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 Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 06.09.2024 г. № 2

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

«Программно-аппаратные средства защиты информации»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**

«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

Составители Коновалова Анжелика Денисовна, старший преподаватель, Высшая школа интеллектуальных систем и кибертехнологий
Курцев Евгений Александрович, ассистент, Высшая школа 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. 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:

владеть: навыками настройки базовых механизмов криптографической и технической защиты, контроля их состояния и оценки эффективности применяемых мер; навыками администрирования средств защиты, документирования конфигурации, контроля работоспособности и устранения типовых неисправностей.

уметь: выбирать и применять программно-аппаратные средства защиты с учетом угроз, требований к объекту защиты, совместимости и условий эксплуатации; устанавливать средства защиты по технической документации, настраивать параметры работы, выполнять резервирование конфигурации, обновление и диагностику.

знать: назначение, классификацию, основные характеристики, достоинства и ограничения программно-аппаратных, криптографических и технических средств защиты информации; порядок установки, первичной настройки, обслуживания и безопасной эксплуатации программных, программно-аппаратных и технических средств защиты информации.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Архитектура и классификация программно-аппаратных средств защиты информации	ОПК-9 ПК-1
2.	Доверенная загрузка, аппаратные корни доверия и контроль целостности	ОПК-9 ПК-1
3.	Аппаратные средства идентификации, аутентификации и управления доступом	ОПК-9 ПК-1

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
4.	Криптографические программно-аппаратные средства и управление ключами	ОПК-9 ПК-1
5.	Программно-аппаратные средства сетевой защиты	ОПК-9 ПК-1
6.	Средства защиты рабочих станций, серверов и хранилищ данных	ОПК-9 ПК-1
7.	Установка, настройка и техническое обслуживание средств защиты	ОПК-9 ПК-1
8.	Контроль эффективности, диагностика и жизненный цикл средств защиты	ОПК-9 ПК-1

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.
Форма промежуточной аттестации по дисциплине - экзамен.

Шкалы оценки уровня сформированности результатов обучения		**Шкала оценки уровня освоения дисциплины**		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
		70-85,9	«хорошо» / 4	зачтено
повышенный	86-100	86-100	«отлично» / 5	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 лабораторных и практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов и заданий для подготовки к экзамену

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

1. Понятие и назначение программно-аппаратных средств защиты информации.
2. Место программно-аппаратных средств в комплексной системе защиты информации.
3. Классификация средств защиты по назначению и уровню применения.
4. Угрозы, учитываемые при выборе программно-аппаратных средств защиты.
5. Сравнение программных, аппаратных и программно-аппаратных средств защиты.
6. Понятие доверенной вычислительной среды.
7. Назначение аппаратного корня доверия.
8. Функции TPM в системе защиты информации.
9. Принципы безопасной и измеренной загрузки.
10. Методы контроля целостности программной среды.
11. Аппаратные идентификаторы, токены и смарт-карты.
12. Принципы многофакторной аутентификации.
13. Назначение и ограничения биометрических средств аутентификации.
14. Назначение аппаратных модулей безопасности HSM.
15. Аппаратные генераторы случайных чисел и требования к ним.
16. Средства защищенного хранения криптографических ключей.
17. Жизненный цикл ключевой информации.
18. Назначение криптографических шлюзов.
19. Программно-аппаратные межсетевые экраны и их функции.
20. Программно-аппаратные VPN-шлюзы и области их применения.
21. Системы обнаружения и предотвращения вторжений.
22. Средства защиты конечных точек и контроля приложений.
23. Шифрование носителей и защищенное хранение данных.
24. Средства контроля подключаемых устройств и каналов передачи данных.
25. Журналирование событий программно-аппаратных средств защиты.
26. Показатели надежности и отказоустойчивости средств защиты.
27. Влияние средств защиты на производительность информационной системы.
28. Совместимость программно-аппаратных средств с информационной инфраструктурой.
29. Методы контроля эффективности применяемых мер защиты.
30. Критерии выбора программно-аппаратного средства защиты для заданного объекта.

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

1. Этапы жизненного цикла программно-аппаратного средства защиты.
2. Подготовка исходных данных перед установкой средства защиты.
3. Анализ системных требований и совместимости средства защиты.
4. Использование технической и эксплуатационной документации при развертывании.
5. Порядок установки программных компонентов средства защиты.
6. Порядок подключения аппаратных компонентов средства защиты.
7. Первичная настройка учетных записей и ролей администраторов.
8. Принцип минимальных привилегий при администрировании средств защиты.
9. Формирование безопасной базовой конфигурации.
10. Настройка криптографических параметров и ключевого материала.
11. Интеграция средства защиты с сетевой инфраструктурой.
12. Интеграция средства защиты с каталогами пользователей и службами аутентификации.
13. Резервное копирование конфигурации средства защиты.
14. Восстановление конфигурации после сбоя.
15. Управление обновлениями и исправлениями безопасности.
16. Контроль версий программных компонентов и сигнатур.
17. Мониторинг состояния и производительности средства защиты.
18. Анализ журналов и диагностических сообщений.
19. Периодическая проверка работоспособности средства защиты.
20. Диагностика типовых неисправностей программно-аппаратных средств.
21. Действия администратора при отказе средства защиты.
22. Организация отказоустойчивости и резервирования.
23. Управление изменениями конфигурации средств защиты.
24. Инвентаризация и учет программно-аппаратных средств защиты.
25. Требования к защищенному удаленному администрированию.
26. Порядок проведения приемочных испытаний после установки.
27. Документирование настроек и результатов технического обслуживания.
28. Правила безопасной эксплуатации средства защиты пользователями.
29. Вывод средства защиты из эксплуатации.
30. Безопасное удаление ключей, конфигурации и служебных данных при списании.