

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

Физико-технический институт

Кафедра информационных технологий

УТВЕРЖДАЮ

Заведующий кафедрой ИТ



Ю.А. Столяренко

«28» августа 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**по дисциплине
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Направление подготовки
09.04.02 Информационные системы и технологии

Профиль подготовки
Защита информации в информационных системах

Квалификация (степень)

выпускника:

магистр

Форма обучения:

очная, заочная

Год набора:

2023 г.

Разработал:

к.т.н., доцент кафедры ИТ,



/Ю.А. Столяренко

«28» августа 2023 г.

Тирасполь, 2023

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Основы информационной безопасности» у обучающегося должны быть сформированы следующие компетенции:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения универсальной компетенции
	ОПК-3. Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ИД-1ОПК-3 Знать принципы, методы и средства анализа и структурирования профессиональной информации
		ИД-2ОПК-3 Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров
		ИД-3ОПК-3 Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями

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. Введение в информационную безопасность Раздел 2. Стандарты и спецификации в области информационной безопасности	ОПК-3	Контрольная работа №1 Лабораторная работа №1 Лабораторная работа №2
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 3. Политика безопасности Раздел 4. Современное состояние в области информационной безопасности		Контрольная работа №2 Лабораторная работа №3 Лабораторная работа №3
Промежуточная аттестация		Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1		ОПК-3	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-3} Знать принципы, методы и средства анализа и структурирования профессиональной информации	Не знает	Знает принципы, методы и средства анализа	Знает принципы, методы и средства анализа и структурирования	Знает принципы, методы и средства анализа и структурирования профессиональной информации
Второй этап	ИД-2 _{ОПК-3} Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров	Не умеет	Умеет анализировать профессиональную информацию	Умеет анализировать профессиональную информацию, выделять в ней главное	Умеет анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров
Третий этап	ИД-3 _{ОПК-3} Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями	Не владеет	Имеет навыки подготовки научных докладов	Иметь навыки подготовки научных докладов, публикаций и аналитических обзоров	Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями

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) – 80-87баллов
		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

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

5.1 Примерные вопросы к контрольной работе №1

1. Понятие информации. Виды, классификация
2. Понятие информационной
3. Безопасности
4. Информационные опасности и угрозы. Основные определения.
5. Наиболее распространенные угрозы доступности.
6. Основные угрозы целостности.
7. Основные угрозы конфиденциальности.
8. Основные понятия критериев оценки доверенных компьютерных систем.
9. Классы безопасности критериев оценки доверенных компьютерных систем.

5.2. Примерные вопросы к контрольной работе №2

1. Политика безопасности. Основные понятия
2. Риски, ущерб.
3. Методика расчета рисков для политики безопасности.
4. Современное состояние области информационной безопасности

5.3 Пример лабораторной работы №1

Лабораторная работа №1. ШИФРЫ ЗАМЕНЫ: ШИФР ЦЕЗАРЯ, ЛОЗУНГОВЫЙ ШИФР, ПАРНЫЙ ШИФР.

Цель: Изучить шифры замены.

Задачи: На примерах научиться производить шифрование и дешифрование текста шифрами замены, указанными в работе алгоритмами.

5.4 Пример лабораторной работы №2

Лабораторная работа №2. ШИФРЫ ПЕРЕСТАНОВКИ: ШИФР ПЕРЕСТАНОВКИ, РЕШЕТКА КАРДАНО, ШИФР ВЕРТИКАЛЬНОЙ ПЕРЕСТАНОВКИ.

Цель: Изучить шифры перестановки.

Задачи: На примерах научиться производить шифрование и дешифрование текста шифрами перестановки, указанными в работе алгоритмами.

5.5 Пример лабораторной работы №3

Лабораторная работа №3. СЖАТИЕ СПОСОБОМ КОДИРОВАНИЯ СЕРИЙ (RLE). АЛГОРИТМ ХАФФМАНА. АЛГОРИТМ ЛЕМПЕЛЯ-ЗИВА.

Цель: Изучить алгоритмы архивации.

Задачи: На примерах научиться производить архивацию текста без указанными в работе алгоритмами.

5.6 Пример лабораторной работы №3

Лабораторная работа №4. КОД ХЭММИНГА.

Цель: Изучить представленный код.

Задачи: На примерах научиться использовать код Хэмминга.

5.7 Вопросы к экзамену по дисциплине «Основы информационной безопасности»

1. Понятие информации. Виды, классификация
2. Понятие информационной
3. Безопасности
4. Информационные опасности и угрозы. Основные определения.
5. Наиболее распространенные угрозы доступности.
6. Основные угрозы целостности.
7. Основные угрозы конфиденциальности.
8. Основные понятия критериев оценки доверенных компьютерных систем.
9. Классы безопасности критериев оценки доверенных компьютерных систем.
10. Политика безопасности. Основные понятия
11. Риски, ущерб.
12. Методика расчета рисков для политики безопасности.
13. Современное состояние области информационной безопасности

- 1. Основная масса угроз информационной безопасности приходится на**
 1. Троянские программы
 2. Черви
 3. Шпионские программы
- 2. Какой вид идентификации и аутентификации получил наибольшее распространение?**
 1. Одноразовые пароли
 2. Постоянные пароли
- 3. Заключительным этапом построения системы защиты является**
 1. Анализ уязвимых мест
 2. Планирование
 3. Сопровождение
- 4. Какие угрозы безопасности информации являются преднамеренными?**
 1. Ошибки персонала
 2. Неавторизованный доступ
 3. Открытие письма, содержащего вирус
- 5. Какой подход к обеспечению безопасности имеет место?**
 1. Комплексный
 2. Теоретический
 3. Логический
- 6. Какие вирусы активизируются в самом начале работы с операционной системой?**
 1. Троянские
 2. Загрузочные
 3. Черви
- 7. Таргетированная атака - ...**
 1. Атака на конкретный компьютер пользователя
 2. Атака на систему крупного предприятия
 3. Атака на сетевое оборудование
- 8. Определите, какие два из перечисленных понятий не относятся к свойствам защищенной информации?**
 1. Адекватность
 2. Целостность
 3. Конфиденциальность
 4. Неисчерпаемость
 5. Доступность
- 9. Что из перечисленного является верным утверждением об "brute force attack"?**
 1. Это вирус, атакующий жесткий диск компьютера
 2. Это один из видов спама
 3. Это попытка злоумышленника подбора пароля до его успешного получения
 4. Это рассылка писем с вирусами
- 10. Какой уровень сетевой модели OSI обеспечивает взаимодействие пользовательских приложений с сетью?**

1. Прикладной уровень
2. Сеансовый уровень
3. Представительный уровень
4. Сетевой уровень
5. Транспортный уровень

11. Какой из перечисленных паролей является наиболее надежным для пользователя admin?

1. password
2. pa\$\$word
3. zpassword
4. passw0rd
5. P@ssw0rd

12. Определите вид атаки по данному рисунку.



1. Ping Flood
2. Cross Site Scripting
3. SQL injection
4. SYN Flood
5. ARP-spoofing

13. Что такое безопасность информации (согласно Руководящего документа "Защита от несанкционированного доступа к информации Термины и определения")?

1. Деятельность по защите систем защиты информации
2. Последовательность действий по созданию защиты информации
3. Управление системой защиты информации
4. Состояние защищенности информации, обрабатываемой средствами ВТ или АС, от внутренних и внешних угроз

14. Что из перечисленного является преднамеренной угрозой безопасности информации?

1. Повреждение кабеля передачи данных в следствии проведения ремонтных работ
2. Несанкционированное копирование информации
3. Ураган
4. Выход из строя оборудования
5. Ошибки в программном обеспечении

15. Какую цель преследует стеганография?

1. Шифрование секретной информации
2. Соккрытие факта наличия секретной информации

3. Установление подлинности авторства секретной информации

16. Какое утверждение о вирусах является неверным?

1. Вирус может создавать копии себя
2. Вирус распространяется через файлы
3. Вирус не влияет на уровень безопасности системы

17. Какие данные являются персональными

1. Фамилия имя
2. Фамилия имя отчество
3. Место рождения
4. Паспортные данные

18. Политика информационной безопасности включает следующие направления системы защиты:

1. Объекты системы, процессы обработки информации, каналы связи, побочные электромагнитные излучения, биологические свойства
2. Хэш-сумма, процессы обработки информации, каналы связи, побочные электромагнитные излучения, управление системой защиты
3. Объекты системы, процессы обработки информации, каналы связи, побочные электромагнитные излучения, управление системой защиты

19. Права доступа к информации (полный перечень)

1. Чтение, копирование, изменение, удаление
2. Чтение, копирование

20. Способ проверки целостности информации

1. Хэш-функция
2. Хэшбраун
3. Хэштег