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

Б1.О.09 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

на 2023/2024 учебный год

Направление

2.09.04.02 Информационные системы и технологии

Профиль
Защита информации в информационных системах

Квалификация
магистр

Форма обучения
очная, заочная

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 «Криптографические методы защиты информации» 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 и социально-экономические методы для использования в профессиональной деятельности
		ИД-2$_{ОПК-1}$ Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний
		ИД-3$_{ОПК-1}$ Иметь навыки: теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте

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. Криптосистемы с открытым ключом	ОПК-1	ЛР1,2
2	Раздел 2. Методы взлома шифров, основанных на дискретном логарифмировании.	ОПК-1	ЛР 3,4
3	Раздел 3. Цифровая подпись.	ОПК-1	ЛР 5,6
4	Раздел 4. Криптографические протоколы	ОПК-1	ЛР 7,8
5	Раздел 5. Криптосистемы на эллиптиче-	ОПК-1	ЛР 9,10

	ских кривых. Теоретическая стойкость криптосистем		
6	Раздел 6. Современные шифры с секретным ключом Случайные числа в криптографии.	ОПК-1	ЛР 11,12
Промежуточная аттестация		Код контролируемой компетенции (или её части)	Наименование оценочного средства
Зачет		ОПК-1	ЛР 1-12

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 и социально-экономические методы для использования в профессиональной деятельности	Знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности но не знает способы решения задач	Знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности, но не может применять знания при решении всех типов задач	Знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности
Второй этап	**Уметь** ОПК-1	Не умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в	Умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в	Умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с	Умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естествен-

		междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний	междисциплинарном контексте, с применением математических, естественнонаучных социально-экономических и профессиональных знаний, но не умеет применять методики их решения	применением математических, естественнонаучных социально-экономических и профессиональных знаний, но не умеет обрабатывать результаты решения	нонаучных социально-экономических и профессиональных знаний
Третий этап	**Владеть** ОПК-1	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте, но не владеет порядком оформления последовательности решения	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте, но делает ошибки при обработки результатов решения	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте
Первый этап	**Знать** ПК-7	Не знает способы определения структуры сети и потоков информации, устанавления и руководства установкой сетевого	Знает способы определения структуры сети и потоков информации, устанавления и руководства установкой сетевого	Знает способы определения структуры сети и потоков информации, устанавления и руководства установкой сетевого программного	Знает способы определения структуры сети и потоков информации, устанавления и руководства установкой сетевого программного обеспечения

		программного обеспечения	программного обеспечения , но не знает способы решения задач	обеспечения, но не может применять знания при решении всех типов задач	
Второй этап	**Уметь** ПК-7	Не умеет определять структуру сети и потоки информации, устанавливать и руководить установкой сетевого программного обеспечения	Умеет определять структуру сети и потоки информации, устанавливать и руководить установкой сетевого программного обеспечения, но не умеет применять методики их решения	Умеет определять структуру сети и потоки информации, устанавливать и руководить установкой сетевого программного обеспечения, но не умеет обрабатывать результаты решения	Умеет определять структуру сети и потоки информации, устанавливать и руководить установкой сетевого программного обеспечения
Третий этап	**Владеть** ПК-7	Не владеет навыками определения структуры сети и потоков информации, установления и руководства установкой сетевого программного обеспечения	Владеет навыками определения структуры сети и потоков информации, установления и руководства установкой сетевого программного обеспечения, но не владеет порядком оформления последовательности решения	Владеет навыками определения структуры сети и потоков информации, установления и руководства установкой сетевого программного обеспечения, но делает ошибки при обработки результатов решения	Владеет навыками определения структуры сети и потоков информации, установления и руководства установкой сетевого программного обеспечения

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)
Зачтено 5 (отлично)	88–100	A (отлично) – 88-100 баллов
Зачтено 4 (хорошо)	70–87	B (очень хорошо) – 80-87баллов
		C (хорошо) – 70-79 баллов
Зачтено 3 (удовлетворительно)	50–69	D(удовлетворительно) – 60-69 баллов
		E(посредственно) – 50-59 баллов
Не зачтено 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
Арифметика остатков
Написать программу, реализующую основные алгоритмы арифметики остатков
Критерии оценки лабораторной работы №1

№ п\п	Параметры КОС	Баллы
1	Правильно работающая программа	5
2	Правильный ответ на контрольные вопросы	3
	Итоговое количество баллов	**8**

Лабораторная работа №1 считается выполненной, если набрано от 4 баллов и выше.

ВОПРОСЫ К ЗАЧЕТУ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
"Криптографические методы защиты информации"

1. Арифметика остатков. Группы и кольца. Функция Эйлера. Мультипликативные обратные по модулю N. Конечные поля.
2. Алгоритм Евклида.
3. Быстрые алгоритмы возведения в степень.
4. Односторонние функции. Дискретное логарифмирование.
5. Система Диффи-Хеллмана.
6. Шифр Шамира.
7. Шифр Эль-Гамаля.
8. Шифр RSA.
9. Метод «Шаг младенца, шаг великана».
10. Алгоритм исчисления порядка.
11. Электронная подпись RSA.
12. Электронная подпись на базе шифра Эль-Гамаля.
13. Стандарты на цифровую подпись.
14. Ментальный покер.
15. Доказательства с нулевым знанием.

16. Электронные деньги.
17. Взаимная идентификация с установлением ключа.
18. Математические основы эллиптических кривых.. Выбор параметров кривых.
19. Построение криптосистем на эллиптических кривых.
20. Эффективная реализация операций.
21. Определение количества точек на кривой.
22. Использование стандартных кривых
23. Теория систем с совершенной секретностью. Шифр Вернама.
24. Элементы теории информации. Расстояние единственности шифра с секретным ключом.
25. Идеальные криптосистемы.
26. Современные блоковые и поточные шифры.
27. Криптографические хеш-функции.