

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
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки
2.09.04.02 Информационные системы и технологии

Профиль подготовки
Защита информации в информационных системах

Квалификация (степень) выпускника:	магистр
Форма обучения:	очная, заочная
Год набора:	2022 г.

Разработал:
преподаватель кафедры ИТиАУПП,



/С.В. Зинченко

«29» августа 2022 г.

Тирасполь, 2022

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Программно-аппаратные средства защиты информации» у обучающегося должны быть сформированы следующие компетенции:

Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
<i>Общепрофессиональные компетенции выпускников и индикаторы их достижения</i>		
-	ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ИД-1 _{ОПК-5} Знать современное программное и аппаратное обеспечение информационных и автоматизированных систем
		ИД-2 _{ОПК-5} Уметь модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач;
		ИД-3 _{ОПК-5} Иметь навыки: разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач

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. Программно-аппаратная защита информации	ОПК-5	Модульный контроль №1 Лабораторная работа №1 Лабораторная работа №2 Лабораторная работа №3
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 2. Несанкционированный доступ Раздел 3. Средства защиты информации Раздел 4. Инфраструктура открытых ключей		Модульный контроль №2 Лабораторная работа №4 Лабораторная работа №5

Промежуточная аттестация	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1	ОПК-5	Зачет

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 современное программное и аппаратное обеспечение информационных и автоматизированных систем, но не знает способы использования в профессиональной деятельности	Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем, но не может выбрать оптимальное применение	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 выбирать программное и аппаратное обеспечение информационных и автоматизированных систем, но не умеет в полной мере модернизировать их для решения профессиональных задач	Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач, но не оптимально осуществляет их применения	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	Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем, но самостоятельно не может применить для решения профессиональных задач	Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач, но допускает незначительные ошибки	Иметь навыки: разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач

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	А (отлично) – 88-100 баллов
4 (хорошо)	70–87	В (очень хорошо) – 80-87 баллов
		С (хорошо) – 70-79 баллов
3 (удовлетворительно)	50–69	Д (удовлетворительно) – 60-69 баллов
		Е (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

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.
F	“Безусловно неудовлетворительно” - теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные за-

дания 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. Примерные вопросы к модульному контролю №1

1. Подсистема управления доступом. Особенности реализации в различных ОС.
2. Подсистема регистрации и учёта событий. Особенности реализации в различных ОС.
3. Криптографическая подсистема. Особенности реализации в различных ОС.
4. Подсистема обеспечения целостности. Особенности реализации в различных ОС.
5. Контрольная сумма CRC.
6. Межсетевые экраны. Определение, назначение, классификация.
7. Архитектура систем активного аудита.
8. Обзор инструментальных средств анализа защищённости АС.
9. Средства защиты информации активного сетевого оборудования.
10. Генерация случайных чисел в ОС Linux.

5.2. Примерные вопросы к модульному контролю №2

11. Атака на переполнение буфера.
12. Принципы построения систем обнаружения вторжений.
13. Сигнатурный анализ как антивирусная техника.
14. Эвристические антивирусные техники.
15. Статические и динамические антивирусные техники.
16. Полиморфизм компьютерных вирусов.
17. Методы защиты от атаки на переполнение буфера.
18. Виртуальные частные сети.
19. Дискреционный контроль доступа.
20. Сравнительный анализ средств защиты информации различных операционных систем.

5.3 Пример лабораторной работы №1

Лабораторная работа №1 «Защита локальной вычислительной сети с помощью межсетевого экрана»

5.4 Пример лабораторной работы №2

Лабораторная работа №2 «Организация защищенной беспроводной компьютерной сети»

5.5 Пример лабораторной работы №3

Лабораторная работа №3 «Исследование возможностей перехвата трафика в компьютерной сети»

5.6 Пример лабораторной работы №4

Лабораторная работа №4 «Защита передаваемых данных с помощью шифрования и электронной цифровой подписи»

5.7 Пример лабораторной работы №5

Лабораторная работа №5 «Работа с защищенными дисками»

5.8. Пример тем курсовых работ.

Курсовые работы не предусмотрены.

5.9. Вопросы к экзамену по дисциплине «**Программно-аппаратные средства защиты информации**»

1. Подсистема управления доступом. Особенности реализации в различных ОС.
2. Подсистема регистрации и учёта событий. Особенности реализации в различных ОС.
3. Криптографическая подсистема. Особенности реализации в различных ОС.
4. Подсистема обеспечения целостности. Особенности реализации в различных ОС.
5. Контрольная сумма CRC.
6. Межсетевые экраны. Определение, назначение, классификация.
7. Архитектура систем активного аудита.
8. Обзор инструментальных средств анализа защищённости АС.
9. Средства защиты информации активного сетевого оборудования.
10. Генерация случайных чисел в ОС Linux.
11. Атака на переполнение буфера.
12. Принципы построения систем обнаружения вторжений.
13. Сигнатурный анализ как антивирусная техника.
14. Эвристические антивирусные техники.
15. Статические и динамические антивирусные техники.
16. Полиморфизм компьютерных вирусов.
17. Методы защиты от атаки на переполнение буфера.
18. Виртуальные частные сети.
19. Дискреционный контроль доступа.
20. Сравнительный анализ средств защиты информации различных операционных систем.