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

«Средства защиты 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» ИОПК-9.3. Применяет технические средства контроля эффективности применяемых мер защиты информации
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

В результате изучения дисциплины обучающийся должен:

Знает:

– основные характеристики, достоинства и недостатки современных средств защиты программного обеспечения; методы контроля эффективности применяемых средств защиты

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

Умеет:

– применять средства криптографической и технической защиты программного обеспечения; оценивать эффективность применяемых средств защиты

– устанавливать и настраивать программные, программно-аппаратные и технические средства защиты программного обеспечения

Владеет:

– навыками применения технических средств контроля эффективности мер защиты программного обеспечения

– навыками обслуживания средств защиты программного обеспечения в процессе эксплуатации

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Тема 1. КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОПК-9
	ТЕМА 2. СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	ОПК-9
	ТЕМА 3. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОПК-9
	ТЕМА 4. КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОПК-9
	ТЕМА 5. АНТИВИРУСНЫЕ СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ПК-1
	ТЕМА 6. СРЕДСТВА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ	ПК-1
	ТЕМА 7. ОБСЛУЖИВАНИЕ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ПК-1
	ТЕМА 8. ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОПК-9 ПК-1

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.
Форма промежуточной аттестации – 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 экзамену

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

1. Классификация средств защиты программного обеспечения.
2. Средства защиты программного обеспечения от несанкционированного доступа (СЗИ от НСД).
3. Криптографические средства защиты программного обеспечения: назначение и характеристики.
4. Средства контроля целостности программного обеспечения.
5. Средства обнаружения и предотвращения вторжений (IDS/IPS) для защиты программного обеспечения.
6. Антивирусные средства защиты программного обеспечения: принципы работы, классификация.
7. Средства защиты программного обеспечения от эксплуатации уязвимостей (EDR, sandboxing).
8. Технические средства контроля эффективности применяемых мер защиты программного обеспечения.
9. Оценка достоинств и недостатков различных классов средств защиты программного обеспечения.
10. Отечественные сертифицированные средства защиты программного обеспечения.

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 средств защиты информации от несанкционированного доступа в соответствии с эксплуатационной документацией.
2. Настройка параметров работы средств защиты программного обеспечения.
3. Порядок обслуживания и сопровождения средств защиты программного обеспечения.
4. Требования к персоналу, осуществляющему эксплуатацию средств защиты программного обеспечения.
5. Порядок обновления баз сигнатур и правил средств защиты программного обеспечения.
6. Настройка политик безопасности средств защиты от несанкционированного доступа.
7. Настройка средств антивирусной защиты программного обеспечения.
8. Настройка систем обнаружения вторжений для защиты программного обеспечения.
9. Контроль работоспособности установленных средств защиты программного обеспечения.
10. Устранение неисправностей средств защиты программного обеспечения в процессе эксплуатации.