Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 08:54:23
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»)

Колледж креативных индустрий и предпринимательства

УТВЕРЖДЕНО
на заседании ПЦК

по образовательной программе 09.02.07 Информационные системы и программирование

Протокол от 24.10.2025 г. № 2

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации

по междисциплинарному курсу

учебному предмету, дисциплине, междисциплинарному курсу, профессиональному модулю

«Сертификация информационных систем»

наименование учебного предмета, дисциплины, междисциплинарного курса, профессионального модуля

по образовательной программе среднего профессионального образования –

программе подготовки специалистов среднего звена

программе подготовки специалистов среднего звена / программе подготовки квалифицированных рабочих, служащих

Информационные системы и программирование

наименование образовательной программы

09.02.07 Информационные системы и программирование

шифр, наименование специальности / профессии

Составитель Попов А.К., преподаватель Колледжа креативных индустрий и предпринимательства

ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2025

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ (ДАЛЕЕ – ФОС)

1.1. Планируемые результаты обучения по междисциплинарному курсу

Код компетенции	Наименование компетенции
ПК 7.3	Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов
ПК 7.5	Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации

В результате освоения МДК обучающийся должен:

иметь практический опыт:

-анализа требований к локальным компьютерным сетям и серверному оборудованию для поддержки баз данных и серверов;

- формирование технических заданий и спецификаций на конфигурацию оборудования;

- взаимодействие с поставщиками и техническими специалистами для выбора оптимальных решений;

проведение аудита систем безопасности баз данных и серверов согласно установленным регламентам. выявление уязвимостей и несоответствий требованиям защиты информации. подготовка отчетов и рекомендаций по устранению выявленных недостатков;

-в участии в соадминистрировании серверов;

- в разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;

- в применении законодательства Российской Федерации в области сертификации программных средств информационных технологий;

уметь:

-разрабатывать требования к аппаратному и программному обеспечению сетей и серверов;

- оценивать совместимость и производительность оборудования;

- составлять документацию по конфигурации и настройке сетей и серверного оборудования;

применять регламенты и стандарты по защите информации при проведении аудита;

- анализировать настройки безопасности и выявлять риски;

- формулировать рекомендации для повышения уровня защиты данных и систем;

- проектировать и создавать базы данных;
- выполнять запросы по обработке данных на языке SQL;
- осуществлять основные функции по администрированию баз данных;
- разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;
- владеть технологиями проведения сертификации программного средства;

знать:

-принципы построения локальных сетей и серверных инфраструктур;
- требования к оборудованию для работы баз данных и серверов;
- стандарты и лучшие практики конфигурирования сетей и серверов.
-нормативные документы и регламенты по информационной безопасности;
-методы аудита и оценки безопасности баз данных и серверов;

- принципы защиты информации и обеспечения конфиденциальности;
- модели данных, основные операции и ограничения;
- технологию установки и настройки сервера баз данных;
- требования к безопасности сервера базы данных;
- государственные стандарты и требования к обслуживанию баз данных.

1.2. Содержание междисциплинарного курса

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Защита и сохранность информации баз данных	ПК 7.3, ПК 7.5
2.	Сертификация информационных систем	ПК 7.3, ПК 7.5

1.3. Система оценивания по междисциплинарному курсу

Междисциплинарный курс изучается в течение одного семестра. Форма промежуточной аттестации по дисциплине – контрольная работа.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	недифференцированная оценка
допороговый	ниже 61	ниже 61	не зачтено
пороговый	61-85,9	61-69,9	зачтено
		70-85,9	
повышенный	86-100	86-100	

3. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Вопросы для подготовки к контрольной работе

№	Содержание вопроса
ПК 7.3 Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов	
1.	Требования к конфигурации серверного оборудования при проектировании системы для работы с базами данных
2.	Меры безопасности при конфигурировании сетевой инфраструктуры для защиты данных в базах данных
3.	Роль шифрования данных в базе данных для защиты от несанкционированного доступа и утечек информации
4.	Аутентификация и авторизация для обеспечения безопасности доступа к базам данных в локальной сети
5.	Влияние конфигурации сети на эффективность системы резервного копирования данных в базах данных

№	Содержание вопроса
6.	Механизмы контроля целостности данных при работе с базами данных в локальной сети
7.	Принципы обеспечения доступности и отказоустойчивости баз данных на серверном оборудовании
8.	Требования к конфиденциальности данных в базе данных при настройке серверного оборудования и сети
9.	Оптимизация параметров конфигурации серверов для повышения производительности баз данных при гарантированной безопасности
10.	Типы атак на базу данных, которые могут быть предотвращены через правильно настроенную серверную и сетевую инфраструктуру
11.	Интеграция систем мониторинга и аудита в серверную инфраструктуру для отслеживания и защиты данных в базе данных
12.	Принципы реализации защиты базы данных на уровне операционной системы и серверного оборудования
13.	Этапы сертификации информационных систем для подтверждения их безопасности и соответствия требованиям защиты данных
14.	Использование сертификатов (например, SSL/TLS) для обеспечения защищённости передаваемых данных между серверами баз данных и клиентами
15.	Процесс сертификации серверного оборудования для соответствия стандартам безопасности информационных систем
16.	Требования к безопасности при сертификации систем, обрабатывающих чувствительные данные (например, персональные данные или финансовая информация)
17.	Процесс подписания и проверки кода при сертификации информационных систем и его значимость для защиты баз данных
18.	Аспекты сертификации при внедрении новых технологий или серверного оборудования для работы с базами данных
ПК 7.5 Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации	
19.	Этапы проведения аудита безопасности баз данных и серверных систем
20.	Учет регламентов при аудите систем безопасности баз данных для обеспечения защиты информации
21.	Оценка эффективности механизма контроля доступа в базе данных в рамках аудита безопасности
22.	Методы проверки целостности данных в процессе аудита безопасности баз данных
23.	Роль шифрования данных в базе данных при аудите безопасности
24.	Меры предосторожности для предотвращения утечек конфиденциальной информации при аудите баз данных
25.	Регламентные процедуры при аудите безопасности серверных систем, работающих с базами данных
26.	Оценка соответствия системы резервного копирования и восстановления данных политикам безопасности при аудите
27.	Инструменты мониторинга активности пользователей в базе данных и выявления аномалий в рамках аудита безопасности
28.	Принципы проверки соответствия системы безопасности серверов баз данных внешним стандартам сертификации
29.	Проверка методов аутентификации и авторизации при проведении аудита систем безопасности базы данных
30.	Проверка соблюдения политики безопасности при подключении удаленных пользователей или приложений к базе данных
31.	Аудит использования сертификатов безопасности для защиты данных в процессе передачи между сервером и клиентом
32.	Регламентные действия для проверки наличия уязвимостей в базе данных при проведении аудита безопасности
33.	Шаги для проверки реализации безопасной настройки серверного оборудования при

№	Содержание вопроса
	аудите баз данных
34.	Оценка надежности механизма защиты от SQL-инъекций и других атак на сервер баз данных в процессе аудита
35.	Проверка соответствия системы защиты данных в базе данных требованиям законодательства и международных стандартов безопасности
36.	Оценка рисков, связанных с безопасностью базы данных и серверов, с учетом текущих сертификационных стандартов