программно-аппаратных средств защиты программного обеспечения

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Тема 1. **УГРОЗЫ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (3 СЕМЕСТР)**	ОПК-9
	ТЕМА 2. **ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (3 СЕМЕСТР)**	ОПК-9
	ТЕМА 3. **ЗАЩИТА ПО ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ И МОДИФИКАЦИИ (3 СЕМЕСТР)**	ОПК-9
	ТЕМА 4. **КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (3 СЕМЕСТР)**	ОПК-9
	ТЕМА 5. **БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (4 СЕМЕСТР)**	ПК-1
	ТЕМА 6. **СТАТИЧЕСКИЙ И ДИНАМИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ПО (4 СЕМЕСТР)**	ПК-1
	ТЕМА 7. **УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (4 СЕМЕСТР)**	ПК-1
	ТЕМА 8. **УСТАНОВКА, НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ ЗАЩИТЫ ПО (4 СЕМЕСТР)**	ПК-1

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение двух семестров.
Форма промежуточной аттестации – зачет/экзамен.

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-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Средства защиты программного обеспечения от статического и динамического анализа.
2. Технологии обфускации программного кода.
3. Средства электронной подписи программного обеспечения.
4. Защита программного обеспечения от отладки и трассировки.

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

1. Уязвимости программного обеспечения: классификация и методы устранения.
2. Средства контроля целостности программного обеспечения.
3. Порядок сертификации средств защиты информации, встроенных в программное обеспечение.
4. Особенности защиты программного обеспечения отечественного производства.
5. Обслуживание и сопровождение средств защиты программного обеспечения в процессе эксплуатации.

Перечень вопросов для подготовки к экзамену

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Понятие и виды угроз безопасности программного обеспечения.
2. Классификация вредоносного программного обеспечения.
3. Методы и средства защиты программного обеспечения от несанкционированного копирования.
4. Методы и средства защиты программного обеспечения от несанкционированной модификации.
5. Криптографические методы защиты программного обеспечения.
6. Аппаратные средства защиты программного обеспечения (электронные ключи, токены).

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

1. Порядок установки и настройки средств защиты программного обеспечения в соответствии с технической документацией.
2. Требования безопасной разработки программного обеспечения (Secure Software Development Lifecycle).
3. Методы статического анализа безопасности программного кода.
4. Методы динамического анализа безопасности программного обеспечения.
5. Тестирование программного обеспечения на устойчивость к атакам.