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

«Управление антивирусной защитой»
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:

– технологии, методы и средства антивирусной защиты информации ограниченного доступа; требования нормативных и методических документов ФСТЭК России в области антивирусной защиты

– принципы работы и архитектуру программных средств антивирусной защиты автоматизированных систем

Умеет:

– применять технологии, методы и средства антивирусной защиты информации ограниченного доступа в автоматизированных системах

– осуществлять конфигурирование параметров средств антивирусной защиты автоматизированных систем

Владеет:

– навыками организации антивирусной защиты информации ограниченного доступа в соответствии с действующими нормативными требованиями

– навыками установки, настройки и обслуживания средств антивирусной защиты автоматизированных систем

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Тема 1. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК ОБЪЕКТ УПРАВЛЕНИЯ АНТИВИРУСНОЙ ЗАЩИТОЙ	ОПК-6
	ТЕМА 2. ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ	ОПК-6
	ТЕМА 3. АРХИТЕКТУРА И МЕТОДЫ ОБНАРУЖЕНИЯ АНТИВИРУСНЫХ СРЕДСТВ	ПК-4
	ТЕМА 4. УСТАНОВКА И НАСТРОЙКА АНТИВИРУСНОГО СРЕДСТВА ЗАЩИТЫ	ПК-4
	ТЕМА 5. ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ	ПК-4
	ТЕМА 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ, СВЯЗАННЫЕ С ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ	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. Понятие и классификация вредоносного программного обеспечения.
2. Нормативные и методические документы ФСТЭК России, регламентирующие антивирусную защиту.
3. Принципы построения системы антивирусной защиты автоматизированной системы.
4. Требования к антивирусной защите информации ограниченного доступа.
5. Централизованное управление антивирусной защитой в организации.
6. Организация антивирусной защиты автоматизированных рабочих мест.
7. Организация антивирусной защиты серверного оборудования.
8. Порядок реагирования на инциденты, связанные с вредоносным программным обеспечением.
9. Взаимодействие антивирусной защиты с иными подсистемами защиты информации.
10. Отчетность и документирование мероприятий по антивирусной защите.

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

1. Архитектура и компоненты современного антивирусного средства защиты.
2. Методы обнаружения вредоносного программного обеспечения (сигнатурный, эвристический, поведенческий анализ).
3. Порядок установки антивирусного средства защиты на автоматизированное рабочее место.
4. Конфигурирование параметров работы антивирусного средства защиты.
5. Настройка расписания проверок и обновлений антивирусного средства защиты.
6. Настройка политик антивирусной защиты в централизованной системе управления.
7. Мониторинг событий антивирусной защиты и реагирование на обнаруженные угрозы.
8. Устранение неисправностей и сбоев в работе антивирусного средства защиты.
9. Обновление баз сигнатур антивирусного средства защиты.
10. Оценка эффективности функционирования системы антивирусной защиты.