Государственное образовательное учреждение

«Приднестровский государственный университет им. Т.Г. Шевченко»

Инженерно-технический институт

Кафедра «Информационных технологий и автоматизированного управления производственными процессами»

УТВЕРЖДАЮ:
Директор института, доцент
_____ Ф.Ю. Бурменко
«16» ____09_____ 20 19 г.

РАБОЧАЯ ПРОГРАММА

на 2019/2020 учебный год

УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.28 «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки:
09.03.04 Программная инженерия

Профиль подготовки
Разработка программно-информационных систем

Для набора
2016 года

Квалификация (степень) выпускника
бакалавр

Форма обучения:
очная

Тирасполь, 2019

Рабочая программа дисциплины «Защита информации» /сост. Г.С. Федорченко – Тирасполь: ГОУ ПГУ, 2019. – 11 с.

Рабочая программа предназначена для преподавания обязательной дисциплины вариативного цикла дисциплин (модули) очной формы обучения по направлению подготовки 09.03.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ».

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего образования по направлению подготовки 09.03.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ», утвержденного приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г. №229.

Составитель  Федорченко Г.С.

«30» августа 2019

Цель дисциплины:

Формирование у студентов способности и умения защищать информационные ресурсы от всех возможных угроз информационной безопасности.

Задачи дисциплины:

- получение знаний, связанных с правовыми основами информационной безопасности;
- получение знаний по поддержке работоспособности информационных систем и технологий в заданных функциональных характеристиках;
- получение навыков по обеспечению безопасности и целостности данных.

2. Место дисциплины в структуре ООП ВО

Дисциплина относится к циклу Б1.Б.26, базовая часть, обязательные дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

Для освоения дисциплины необходимы знания, умения, навыки, полученные и сформированные в ходе изучения дисциплин: «Дискретная математика», «Информатика», «Программирование», «Базы данных».

Знания, умения и навыки, приобретенные при изучении данной дисциплины, используются при написании выпускной квалификационной работы и в профессиональной деятельности по профилю «Разработка программно-информационных систем».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций: ПК-4.

Код компетенции	Формулировка компетенции
ПК-4	владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества.

В результате освоения дисциплины обучающийся должен:

3.1. Знать:

- основные понятия информационной безопасности;
- основные способы обеспечения защиты информации;

3.2. Уметь:

- выполнять анализ угроз информационной безопасности для различных информационных систем;
- использовать системы шифрования различного типа;
- использовать и настраивать основные средства защиты сетей;

3.3. Владеть:

- навыками работы с конкретными программными продуктами средств шифрования, аутентификации, сетевой защиты, средствами защиты от несанкционированного доступа, антивирусными программами.

4. Структура и содержание дисциплины (модуля)

Основные понятия и определения Криптографические методы защиты информации

Методы защиты сетей

4.1. Распределение трудоемкости в часах по видам аудиторной и самостоятельной работы студента по семестрам

Семестр	Количество часов							Форма итогового контроля
	Трудоемкость з.е./часы	В том числе						
		Аудиторных				Самост. работа	Контроль	
		Всего	Лекции	Лабораторных занятия	Практических занятий			
7	3/108	108	26	34	-	48		Экзамен
Итого:	3/108	108	26	34	-	48		Экзамен

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

№ п/п	Наименование раздела дисциплины (модуля)	Всего	Аудиторная работа			Внеаудиторная работа СР
			ЛК	ЛР	ПЗ	
1	Введение. Основные виды и источники атак на информацию	22	6	8	-	8
2	Криптография	26	8	8	-	10
3	Сетевая безопасность	18	4	4	-	10
4	ПО и информационная безопасность	22	6	6	-	10
5	Комплексная система безопасности	20	2	8	-	10
6	Экзамен					
	Итого:	108	26	34	-	48

4.3. Тематический план по видам учебной деятельности

Лекции:

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
1	1	2	Современная ситуация в области информационной безопасности	ММП
2	1	2	Категории информационной безопасности	ММП
3	1	2	Обзор наиболее распространенных методов «взлома» паролей	ММП
4	2	2	Классификация криптоалгоритмов	ММП
5	2	2	Симметричные криптоалгоритмы	ММП
6	2	2	Асимметричные криптоалгоритмы	ММП
7	2	2	Криптографические протоколы	ММП
8	3	2	Атакуемые сетевые компоненты	ММП
9	3	2	Уровни сетевых атак согласно модели *OSI (Open System Interconnectoin)*	ММП

10	4	2	Обзор современного ПО	ММП
11	4	2	Ошибки, приводящие к возможности атак на информацию	ММП
12	4	2	Основные положения по разработке ПО	ММП
13	5	2	Политика ролей	ММП
Итого:		26		

Практические (семинарские) занятия: не предусмотрены учебным планом.

Лабораторные работы:

№ п/п	Номер раздела дисциплины	Наименование лабораторных работ	Трудоемкость (часы)
1	1	Шифрование текста	2
2	1	Шифрование текста	2
3	1	Шифрование текста	2
4	1	Шифрование текста	2
5	2	Защита БД	2
6	2	Защита БД	2
7	2	Взлом моноалфавитного подстановочного шифра методом частотной атаки	2
8	2	Взлом моноалфавитного подстановочного шифра методом частотной атаки	2
9	3	Применение ПО в шифровании	2
10	3	Применение ПО в шифровании	2
11	4	Хэш-функция. Формирование цифровой подписи	2
12	4	Хэш-функция. Формирование цифровой подписи	2
13	4	Хэш-функция. Формирование цифровой подписи	2
14	5	Защита конфиденциальной информации в ОС	2
15	5	Защита конфиденциальной информации в ОС	2
16	5	Защита конфиденциальной информации в ОС	2
17	5	Защита конфиденциальной информации в ОС	2
		Итого	**34**

Самостоятельная работа студента

Раздел дисциплины	№ п/п	Тема и вид СРС	Трудоемкость (в часах)
Раздел 1	1	Тема: Введение. Основные виды и источники атак на информацию СРС №1: - работа обучающихся с лекционным материалом и раздаточными материалами, - поиск и анализ литературы и электронных источников информации, - подготовка к лабораторным работам	8
Раздел 2	2	Тема: Криптография СРС №2: - работа обучающихся с лекционным материалом и раздаточными материалами, - поиск и анализ литературы и электронных источников информации, - подготовка к лабораторным работам	10
Раздел 3	3	Тема: Сетевая безопасность СРС №3: - работа обучающихся с лекционным материалом и раздаточными материалами, - поиск и анализ литературы и электронных источников информации,	10

		- подготовка к лабораторным работам	
Раздел 4	4	Тема: ПО и информационная безопасность СРС №4: - работа обучающихся с лекционным материалом и раздаточными материалами, - поиск и анализ литературы и электронных источников информации, - подготовка к лабораторным работам	10
Раздел 5	5	Тема: Комплексная система безопасности СРС №5: - работа обучающихся с лекционным материалом и раздаточными материалами, - поиск и анализ литературы и электронных источников информации, - подготовка к лабораторным работам	10
		Итого	**48**

5. Примерная тематика курсовых проектов (работ): не предусмотрено учебным планом.

6. Образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
8	Л	-информационно-развивающие технологии; -комплексные лекции; -лекция-конференция.	32
	ЛР	-компьютерные технологии обучения.	34
		Итого	**66**

7. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тест для проверки теоретической подготовки студентов

Конфиденциальность – это:

- гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена
- гарантия того, что информация сейчас существует в ее исходном виде
- гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор
- гарантия того, что источником информации является ни кто другой как то лицо, которое заявлено как ее автор.

2. Надежность – это:

- гарантия точного и полного выполнения всех команд;
- гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются;
- гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;
- гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает.

3. Апеллируемость – это:

- гарантия того, что информация сейчас существует в ее исходном виде
- гарантия того, что источником информации является ни кто другой как то лицо, которое заявлено как ее автор
- гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор
- гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена

4. Субъекты и объекты делятся по нескольким уровням доступа – принцип модели:

- Биба
- Гогена-Мезигера
- Сазерлендской
- Кларка-Вильсона

5. Пароль для доступа к терминалу с физическим доступом можно не устанавливать, если:

- к терминалу имеет доступ один человек
- ответственность распространяется на группу лиц
- терминал установлен в публичном месте

6. Достоинства программы перехватчика паролей:

- ее работа не заметна
- может сама передавать результаты работы по сети
- для установки не нужен физический доступ к терминалу

7. Ограниченными криптоалгоритмы называются в случае:

- когда функции алгоритма шифрования ограничены
- когда в тайне содержится сам криптоалгоритм

8. Недостатки симметричных алгоритмов:

- наличие одного ключа для шифрования
- надежность алгоритма шифрования определяется выбором ключа

9. Криптопакет – это:

- криптоалгоритм
- программная реализация криптоалгоритма

10. Случайные последовательности применяются при использовании:

- симметричных криптоалгоритмов
- асимметричных криптоалгоритмов

11. Достоинства симметричных криптоалгоритмов:

- использование двух ключей
- время шифрования

12. При распространении закрытого ключа:

- можно просто выставить его в Internet для всеобщего использования
- необходимо придерживаться определенных правил при его распространении

13. Стегосистема – это:

- совокупность средств и методов, использующихся для формирования скрытого канала передачи информации
- совокупность средств и методов, использующихся для реализации защищенного канала связи

14. В зависимости от характера воздействий, производимых над данными, алгоритмы делятся на:

- перестановочные
- подстановочные
- блочные

15. Длина выходной последовательности после применения хеш-функции зависти от:

- длины входной последовательности
- от самой хеш-функции
- от времени применения

16. Тайнопись это:

17. Используется ли в симметричных криптосистемах ключи сеанса

- да
- нет

Зашифровать свою фамилию следующими шифрами: квадрат Полибия, шифр Цезаря, шифр вертикальной перестановки.

1. Стегосистема – это:

- совокупность средств и методов, использующихся для формирования скрытого канала передачи информации
- совокупность средств и методов, использующихся для реализации защищенного канала связи
- обмен информацией таким образом, что скрывается сам факт существования секретной связи

2. Программа Masker 7.0 может скрывать текстовые файлы в файлы форматов:
    - *.bmp
    - *.wav
    - *.gif
    - *.exe
    - *.mp3
    - *.dll

3. В какой из программ используется контейнер, для передачи засекреченного файла?
    - Masker 7.0
    - S-Tools
    - VipNet Safe Disk

4. Системы селектирующей стеганографии:
    - генерируют один контейнер
    - генерируют несколько контейнеров

- используют контейнер извне

5. Какая из программ использует открытый/закрытый ключ?
   - Masker 7.0
   - S-Tools
   - VipNet Safe Disk
6. В каком из протоколов участник, которому доверяются все остальные участники протокола выступает только при необходимости:
   - самоутверждающийся протокол
   - протокол с судейством
   - протокол с арбитражем

7. Что такое Хеш-функция?

8. Простой или слабой называется хеш-функция которая:
9. Какая из команд в GPG генерирует ключ?
   - [student@lhaos stud]$ gpg --list-keys
   - [student@lhaos stud]$ gpg --gen-key
   - [user@mdk]$ gpg --clearsign -a test.key

10. К шифрам замены относятся:
    - Лозунговый шифр
    - Шифр Цезаря
    - Квадрат Полибия

11. Какие сети относятся к широковещательной категории сетей:
- *TokenRing,*
- *ARP*
- *RIP*
- *EtherNet*

12. В каком из протоколов участник, которому доверяются все остальные участники протокола выступает только при необходимости:
- самоутверждающийся протокол
- протокол с судейством
- протокол с арбитражем

13. Простой или слабой называется хеш-функция которая:

14. Какая из команд в GPG генерирует ключ?
- [student@lhaos stud]$ gpg --list-keys
- [student@lhaos stud]$ gpg --gen-key
- [user@mdk]$ gpg --clearsign -a test.key

15. Защищая любую конфиденциальную информацию:
- всегда нужно пользоваться самыми надежными и передовыми технологиями
- необходимо применять средства защиты в зависимости от уровня конфиденциальности информации

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

8.1. Основная литература

1) Э. Таненбаум, Х. Бос. Современные операционные системы, 4-е издание — СПБ: ИД «Питер», 2015 г.
2) Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 261 с. — (Высшее образование). — ISBN 978-5-534-01678-9.
3) Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. Ун-та, 2009 г.
4) Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб: НИУ ИТМО, 2012 г.

8.2. Дополнительная литература

1) В. Жельников. Криптография от папируса до компьютера. М.: ABF. 2006 г.
2) В. Мельников. Защита информации в компьютерных сетях.- М.: Финансы и статистика. 2001.

8.3. Программное обеспечение и Интернет-ресурсы

ОС Windows, пакет MS Office, средства программирования..

8.4. Методические указания и материалы по видам занятий разрабатываются.

9. Материально-техническое обеспечение дисциплины (модуля):

Учебный кабинет, лаборатория ИТО ИТИ.

10. 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, методики защиты информации.

Успешное освоение курса требует напряженной самостоятельной работы обучающегося. В программе курса отведено минимально необходимое время для работы обучающегося 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;
- подготовку к лабораторным работам;
- оформление отчетов к лабораторным работам;
- подготовку к модульным контролям;
- подготовка к экзамену.

Руководство и контроль за самостоятельной работой обучающегося осуществляется в форме индивидуальных консультаций, защиты лабораторных работ, выполнения модульных контролей.

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 «Защита информации» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО с учетом рекомендаций ПрООП ВО по направлению 09.03.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ» и учебного плана по профилю подготовки «Разработка программно-информационных систем».

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

Курс **4**
Семестр **7**
Группа **ИТ16ДР62ПИ**
Преподаватель – лектор **Федорченко Г.С.**
Преподаватели, ведущие практические занятия – **Федорченко Г.С.**

Кафедра «Информационных технологий и автоматизированного управления производственными процессами»

Наименование дисциплины / курса	Уровень //ступень образования (бакалавриат, специалитет, магистратура)	Статус дисциплины в рабочем учебном плане (А, Б, В, Г)	Количество зачетных единиц / кредитов
Защита информации	бакалавриат	Б	5

Смежные дисциплины по учебному плану:				
Математика, Информатика, Программирование				
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
1-й календарный модульный контроль	Тест, ПЗ	Аудиторная	10	20
Лабораторная работа №1	ЛР	Аудиторная	5	10
Лабораторная работа №2	ЛР	Аудиторная	3	5
Лабораторная работа №3	ЛР	Аудиторная	2	5
РУБЕЖНЫЙ КОНТРОЛЬ	РК	Аудиторная	**20**	**40**
2-ой календарный модульный контроль	Тест, ПЗ	Аудиторная	13	25
Лабораторная работа №4	ЛР	Аудиторная	3	5
Лабораторная работа №5	ЛР	Аудиторная	7	15
Лабораторная работа №6	ЛР	Аудиторная	7	15
РУБЕЖНЫЙ АТТЕСТАЦИЯ	РА	Аудиторная	**30**	**60**
Итого:			**50**	**100**

Составитель, ст. преподаватель Г.С. Федорченко

Рабочая учебная программа рассмотрена методической комиссией инженерно-технического института протокол № 1 от «12» 09 2019 г. и признана соответствующей требованиям Федерального Государственного образовательного стандарта и учебного плана по направлению 09.03.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ».

Председатель МК ИТИ Е.И. Андрианова

Зав. Кафедрой ПОВТ и АС, доцент С.Г. Федорченко