Государственное образовательное учреждение
«Приднестровский государственный университет им. Т.Г. Шевченко»

Физико-технический институт
Факультет информатики и вычислительной техники

Кафедра информационных технологий

УТВЕРЖДАЮ:
Зав. кафедрой, доцент
Ю.А.Столяренко

«28» августа 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Направление подготовки:
2.09.03.02 Информационные системы и технологии

Профиль подготовки:
Защита информации в информационных системах

квалификация
Бакалавр

Форма обучения
Очная

ГОД НАБОРА 2023

Разработал:
к.т.н., доцент кафедры ИТ
/Т.Д.Бордя/
«28» августа 2023 г..

Тирасполь, 2023

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Теоретические основы компьютерной безопасности» у обучающихся должны быть сформированы следующие компетенции:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения универсальной компетенции
Общепрофессиональные компетенции и индикаторы их достижения		
	ОПК-1. Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте;	ИД-1$_{ОПК-1}$ Знать: математические, естественнонаучные, социально-экономические методы для решения нестандартных задач
		ИД-2$_{ОПК-1}$ Уметь: обосновывать выбор современных математических, естественнонаучных, социально-экономических методов для решения нестандартных задач
		ИД-3$_{ОПК-1}$ Иметь навыки: разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникацион-ных и интеллектуальных технологий, нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
	ОПК-7. Способен разрабатывать и применять математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений;	ИД-1$_{ОПК-7}$ Знать: математические модели процессов и объектов для решения задач
		ИД-2$_{ОПК-7}$ Уметь: обосновывать выбор математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений
		ИД-3$_{ОПК-7}$ Иметь навыки: разработки распределенных информационных систем и систем поддержки принятия решений

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины и их наименование	Код контролируемой компетенции (или её части)	Наименование оценочного средства

1	Раздел 1. Основные положения теории компьютерной безопасности	ОПК-1, ОПК-7	Тест, ЛР1
2	Раздел 2 Модели безопасности компьютерных систем	ОПК-1, ОПК-7	Тест, ЛР2-12
3	Раздел 3 Методы анализа и оценки защищенности компьютерных систем	ОПК-1, ОПК-7	Тест, ЛР13
Промежуточная аттестация		Код контролируемой компетенции (или её части)	Наименование оценочного средства
Экзамен		ОПК-1, ОПК-7	Тест

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	**Знать** ОПК-1	Не знает математические, естественнонаучные, социально-экономические методы для решения нестандартных задач	Знает математические, естественнонаучные, социально-экономические методы, но не знает способы решения задач	Знает математические, естественнонаучные, социально-экономические методы, но не может применять знания при решении всех типов задач	Знает математические, естественнонаучные, социально-экономические методы. Умеет применять методики всех типов задач
Второй этап	**Уметь** ОПК-1	Не умеет обосновывать выбор современных математических, естественнонаучных, социально-экономических методов	Умеет правильно обосновывать выбор современных математических, естественнонаучных, социально-экономических методов, но не умеет	Умеет обосновывать выбор современных математических, естественнонаучных, социально-экономических методов, но не умеет обрабатывать	Умеет обосновывать выбор современных математических, естественнонаучных, социально-экономических методов, оформлять и обрабатывать результаты расчетов

			применять методики их решения	результаты решения	
Третий этап	**Владеть** ОПК-1	Не владеет методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий	Владеет разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, но не владеет порядком оформления последовательности решения	Владеет методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, но делает ошибки при обработки результатов решения	Владеет методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, грамотно составляет последовательность решения задач и обрабатывает их результаты
Первый этап	**Знать** ОПК-7	Не знает математические модели процессов и объектов	Знает математические модели процессов и объектов, но не знает способы решения задач	Знает математические модели процессов и объектов, но не может применять знания при решении всех типов задач	Знает математические модели процессов и объектов. Умеет применять методики всех типов задач
Второй этап	**Уметь** ОПК-7	Не умеет обосновывать выбор математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем под-	Умеет правильно обосновывать выбор математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и си-	Умеет обосновывать выбор математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений, но не	Умеет обосновывать выбор математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений, оформлять и обрабатывать результаты расчетов

		держки принятия решений	стем поддержки принятия решений, но не умеет применять методики их решения	умеет обрабатывать результаты решения	
Третий этап	**Владеть** ОПК-7	Не владеет навыками разработки распределенных информационных систем и систем поддержки принятия решений	Владеет навыками разработки распределенных информационных систем и систем поддержки принятия решений, но не владеет порядком оформления последовательности решения	Владеет навыками разработки распределенных информационных систем и систем поддержки принятия решений, но делает ошибки при обработки результатов решения	Владеет навыками разработки распределенных информационных систем и систем поддержки принятия решений, грамотно составляет последовательность решения задач и обрабатывает их результаты

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 ЗЕ (% успешно аттестованных)
5 (отлично)	88–100	A (отлично) – 88-100 баллов
4 (хорошо)	70–87	B (очень хорошо) – 80-87баллов
		C (хорошо) – 70-79 баллов
3 (удовлетворительно)	50–69	D(удовлетворительно) – 60-69 баллов
		E(посредственно) – 50-59 баллов
2 (неудовлетворительно)	0–49	Fx– неудовлетворительно, с возможной пересдачей – 21-49 баллов
		F– неудовлетворительно, с повторным изучением дисциплины – 0-20 баллов

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

A	“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.
B	“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.
C	“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.
D	“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.
E	“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.
F	“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

Лабораторная работа №1

Пример задания

Основные положения теории компьютерной безопасности

Сформулировать основные положения теории компьютерной безопасности

Критерии оценки практической работы №1

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №1 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №2

Пример задания

Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона

Дать общую характеристику моделей дискреционного доступа. Сформировать пятимерное пространство Хартсона

Критерии оценки практической работы №2

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №2 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №3

Пример задания

Методы анализа и методика экспертного оценивания угроз безопасности

Модель Харрисона-Рузо-Ульмана (HRU)

Построить сценарий атаки в том случае, когда доверенный пользователь s1 в исходном состоянии имеет на каталог o2 только права чтения r. Отобразите соответствующие последовательности команд перехода и изменений матрицы доступа.

Критерии оценки практической работы №3

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №3 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №4

Пример задания

Модели TAM

Построить по команде α граф отношений наследственности

Критерии оценки практического задания №4

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №4 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №5.

Пример задания

Модели TAKE-GRANT

Построить систему команд перехода передачи субъекту *x* прав доступа α на объект *s* от субъекта *y*.

Критерии оценки практического задания №5.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №5 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №6.

Пример задания

Расширенная модель TAKE-GRANT

Построить систему команд перехода передачи субъекту *x* прав доступа α на объект *s* от субъекта *y*.

Критерии оценки практического задания №6.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №6 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №7.

Пример задания

Модели Белла-ЛаПадуллы

Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа $\boldsymbol{A}[\boldsymbol{u,o}]$.

Критерии оценки практического задания №7.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №7 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №8.

Пример задания

Модели тематического разграничения доступа на основе иерархических рубрикаторов

Определить отношения доминирования (уже, шире, несравнимо) между мультирубриками

Критерии оценки практического задания №8.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5

№ п\п	Параметры КОС	Баллы
	Итоговое количество баллов	**5**

Лабораторная работа №8 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №9.

Пример задания

Модели ролевого доступа при иерархически организованной системе ролей

Определить тип наделения ролей полномочиями (листовой таксономический, листовой нетаксономический, иерархически охватный).

Критерии оценки практического задания №9.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №9 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №9.

Пример задания

Модель ролевого доступа при иерархически организованной системе ролей

Составить матрицу смежности объектов доступа H (строка – куда; столбец – кто входит; диагональные элементы равны 0) и матрицу итоговой достижимости HS (за один шаг, за два шага и т.д.).

Критерии оценки практического задания №9.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №9 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №10.

Пример задания

Модель анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа

Составить матрицу смежности объектов доступа H (строка – куда; столбец – кто входит; диагональные элементы равны 0) и матрицу итоговой достижимости HS (за один шаг, за два шага и т.д.).

Критерии оценки практического задания №10.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №10 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №11.

Пример задания

Дискреционная модель Кларка-Вильсона

Составить матрицу смежности объектов доступа H (строка – куда; столбец – кто входит; диагональные элементы равны 0) и матрицу итоговой достижимости HS (за один шаг, за два шага и т.д.).

Критерии оценки практического задания №11.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №11 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №12.

Пример задания

Мандатная модель Кена Биба

Составить матрицу смежности объектов доступа H (строка – куда; столбец – кто входит; диагональные элементы равны 0) и матрицу итоговой достижимости HS (за один шаг, за два шага и т.д.).

Критерии оценки практического задания №12.

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №12 считается выполненной, если набрано от 2,5 баллов и выше.

Лабораторная работа №13

Пример задания

Методы анализа и оценки защищенности компьютерных систем

Сформулировать основные методы анализа и оценки защищенности компьютерных систем

Критерии оценки практической работы №13

№ п\п	Параметры КОС	Баллы
1	Правильный ответ на задание	5
	Итоговое количество баллов	**5**

Лабораторная работа №13 считается выполненной, если набрано от 2,5 баллов и выше.

Типовой вариант теста

Пример теста

Вопрос 1 Защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера чреватых нанесением ущерба называется…

а) защитой информации
б) авторизацией
в) информационной безопасностью
г) безопасным состоянием

Вопрос 2 Как называется комплекс мероприятий направленных на обеспечение информационной безопасности?

а) защитой информации
б) авторизацией
в) информационной безопасностью
г) безопасным состоянием

Вопрос 3 Как называется предоставление доступа пользователю, программе или процессу?

а) авторизация данных
б) авторизация
в) аппаратная защита
г) безопасное состояние

Вопрос 4 Кто отвечает за защиту автоматизированной системы от несанкционированного доступа к информации?

а) пользователь
б) аутентификатор
в) авторизатор
г) администратор защиты

Вопрос 5 Условие, при выполнении которого не один субъект не может получить доступ ни к какому объекту без имеющихся полномочий называется…

а) безопасное состояние
б) криптостойкость
в) активность защиты
г) авторизация

Вопрос 6 Какого вида угроз не существует?

а) программно - аппаратные
б) программно - математические
в) информационные, организационные
г) физические

Вопрос 7 Какая из угроз в организации является наиболее опасной?

а) обиженные сотрудники
б) информационная
в) организационная
г) вирусная

Вопрос 8 Что не относится к компьютерной преступности?

а) подделка компьютерной информации
б) хищение информации
в) распространение вирусов
г) согласованное копирование данных

Вопрос 9 Какой мерой предупреждения компьютерных преступлений не существует в теории ИБ?

а) правовой
б) организационной
в) технической
г) программной

Вопрос 10 В основные сервисы обеспечения безопасности не входит?

а) сканирование информации
б) управление доступом

в) аудит
г) экранирование
Вопрос 11 Биометрические характеристики относятся к средствам…
а) аутентификации
б) идентификации
в) протоколирования
г) аудита
Вопрос 12 Надёжность парольной защиты повышает…
а) использование идентификации
б) использование программных генераторов паролей
в) использование электронного ключа
г) использование сертификата
Вопрос 13 Средство, позволяющее специфировать и контролировать действия субъекта над объектом воздействия называется…
а) контроль
б) аудит
в) управление доступом
г) идентификация
Вопрос 14 При принятия решения о предоставлении доступа, какая информация не анализируется?
а) личная информация
б) атрибуты субъектов
в) идентификатор субъекта
г) внутреннее ограничение сервиса
Вопрос 15 Сбор и накопление информации о событиях происходящих в информационной
системе называется…
а) протоколированием
б) аудитом
в) экранированием
г) криптографией
Вопрос 16 С помощью чего происходит анализ накопленной информации проводимой оперативно?
а) систематизации
б) криптостойкости
в) экранирования
г) аудита
Вопрос 17 Как называется средства обеспечения конфиденциальности и контроля целостности информации?
а) криптография
б) криптостойкость
в) криптозависимость
г) криптоанализ
Вопрос 18 Сколько ключей используется в методе симметричного шифрования?
а) 4
б) 2
в) 3
г) 1
Вопрос 19 Сколько ключей используется в методе асимметричного шифрования?
а) 2
б) 4
в) 6

г) 8

Вопрос 20 Предполагает ли эффективное шифрование сообщений использование своего ключа который генерируется для каждого сообщения?

а) только в симметричном методе шифрования

б) если имеется единый ключ

в) не во всех случаях

г) всегда

Вопрос 21 Какое средство контролирует информационные потоки между двумя множествами систем?

а) экран

б) скремблер

в) составной ключ

г) байт код

Вопрос 22 Какого классификационного признака вирусов не существует?

а) по среде обитания

б) по способу заражения среды обитания

в) по воздействию

г) по степени обновления

Вопрос 23 Какой группы вирусов не существует?

а) загрузочные

б) файловые

в) системные

г) файлово - загрузочные

Вопрос 24 Какого класса антивирусного программного обеспечения не существует?

а) программы - детекторы

б) программы - фаги

в) программы - фильтры

г) программы - боты

Вопрос 25 Какой из типов вирусов наиболее опасен?

а) полиморфный

б) загрузочный

в) файловый

г) файлово - загрузочный

Вопрос 26 Что не относится к основополагающим документам в области информационной безопасности?

а) Концепция о криптостойкости систем

б) Оранжевая книга

в) Рекомендации Х.800

г) Концепция защиты от несанкционированного доступа Гостехкомиссии при Президенте РФ

Вопрос 27 Как называется набор законов, правил и норм поведения, определяющих как организация обрабатывает, защищает и распространяет информацию?

а) эффективность защиты

б) политика безопасности

в) гарантированность

г) гармонизированность безопасности

Вопрос 28 Что не входит в аспекты информационной безопасности?

а) доступность

б) целостность

в) стойкость

г) конфиденциальность

Вопрос 29 Какой аспект не затрагивает гарантированность корректности?

а) детализацию
б) процесс разработки
в) среду разработки
г) эксплуатационную документацию

Вопрос 30 Сколько существует уровней корректности в гарантированности корректности?

а) 2
б) 4
в) 6
г) 8

Вопросы к экзамену по дисциплине

1. Понятия "информационная безопасность" и компьютерная безопасность. Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.
2. Общие принципы обеспечения компьютерной безопасности. Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации
3. Методы и механизмы общеархитектурного характера
4. Методы и механизмы инфраструктурного характера
5. Методы и механизмы обеспечивающего (профилактирующего) характера
6. Понятие угрозы. Угрозы безопасности информации в компьютерных системах.
7. Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация".
8. Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации
9. Идентификация и спецификация (описание) угроз Общая схема оценивания угроз
10. Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Составляющие модели безопасности
11. Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.
12. Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы.
13. Основные типы политик безопасности Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств). Модель и теоремы гарантирования безопасности (по Щербакову). Изолированная программная среда.
14. Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект.
15. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.
16. Модели разграничения доступа на основе матрицы доступа.
17. Модель распространения прав доступа Харисона-Руззо-Ульмана.
18. Теоретико-графовая модель TAKE-GRANT
19. Общая характеристика политики мандатного (полномочного) доступа.
20. Модель безопасности Белла-ЛаПадулы.
21. Общая характеристика политики тематического доступа

22. Общая характеристика политики ролевого (типизованного) доступа.
23. Системы с иерархической организацией ролей
24. Модель индивидуально-группового доступа.
25. MMS-модель (military message system) Лендвера-МакЛина
26. Понятие и общая характеристика скрытых каналов утечки информации.
27. Автоматная модель информационного невлияния Гогена-Мессигера.
28. Мандатная модель К.Биба. Уровни целостности данных.
29. Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.
30. Оперативное сохранение (журнализация) изменений данных.
31. Модель безопасности Варахаратжана. Фазы доступа.
32. Многомерное оценивание сложных объектов и его целевые разновидности
33. Оценка защищенности (безопасности) компьютерных систем
34. Теоретико-графовая модель систем защиты с полным перекрытием [угроз] на основе двудольного графа "Угрозы-Объекты". Модель Клементса.
35. Проблемы проектирования (синтеза) и анализа систем индивидуально-группового доступа.