

Государственное образовательное учреждение
"Приднестровский государственный университет им. Т.Г. Шевченко"

Физико-технический институт

Кафедра информационных технологий

УТВЕРЖДАЮ

Заведующий кафедрой ИТ

 Ю.А. Столяренко

«_28_» сентября 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

**БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

Направление подготовки

2.09.04.01 Информатика и вычислительная техника

Профиль подготовки

Информационное и программное обеспечение вычислительных систем

Квалификация (степень)

выпускника: **магистр**

Форма обучения: **очная**

Год набора: **2023 г.**

Разработал:

к.т.н., доцент кафедры ИТ,

 /Ю.А. Столяренко

«28» сентября 2024 г.

Тирасполь, 2023

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Кластерные системы» у обучающегося должны быть сформированы следующие компетенции:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения универсальной компетенции
<i>Общепрофессиональные компетенции выпускников и индикаторы их достижения</i>		
	ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	<p>ИД-1_{ОПК-5} Знать современное программное и аппаратное обеспечение информационных и автоматизированных систем</p> <p>ИД-2_{ОПК-5} Уметь модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач;</p> <p>ИД-3_{ОПК-5} Иметь навыки разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач</p>
	ОПК-6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования;	<p>ИД-1_{ОПК-6} Знать: аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности</p> <p>ИД-2_{ОПК-6} Уметь: анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования</p> <p>ИД-3_{ОПК-6} Владеть: навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса</p>

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины их название	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
РУБЕЖНЫЙ КОНТРОЛЬ	Раздел 1 Раздел 2	ОПК-5, ОПК-6	Контрольная работа №1 Лабораторные работы №1-2
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 3 Раздел 4		Контрольная работа №2 Лабораторные работы №3-4
Промежуточная аттестация		Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1		ОПК-5, ОПК-6	Экзамен

3. Показатели и критерии оценивания компетенции по этапам формирования, описание шкал оценивания

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	3	4	5
Первый этап	ИД-1 _{ОПК-5} Знать современное программное и аппаратное обеспечение информационных и автоматизированных систем	Не знает	Знает принципы работы современного аппаратного обеспечения	Знает современное программное и аппаратное обеспечение	Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем
Второй этап	ИД-2 _{ОПК-5} Уметь модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач	Не умеет	Умеет модернизировать программное обеспечение	Умеет модернизировать программное и аппаратное обеспечение	Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач
Третий этап	ИД-3 _{ОПК-5} Иметь навыки разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	Не владеет	Имеет навыки разработки программного обеспечения	Имеет навыки разработки программного и аппаратного обеспечения	Имеет навыки разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач
Первый этап	ИД-1 _{ОПК-6} Знать: аппаратные средства и платформы инфраструктуры информационных технологий,	Не знает	Знает аппаратные средства	Знает аппаратные средства и платформы	Знает аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение,

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	3	4	5
	виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности				архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности
Второй этап	ИД-2опк-6 Уметь: анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования	Не умеет	Умеет анализировать техническое задание	Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код	Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования
Третий этап	ИД-3опк-6 Владеть: навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса	Не владеет	Владеет навыками составления технической документации	Владеет навыками составления технической документации по использованию АПК	Владеет навыками составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса

4. Шкала оценивания

Согласно Положению «О порядке организации аттестации в ИТИ ПГУ им. Т.Г. Шевченко, итоговая оценка представляет собой сумму баллов, полученных студентом по итогу освоения дисциплины (модуля):

Оценка в традиционной шкале	Оценка в 100-балльной шкале	Буквенные эквиваленты оценок в шкале 3Е (% успешно аттестованных)
5 (отлично)	88–100	А (отлично) – 88-100 баллов
4 (хорошо)	70–87	В (очень хорошо) – 80-87баллов
		С (хорошо) – 70-79 баллов
3 (удовлетворительно)	50–69	Д (удовлетворительно) – 60-69 баллов
		Е (посредственно) – 50-59 баллов
2 (неудовлетворительно)	0–49	Фх – неудовлетворительно, с возможной пересдачей – 21-49 баллов
		Ф – неудовлетворительно, с повторным изучением дисциплины – 0-20 баллов

Расшифровка уровня знаний, соответствующего полученным баллам, дается в таблице, указанной ниже

А	“Отлично” - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.
В	“Очень хорошо” - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.
С	“Хорошо” - теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.
Д	“Удовлетворительно” - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.
Е	“Посредственно” - теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному.
FX	“Условно неудовлетворительно” - теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.
Ф	“Безусловно неудовлетворительно” - теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.

5. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы

5.1 Образец индивидуального задания к лабораторной работе

Тема: Построение отказоустойчивого кластера *Hyper-V*.

Практические задания к лабораторной работе:

1. Выполните описанные выше действия. Проанализируйте результаты.
2. Выполните индивидуальное задание.
3. Ответьте на контрольные вопросы.
4. Подготовьте отчет.

Контрольные вопросы к лабораторной работе:

1. Отказоустойчивые кластеры
2. Расчет времени ожидания обработки запросов на кластере.
3. Оптимизация структуры кластера.
4. Архитектура центров обработки и хранения данных.
5. Кластерная архитектура серверных систем.
6. Организация систем хранения данных для серверов.

5.2 Типовой тест

- Что понимается под информационной безопасностью?
 - а) Надёжное хранение данных на диске
 - б) Устойчивость информации к внешнему вмешательству
 - в) Состояние защищённости информации от несанкционированного доступа, модификации и уничтожения
 - г) Возможность передачи информации по сети

- Какой принцип относится к основным требованиям ИБ?
 - а) Увеличение скорости передачи
 - б) Удобство пользования
 - в) Конфиденциальность
 - г) Количество подключений

- Что означает термин «конфиденциальность»?
 - а) Защита данных от случайного удаления
 - б) Обеспечение доступа к данным только авторизованным пользователям
 - в) Хранение информации в базе данных
 - г) Шифрование трафика

- Что означает термин «целостность» информации?
 - а) Полнота базы данных
 - б) Актуальность данных
 - в) Защита от несанкционированных изменений
 - г) Возможность пересылки

- Что такое доступность информации?
 - а) Возможность продать информацию
 - б) Наличие лицензии
 - в) Возможность получения информации уполномоченными лицами в нужный момент
 - г) Хранение на сервере

- Что такое угроза информационной безопасности?
 - а) Любой физический объект
 - б) Возможность случайной ошибки
 - в) Потенциально возможное действие, способное нанести вред информационным ресурсам
 - г) Антивирусная программа

- Что такое уязвимость?
 - а) Любая вредоносная программа
 - б) Слабое место в системе, которое может быть использовано для атаки
 - в) Брандмауэр
 - г) Метод шифрования

- Какой документ регламентирует защиту государственной тайны в РФ?
 - а) Закон «О полиции»
 - б) Закон «О связи»
 - в) Закон «О государственной тайне»
 - г) Трудовой кодекс

- Какой способ относится к техническим методам защиты информации?
 - а) Политика безопасности
 - б) Аппаратное шифрование

- в) Инструкция пользователя
- г) Юридическая ответственность

• Что такое криптографическая защита информации?

- а) Физическая охрана серверной
- б) Уничтожение информации
- в) Защита информации путём преобразования (шифрования)
- г) Установка паролей

• Какой метод используется при проверке целостности данных?

- а) Кеширование
- б) Хеш-функции
- в) Архивация
- г) Сортировка

• Что такое аутентификация?

- а) Удаление данных
- б) Подтверждение подлинности субъекта
- в) Сканирование сети
- г) Контроль доступа

• Что такое межсетевой экран (Firewall)?

- а) Программа для чтения PDF
- б) Система резервного копирования
- в) Средство фильтрации сетевого трафика
- г) Обновление ОС

• Что означает термин «несанкционированный доступ»?

- а) Правомерное действие администратора
- б) Обновление операционной системы
- в) Доступ к информации без разрешения
- г) Резервное копирование

• Какая модель управления доступом основана на ролях пользователей?

- а) MAC
- б) DAC
- в) RBAC
- г) VLP

• Что такое логирование?

- а) Сжатие данных
- б) Хранение паролей
- в) Регистрация событий и действий в системе
- г) Удаление журналов

• Какой метод относится к организационным мерам защиты?

- а) Установка антивируса
- б) Ограничение прав доступа
- в) Регистрация действий
- г) Инструктаж сотрудников по безопасности

• Что такое фишинг?

- а) Метод взлома серверов

- б) Массовая рассылка рекламы
- в) Мошенничество с целью получения конфиденциальных данных
- г) Метод резервного копирования

• Какой стандарт обеспечивает управление информационной безопасностью?

- а) ISO 9001
- б) ISO 14001
- в) ISO/IEC 27001
- г) ГОСТ 2.301

• Что такое брутфорс-атака?

- а) Атака с использованием социальной инженерии
- б) Подбор пароля путём перебора
- в) Сканирование портов
- г) Блокировка IP-адреса

• Что такое резервное копирование?

- а) Шифрование данных
- б) Создание дубликата данных на случай их утраты
- в) Хранение на флешке
- г) Перенос базы данных

• Что из перечисленного — программное средство защиты?

- а) Сейф
- б) Доступ по отпечатку пальца
- в) Антивирус
- г) Электрозамок

• Что такое IDS?

- а) Протокол шифрования
- б) Система обнаружения вторжений
- в) Тип вредоносной программы
- г) Метод резервного копирования

• Какая функция относится к функциям антивируса?

- а) Монтаж серверного оборудования
- б) Защита документации
- в) Обнаружение и устранение вредоносного ПО
- г) Фильтрация рекламы

• Что из перечисленного является физической мерой защиты?

- а) Аудит
- б) Камеры наблюдения
- в) Пароль
- г) Логирование

• Что такое социальная инженерия?

- а) Математическая модель доступа
- б) Метод инженерного анализа
- в) Психологическое воздействие с целью получения конфиденциальной информации
- г) Шифрование данных

- Что такое DDoS-атака?
 - а) Удалённое обновление программ
 - б) Устранение уязвимостей
 - в) Массовая атака, перегружающая ресурсы сервера
 - г) Защита данных от удаления

- Что входит в состав политики информационной безопасности?
 - а) Инструкция по уборке помещения
 - б) Описание архитектуры сети
 - в) Правила, регламентирующие порядок защиты информации
 - г) Список программ

- Что означает термин «анонимизация»?
 - а) Изъятие информации из оборота
 - б) Шифрование файлов
 - в) Удаление признаков, позволяющих идентифицировать личность
 - г) Массовая рассылка

- Кто несёт ответственность за нарушение информационной безопасности?
 - а) Только сисадмин
 - б) Любой сотрудник, допустивший нарушение
 - в) Только директор
 - г) Только охрана

5.3 Перечень вопросов к экзамену по предмету

1. Понятие информации.
2. Виды и свойства информации
3. Структура информационного процесса
4. Понятие информационной безопасности
5. Информационные опасности и угрозы
6. Принципы обеспечения информационной безопасности
7. Основные определения. Наиболее распространенные угрозы доступности.
8. Основные угрозы целостности. Основные угрозы конфиденциальности
9. Основные понятия критериев оценки доверенных компьютерных систем
10. Классы безопасности критериев оценки доверенных компьютерных систем
11. Политика безопасности. Основные понятия
12. Риски, ущерб
13. Методика расчета рисков для политики безопасности
14. Методика расчета рисков для политики безопасности
15. Современное состояние области информационной безопасности
16. Шифры замены: шифр Цезаря, лозунговый шифр, парный шифр.
17. Шифры замены: шифр Цезаря, лозунговый шифр, парный шифр.

18. Шифры перестановки: шифр перестановки, решетка Кардано, шифр вертикальной
19. перестановки.
20. Сжатие способом кодирования серий (RLE). Алгоритм Хаффмана. Алгоритм Лемпеля-Зива.
21. Код Хэмминга