### Государственное образовательное учреждение

### "Приднестровский государственный университет им. Т.Г. Шевченко"

### Инженерно-технический институт

## Кафедра информационных технологий и автоматизированного управления производственными процессами

**УТВЕРЖДАЮ** 

Заведующий кафедрой ИТиАУПП

Ю.А. Столяренко

«29» августа 2022 г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ по дисциплине

### Б1.О.09 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

на 2022/2023 учебный год

Направление

2.09.04.02 Информационные системы и технологии

Профиль

Защита информации в информационных системах

Квалификация

магистр

Форма обучения

очная, заочная

2022 ГОД НАБОРА

Разработал:

к.т.н., доцент каф. ИТиАУПП

/ / Т.Д.Бордя /

29 августа 2022

Тирасполь, 2022

# Паспорт фонда оценочных средств по учебной дисциплине

# 1. В результате изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие компетенции:

Категория		Код и наименование	
(группа)	Код и наименование	индикатора достижения	
компетенций		универсальной компетенции	
Оби		етенции и индикаторы их достижения	
	ОПК-1. Способен са-	ИД-1 <sub>ОПК-1</sub>	
	мостоятельно приоб-	Знать: математические, естественнонаучные и	
	ретать, развивать и	социально-экономические методы для исполь-	
	применять математи-	зования в профессиональной деятельности	
	ческие, естественно-	ИД-20ПК-1	
	научные, социально-	Уметь: решать нестандартные профессиональ-	
	экономические и про-	ные задачи, в том числе в новой или незнакомой	
	фессиональные зна-	среде и в междисциплинарном контексте, с при-	
	ния для решения не-	менением математических, естественнонаучных	
	стандартных задач, в	социально-экономических и профессиональных	
	том числе в новой или	знаний	
	незнакомой среде и в	ИД-3 <sub>ОПК-1</sub>	
	междисциплинарном	Иметь навыки: теоретического и эксперимен-	
	контексте;	тального исследования объектов профессио-	
		нальной деятельности, в том числе в новой или	
		незнакомой среде и в междисциплинарном кон-	
		тексте	

# 2. Программа оценивания контролируемой компетенции:

Текущая	Контролируемые мо-	Код контролируе-	Наименование оце-
аттестация	дули, разделы (темы)	мой компетенции	ночного средства
	дисциплины и их наиме-	(или её части)	
	нование		
1	Раздел 1. Криптоси-	ОПК-1	ЛР1,2
	стемы с открытым клю-		
	ЧОМ		
2	Раздел 2. Методы	ОПК-1	ЛР 3,4
	взлома шифров, осно-		
	ванных на дискретном		
	логарифмировании.		
3	Раздел 3. Цифровая под-	ОПК-1	ЛР 5,6
	пись.		
		OFFIC 1	HD 7.0
4	Раздел 4. Криптографи-	ОПК-1	ЛР 7,8
	ческие протоколы		
5	Dec. 5 May 2	ОПК-1	ПР 0 10
3	Раздел 5. Криптоси-	OHK-1	ЛР 9,10
	стемы на эллиптиче-		

	ских кривых. Теорети-		
	ческая стойкость крип-		
	тосистем		
6	Раздел 6. Современные	ОПК-1	ЛР 11,12
	шифры с секретным		
	ключом Случайные		
	числа в криптографии.		
Промежуточная аттестация		Код контролируе-	Наименование оце-
		мой компетенции	ночного средства
		(или её части)	
Зачет		ОПК-1	ЛР 1-12

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

Этапы оцени- вания компе- тенции	Показатели достижения заданного уровня осво-	Критерии оценивания результатов обучения			
Эта ван тен	ения компе- тенции	2	3	4	5
Пер- вый этап	Знать ОПК-1	Не знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	Знает мате- матические, естественно- научные и социально- экономиче- ские методы для исполь- зования в профессио- нальной дея- тельности но не знает спо- собы реше- ния задач	Знает математические, естественно- научные и социально-экономические методы для использования в профессиональной деятельности, но не может применять знания при решении всех типов задач	Знает математические, естественно- научные и соци- ально-экономические методы для использования в профессиональной деятельности
Вто- рой этап	<b>Уметь</b> ОПК-1	Не умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в	Умеет ре- шать нестан- дартные профессио- нальные за- дачи, в том числе в но- вой или не- знакомой 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-

		Межинони	Межинони	примоновичем	пополина у семи
		междисци-	междисци-	применением	нонаучных соци-
		плинарном	плинарном	математиче-	ально-экономиче-
		контексте, с	контексте, с	ских, есте-	ских и профессио-
		примене-	примене-	ственнонауч-	нальных знаний
		нием мате-	нием мате-	ных соци-	
		матических,	матических,	ально-эконо-	
		естественно-	естественно-	мических и	
		научных со-	научных со-	профессио-	
		циально-эко-	циально-эко-	нальных зна-	
		номических	номических	ний, но не	
		и професси-	и професси-	умеет обраба-	
		ональных	ональных	тывать ре-	
		знаний	знаний, но	зультаты ре-	
			не умеет	шения	
			применять		
			методики их		
Тротгей	Риодоли	Цо вто тост	решения	<b>В</b> полож жет	Внаност испутуести
Третий	Владеть ОПК-1	Не владеет	Владеет	Владеет навы-	Владеет навыками
этап	OHK-1	навыками	навыками	ками теорети-	теоретического и
		теоретиче-	теоретиче-	ческого и экс-	эксперименталь- ного исследования
		ского и экс-	ского и экс-	перименталь-	
		перимен-	перимен-	ного исследо-	объектов профес-
		тального ис-	тального ис-	вания объек-	сиональной дея-
		следования объектов	следования объектов	тов професси-	тельности, в том числе в новой или
				ональной дея-	
		профессио-	профессио-	тельности, в	незнакомой среде и
		нальной дея-	нальной дея-	том числе в	в междисципли-
		тельности, в	тельности, в	новой или не-	нарном контексте
		том числе в	том числе в	знакомой	
		новой или	новой или	среде и в	
		незнакомой	незнакомой	междисци-	
		среде и в	среде и в	плинарном	
		междисци-	междисци-	контексте, но	
		плинарном	плинарном	делает	
		контексте	контексте,	ошибки при	
			но не вла-	обработки результатов	
			деет поряд-	* *	
			ком оформ- ления после-	решения	
			довательно-		
Пер-	Знать	Не знает	Знает спо-	Знает спо-	Знает способы
вый	Знать ПК-7	способы	собы опре-	собы опреде-	определения струк-
	1111-7	определения	деления	ления струк-	туры сети и пото-
этап		структуры	структуры	туры сети и	ков информации,
		структуры сети и пото-	структуры сети и пото-	потоков ин-	устанавления и ру-
		ков инфор-	ков инфор-	формации,	ководства установ-
		мации, уста-	мации, уста-	формации, устанавления	ководства установ-
		навления и	навления и	и руководства	граммного обеспе-
		руководства	руководства	установкой	чения
		установкой	установкой	сетевого про-	1011FIA
		сетевого	сетевого	граммного	
		CCICROIO	CCICROIO	т раммного	

Вто-рой этап	Уметь ПК-7	программ- ного обеспе- чения  Не умеет определять структуру сети и по- токи инфор- мации, уста- навливать и руководить установкой сетевого программ- ного обеспе- чения	программ- ного обеспе- чения, но не знает спо- собы реше- ния задач Умеет опре- делять структуру сети и по- токи инфор- мации, уста- навливать и руководить установкой сетевого программ- ного обеспе- чения, но не умеет при- менять мето- дики их ре- шения	обеспечения, но не может применять знания при решении всех типов задач 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	<b>Владеть</b> ПК-7	Не владеет навыками определения структуры сети и потоков информации, устанавления и руководства установкой сетевого программного обеспечения	Владеет навыками определения структуры сети и пото- ков инфор- мации, уста- навления и руководства установкой сетевого программ- ного обеспе- чения, но не владеет по- рядком оформления последова- тельности решения	Владеет навы- ками опреде- ления струк- туры сети и потоков ин- формации, устанавления и руководства установкой сетевого про- граммного обеспечения, но делает ошибки при обработки результатов решения	Владеет навыками определения структуры сети и потоков информации, устанавления 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	Оценка	Буквенные эквиваленты	
в традиционной	в 100-балльной	оценок в шкале ЗЕ	
шкале	шкале	(% успешно аттестованных)	
Зачтено 5 (отлично)	88–100	A (отлично) – 88-100 баллов	
Зачтено 4 (хорошо)	70–87	В (очень хорошо) – 80-87баллов	
Зачтено 4 (хорошо)	70-67	С (хорошо) – 70-79 баллов	
Зачтено 3 (удовле-	50.60	D(удовлетворительно) – 60-69 баллов	
творительно)	50–69	Е(посредственно) – 50-59 баллов	
Не зачтено 2 (неудо-		Fx- неудовлетворительно, с возможной пересдачей – 21-49 баллов	
влетворительно)	0–49	F– неудовлетворительно, с повтор-	
ылстворительно)		ным 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.
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.
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.
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.

"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.