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

Физико-технический институт
Факультет информатики и вычислительной техники

Кафедра информационных технологий

УТВЕРЖДАЮ

Директор института, доцент
_____ Д.Н. Калошин
«___» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.06 «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

на 2023/2024 учебный год

Направление подготовки
09.04.02 Информационные системы и технологии

Профиль подготовки
Защита информации в информационных системах

Квалификация
магистр

Форма обучения
Очная, заочная

ГОД НАБОРА 2023

Тирасполь 2023 г.

Рабочая программа дисциплины **«Теоретические основы компьютерной безопасности»** разработана в соответствии с требованиями Государственного образовательного стандарта ВО по направлению подготовки **09.04.02 «Информационные системы и технологии»** и основной профессиональной образовательной программы (учебного плана) по профилю подготовки «**Защита информации в информационных системах».**

Составители рабочего программы

Доцент, к.т.н. Т.Д.Бордя

Рабочая программа утверждена на заседании кафедры *информационных технологий*
28 августа 2023 г. протокол № 1

Зав. кафедрой, отвечающий за реализацию дисциплины,
к.т.н., доцент

«28» августа 2023 г. Ю.А. Столяренко

Зав. выпускающей кафедрой,
к.т.н., доцент

«28» августа 2023 г. Ю.А. Столяренко

1. Цели и задачи освоения дисциплины (модуля)

Цели освоения дисциплины «Теоретические основы компьютерной безопасности» - раскрытие основы технических средств, используемых в компьютерной индустрии для защиты информации, теоретические модели защиты информации, их практическое применение в современных компьютерных системах, а также приобретение знаний по техническому обеспечению защиты информации и формирование практических навыков работы.

Задачи освоения дисциплины «Теоретические основы компьютерной безопасности» - обучающие по окончании изучения дисциплины должны получить основы:

– исходных понятий и формализации в сфере компьютерной безопасности;

– представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;

– методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

2. Место дисциплины в структуре ОПОП

Шифр дисциплины в учебном плане – Б1.О.06

Дисциплина относится к обязательной части блока Б1 учебного плана направления 09.04.02 Информационные системы и технологии.

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов

3.Требования к результатам освоения дисциплины (модуля):

Изучение дисциплины направлено на формирование компетенций, приведенных в таблице ниже

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-коммуникационных 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

4.Структура и содержание дисциплины (модуля)

4.1. Распределение трудоемкости в з.е./часах по видам аудиторной и самостоятельной работы студентов по семестрам:

Форма обучения	Семестр (оч.ф), Курс (з.ф)	Трудоемкость, з.е./часы	Количество часов					Форма контроля
			В том числе				Самостоятельная работа (СР)	
			Аудиторных					
			Всего	Лекций (Л)	Практических (ПЗ)	Лабораторных занятий (ЛЗ)		
Очная	1	5/180	180	16	-	32	96	Экзамен (36ч)
	Итого:	5/180	180	16	-	32	96	
Заочная	1	5/180	180	12	-	12	147	Экзамен (9ч)
	Итого:	5/180	180	12	-	12	147	

4.2. Распределение видов учебной работы и их трудоемкости по разделам дисциплины

№ Раздела	Наименование раздела	Количество часов									
		Всего		Аудиторная работа						СР	
				Л		ПЗ		ЛЗ			
		очн.ф	з.ф	очн.ф	з.ф	очн.ф	з.ф	очн.ф	з.ф	очн.ф	з.ф
1	Раздел 1. Основные положения теории компьютерной безопасности	28	33	4	2	-	-	2	2	22	29
2	Раздел 2 Модели безопасности компьютерных систем	90	104	10	8	-	-	26	8	54	88
5	Раздел 3 Методы анализа и оценки защищенности компьютерных систем	26	34	2	2	-	-	4	2	20	30
Всего		144	171	16	12	-	-	32	12	96	147
Контроль		**36**	9	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Итого		**180**	**180**	**16**	**12**	**-**	**-**	**32**	**12**	**96**	**147**

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов		Тема лекций	Учебно-наглядные пособия
		очн.ф	з.ф		
Основные положения теории компьютерной безопасности					
1	1	2	2	Содержание и основные понятия компьютерной безопасности	Презентация
2	1	2		Политика и модели безопасности в компьютерных системах	Презентация
Итого по разделу часов:		**4**	**2**		
Классические модели компьютерной безопасности					
3	2	2	2	Модели безопасности на основе дискреционной и мандатной политики	Презентация
4	2	2	2	Модели безопасности на основе тематической и ролевой политики	Презентация
5	2	2	2	Модели и механизмы обеспечения целостности данных	Презентация
6	2	2	2	Методы и технологии обеспечения доступности (сохранности) данных	Презентация
7	2	2		Политика и модели безопасности в распределенных компьютерных системах	Презентация
Итого по разделу часов:		**10**	**8**		
Методы анализа и оценки защищенности компьютерных систем					

8	3	2	2	Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа	Презентация Презентация
Итого по разделу часов:		**2**	**2**		
ИТОГО:		**16**	**12**		

Практические (семинарские) занятия

Учебным планом не предусмотрены.

Лабораторные занятия

№ п/п	Номер раздела дисциплины	Объем часов		Тема лабораторных занятий	Учебно-наглядные пособия
		Очно	**Заочно**		
Основные положения теории компьютерной безопасности					
1	1	2	2	Основные положения теории компьютерной безопасности	Методические указания
Итого по разделу часов:		**2**	**2**		
Классические модели компьютерной безопасности					
2	2	2	2	Общая характеристика моделей дискреционного доступа.	Методические указания
3	2	2		Пятимерное пространство Хартсона	Методические указания
4	2	2		Модель Харисона-Руззо-Ульмана (HRU-модель)	Методические указания
5	2	2		Модели на основе матрицы доступа	Методические указания
6	2	2		Модель TAKE-GRANT	Методические указания
7	2	2		Расширенная модель TAKE-GRANT	Методические указания
8	2	2	2	Модель Белла-ЛаПадулы	Методические указания
9	2	2		Модель тематического разграничения доступа на основе иерархических рубрикаторов	Методические указания
10	2	2	2	Модель ролевого доступа при иерархически организованной системе ролей	Методические указания
11	2	2		Модель анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа	Методические указания
12	2	2	2	Дискреционная модель Кларка-Вильсона	Методические указания
13	2	2		Мандатная модель Кена Биба	Методические

					указания
Итого по разделу часов:		**24**	**8**		
Методы анализа и оценки защищенности компьютерных систем					
14	3	2	2	Методы анализа и оценки защищенности компьютерных систем	Методические указания
16	3	2		Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости	
Итого по разделу часов:		**4**	**2**		
ИТОГО:		**32**	**12**		

Самостоятельная работа обучающегося по очной форме обучения

Раздел дисциплины	**№ п/п**	**Тема и вид самостоятельной работы обучающегося**	**Трудоемкость (в часах)**
Основные положения теории компьютерной безопасности			
Раздел 1	1	Содержание и основные понятия компьютерной безопасности	6
	2	Угрозы безопасности в компьютерных системах	8
	3	Политика и модели безопасности в компьютерных системах	8
		Итого по разделу часов	**22**
Классические модели компьютерной безопасности			
Раздел 2	1	Модели безопасности на основе дискреционной политики	6
	2	Модели безопасности на основе мандатной политики	6
	3	Модели безопасности на основе тематической политики	6
	4	Модели безопасности на основе ролевой политики	6
	5	Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости	6
	6	Модели и механизмы обеспечения целостности данных	8
	7	Методы и технологии обеспечения доступности (сохранности) данных	8
	8	Политика и модели безопасности в распределенных компьютерных системах	8
		Итого по разделу часов	**54**
Методы анализа и оценки защищенности компьютерных систем			

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
Раздел 3	1	Теоретико-графовые модели комплексной оценки защищенности	10
	2	Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа	10
		Итого по разделу часов	**20**
		ИТОГО:	**96**

Самостоятельная работа обучающегося по заочной форме обучения

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
Основные положения теории компьютерной безопасности			
Раздел 1	1	Содержание и основные понятия компьютерной безопасности	9
	2	Угрозы безопасности в компьютерных системах	10
	3	Политика и модели безопасности в компьютерных системах	10
		Итого по разделу часов	**29**
Классические модели компьютерной безопасности			
Раздел 2	1	Модели безопасности на основе дискреционной политики	10
	2	Модели безопасности на основе мандатной политики	10
	3	Модели безопасности на основе тематической политики	10
	4	Модели безопасности на основе ролевой политики	10
	5	Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости	12
	6	Модели и механизмы обеспечения целостности данных	12
	7	Методы и технологии обеспечения доступности (сохранности) данных	12
	8	Политика и модели безопасности в распределенных компьютерных системах	12
		Итого по разделу часов	**88**
Методы анализа и оценки защищенности компьютерных систем			
Раздел 3	1	Теоретико-графовые модели комплексной оценки защищенности	15

Раздел дисциплины	№ п/п	Тема и вид самостоятельной работы обучающегося	Трудоемкость (в часах)
	2	Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа	15
		Итого по разделу часов	**30**
		ИТОГО:	**147**

Вид занятий: лекция, практическая работа, самостоятельная работа и другие.
Учебно– наглядные пособия: плакат, стенд, карточки с заданиями, раздаточный материал, методическое пособие, методические рекомендации.

5. Примерная тематика курсовых проектов (работ)

Учебным планом не предусмотрены

6. Учебно- методическое и информационное обеспечение дисциплины (модуля)

6.1 Обеспеченность обучающихся учебниками, учебными пособиями

№ п/п	Наименование учебника, учебного пособия	Автор	Год издания	Ко-во экземпляров	Электронная версия	Место Размещения электронной версии
Основная литература						
1	Грушо А. А. Теоретические основы компьютерной безопасности : учеб, пособие для студентов высш. учеб, заведений / А. А. Грушо, Э. А. Применко, Е.Е.Тимонина. — М.: Издательский центр «Академия», 2009. — 272 с.	Грушо А. А.	2009		эл. версия	Кафедра
2	Галатенко В. А. Основы информационной безопасности : учеб. пособие для студентов вузов - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016. - 205 с.	Галатенко В. А.	2016		эл. версия	Кафедра
Дополнительная литература						
3	Шаньгин В.Ф. Защита компьютерной	Шаньгин В.Ф.	2008		эл. версия	Кафедра

№ п/п	Наименование учебника, учебного пособия	Автор	Год издания	Ко-во экземпляров	Электронная версия	Место Размещения электронной версии
	информации. М: ДМК Пресс, 2008.542 с.					
3	Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс. 2012. 592 с.	Шаньгин В.Ф.	2012			
Итого по дисциплине: 0% печатных изданий; 100 % электронных						

6.2. Программное обеспечение и Интернет- ресурсы

Программное обеспечение: *ОС Windows*,

Интернет-ресурсы

1. http://citforum.ru.
2. https://www.intuit.ru.
3. http://www.securitylab.ru.
4. ЭБС IPRbooks: http://www.iprbookshop/ru/
5. Электронно-библиотечная система «Университетская библиотека онлайн»:www.biblioclub.ru
6. Единое окно доступа к образовательным ресурсам. http://window.edu.ru/
7. http://www.microsoft.com/msf
8. http://www.uml.org
9. http://www.wikipedia.org

6.3. Методические указания и материалы по видам занятий

Методические указания к лабораторным работам по дисциплине «Теоретические основы компьютерной безопасности» в электронном варианте**.**

ВОПРОСЫ К ЭКЗАМЕНУ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ "Теоретические основы компьютерной безопасности"

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.

7.Материально- техническое обеспечение дисциплины:

Лаборатория ИТО ИТИ

8. Методические рекомендации по организации изучения дисциплины:

Обучающийся, изучающий дисциплину, должен, с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины обучающийся должен знать основные определения, понятия, основные аспекты программной инженерии.

Успешное освоение курса требует самостоятельной работы обучающихся. В программе курса отведено минимально необходимое время для работы обучающихся над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;

- проработку учебного материала (по конспектам занятий, учебной и научной литературе), подготовку ответов на вопросы, предназначенные для самостоятельного изучения, доказательство отдельных утверждений, свойств, решение задач;

- подготовка к экзамену.

Руководство и контроль над самостоятельной работой обучающихся осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов следует обращаться за консультациями к лектору.

Рабочая учебная программа по дисциплине «Теоретические основы компьютерной безопасности» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО по направлению 09.04.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» и учебного плана по профилю «Защита информации в информационных системах».

9. Технологическая карта дисциплины
Курс 1
Семестр 1
Группа ИТ23ДР68ИС1(очная форма)
Преподаватель – лектор Бордя Т.Д.
Преподаватели, ведущие лабораторные, практические занятия – БордяТ.Д..

Кафедра «Информационные технологии»

Наименование дисциплины/курса	Уровень образования (бакалавриат, специалитет, магистратура)	Статус дисциплины в учебном плане (А, Б)	Количество зачетных единиц
Теоретические основы компьютерной безопасности	магистратура	А	5
СМЕЖНЫЕ ДИСЦИПЛИНЫ ПО УЧЕБНОМУ ПЛАНУ:			
Научно-исследовательская работа, практика			
БАЗОВЫЙ МОДУЛЬ (проверка знаний и умений по дисциплине)			

Тема, задание или мероприятие текущего контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Минимальное количество баллов	Максимальное количество баллов
Лабораторная работа №1	ЛР1	Аудиторная	2,5	5
Лабораторная работа №2	ЛР2	Аудиторная	2,5	5
Лабораторная работа №3	ЛР3	Аудиторная	2,5	5
Лабораторная работа №4	ЛР4	Аудиторная	2,5	5
Лабораторная работа №5	ЛР5	Аудиторная	2,5	5
Лабораторная работа №6	ЛР6	Аудиторная	2,5	5
Лабораторная работа №7	ЛР7	Аудиторная	2,5	5
РУБЕЖНЫЙ КОНТРОЛЬ	**РК**		**17,5**	**35**
Лабораторная работа №8	ЛР8	Аудиторная	2,5	5
Лабораторная работа №9	ЛР9	Аудиторная	2,5	5
Лабораторная работа №10	ЛР10	Аудиторная	2,5	5
Лабораторная работа №11	ЛР11	Аудиторная	2,5	5
Лабораторная работа №12	ЛР12	Аудиторная	2,5	5
Лабораторная работа №13	ЛР13	Аудиторная	2,5	5
Тест1	Т1	Аудиторная	17,5	35
РУБЕЖНАЯ АТТЕСТАЦИЯ	**РА**		**32,5**	**65**
		Итого	**50**	**100**