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
«14» 09 2018 г.

РАБОЧАЯ ПРОГРАММА

на 2018/2019 учебный год

УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.21 «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки:
09.03.02 Информационные системы и технологии

Профиль подготовки
Безопасность информационных систем

Для набора
2015 года

Квалификация (степень) выпускника
бакалавр

Форма обучения:
очная

Тирасполь, 2018

Рабочая программа дисциплины «Защита информации» /сост. Г.С. Федорченко – Тирасполь: ГОУ ПГУ, 2018. – 11 с.

Рабочая программа предназначена для преподавания обязательной дисциплины вариативного цикла дисциплин (модули) очной формы обучения по направлению подготовки 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ».

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ», утвержденного приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г. №219.

Составитель _____ ст. преп. Федорченко Г.С.

«01» 09 2018 г.

1. Цели и задачи освоения дисциплины

Настоящая дисциплина посвящена изучению современного состояния проблемы защиты информации. Знания в этой области достаточно востребованы во всех сферах применения персональных ЭВМ, поэтому навыки и знания полученные в процессе изучении данного предмета будут применены при дальнейшем обучении.

Целью преподавания дисциплины является формирование способности и умения защищать информационные ресурсы от всех возможных угроз информационной безопасности.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– понимание сущности и значения информации в развитии современного информационного общества, соблюдении основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

– способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПК-25).

2. Место дисциплины в структуре ООП ВО

Б1.Б.21. Дисциплины (модули). Базовая часть. Обязательные дисциплины. Трудоемкость 5 ЗЕ.

Дисциплина «Защита информации» входит в базовую часть. Для изучения дисциплины необходимы знания курсов «Информатика» и «Программирование».

Изучение дисциплины «Защита информации» является базой для дальнейшего освоения студентами дисциплин, курсов по выбору профессионального цикла, а также для прохождения практики.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-4, ПК-25.

Код компетенции	Формулировка компетенции
ОПК-4	пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны
ПК-25	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований

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)

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			
8	5/180	180	34	16	16	78	36	Экзамен
Итого:	5/180	180	34	16	16	78	36	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	10	6	4	-	
2	Криптография		8	4	16	
3	Сетевая безопасность		6	2	-	
4	ПО и информационная безопасность		6	2	-	
5	Комплексная система безопасности		8	4	-	
6	Экзамен	36				
	Итого:	180	34	16	16	78

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	Абстрактные модели защиты информации	ММП
4	1	2	Обзор наиболее распространенных методов «взлома» паролей	ММП
5	2	2	Классификация криптоалгоритмов	ММП
6	2	2	Симметричные криптоалгоритмы	ММП
7	2	2	Асимметричные криптоалгоритмы	ММП
8	2	2	Другие системы и виды информации	ММП
9	2	2	Криптографические протоколы	ММП
10	3	2	Атакуемые сетевые компоненты	ММП
11	3	2	Уровни сетевых атак согласно модели *OSI (Open System Interconnectoin)*	ММП
		2	Уровни сетевых атак согласно модели *OSI (Open*	ММП

			System Interconnectoin)	
12	4	2	Обзор современного ПО	ММП
13	4	2	Ошибки, приводящие к возможности атак на информацию	ММП
14	4	2	Основные положения по разработке ПО	ММП
		2	Основные положения по разработке ПО	ММП
15	5	2	Классификация информационных объектов	ММП
16	5	2	Политика ролей	ММП
	Итого:	34		

Практические (семинарские) занятия:

№ п/п	Наименование практических работ	Трудоемкость (часы)
1	Алгоритм шифрования Эль-Гамаля	2
	Алгоритм шифрования Эль-Гамаля	2
2	Алгоритм RSA	2
3	Сеть Фейстеля	2
4	Рюкзачные криптосистемы	2
5	Криптосистема Рабина	2
6	**ГОСТ 28147-89**	4
	Итого	**16**

Лабораторные работы:

№ п/п	Наименование раздела дисциплины (модуля)	Наименование лабораторных работ	Трудоемкость (часы)
1	Введение. Основные виды и источники атак на информацию	Шифрование текста	2
		Шифрование текста	2
2	Криптография	Защита БД	2
		Взлом моноалфавитного подстановочного шифра методом частотной атаки	2
3	Сетевая безопасность	Применение ПО в шифровании	2
4	ПО и информационная безопасность	Хэш-функция. Формирование цифровой подписи	2
5	Комплексная система безопасности	Защита конфиденциальной информации в ОС	4
		Защита конфиденциальной информации в ОС	4
		Итого	**16**

Самостоятельная работа студента

Разделы дисциплины	№ п/п	Тема и вид СРС	Трудоемкость (в часах)
Раздел 1	1	Современная ситуация в области информационной безопасности. Подготовка докладов.	8
	2	Абстрактные модели защиты информации. Подготовка докладов.	10
Раздел 2	3	Классификация криптоалгоритмов. Подготовка докладов.	10
	4	Подготовка к модульному контролю №1	10
Раздел 3	5	Уровни сетевых атак согласно модели *OSI.* Подготовка докладов.	10
Раздел 4	6	Обзор современного ПО. Подготовка докладов.	10

Раздел 5	7	Политика ролей. Подготовка докладов к разделу	10
	8	Подготовка к модульному контролю №2	10
Итого			78

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.	34
	ЛР	-компьютерные технологии обучения.	16
		Итого	**50**

7. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы 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) Б. Анин. Защита компьютерной информации – СПб.: БХВ-Петербург, 2000 г.
2) А.В. Соколов, О.М. Степанюк. Методы информационной защиты объектов и компьютерных сетей – СПб.: ООО «Издательство полигон», 2000 г.
3) Г.Н. Чижухин. Основы защиты информации в вычислительных системах и сетях ЭВМ. Учебное пособие - Пензенский государственный университет, 2001 г.
4) В.И. Ярочкин. Информационная безопасность: Учебник для студентов ВУЗов. – М.: Академический проект, 2003.

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..

9. Материально-техническое обеспечение дисциплины (модуля):

Компьютерный класс, оснащенные компьютерами и оргтехникой. На компьютерах должен быть установлен полный паке MS Office и иное ПО.

10. Методические рекомендации по организации изучения дисциплины:

При преподавании курса необходимо ориентироваться на современные образовательные технологии. Аудиторная и самостоятельная работы должны быть направлены на углубление и расширение полученных знаний, на закрепление приобретенных навыков и применение формируемых компетенций. Кроме того, рекомендуется использовать дифференцированное обучение и активные методы проверки знаний при проведении проверочных работ, тестирования. Это достигается, например, путем организации индивидуальной самостоятельной работы студентов.

Примерный перечень экзаменационных вопросов должен доводиться до студентов в начале изучения дисциплины. При необходимости он может быть уточнен не позднее, чем за месяц до начала экзаменационной сессии. На его основе составляются экзаменационные билеты, утверждаемые заведующим кафедрой.

ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

Курс 4
Семестр 7
Группа **ИТ13ДР62ПИ**
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, преподаватель Г.С. Федорченко

Рабочая учебная программа рассмотрена методической комиссией инженерно-технического института протокол №1 от «12» 09 2018 г. и признана соответствующей требованиям Федерального Государственного образовательного стандарта и учебного плана по направлению 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ».

Председатель МК ИТИ Е.И. Андрианова

Зав. обслуживающей кафедры, доцент Ю.А. Столяренко