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 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки
2.09.03.01 Информатика и вычислительная техника

Профиль подготовки
Вычислительные машины, комплексы, системы и сети

Квалификация (степень) выпускника:	**бакалавр**
Форма обучения:	**очная, заочная**
Год набора:	**2021 г.**

Разработал:
к.т.н., доцент кафедры ИТ,

/Ю.А. Столяренко

«28» августа 2024 г.

Тирасполь, 2024

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Защита информации» у обучающегося должны быть сформированы следующие компетенции:

Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Общепрофессиональные компетенции выпускников и индикаторы их достижения		
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1$_{УК-1}$ Знать: методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа
		ИД-2$_{УК-1}$ Уметь: применять методики поиска, сбора и обработки информации: осуществлять критический анализ и синтез информации, полученной из разных источников
		ИД-3$_{УК-1}$ Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации: методикой системного подхода для решения поставленных задач
-	ПК-9. Способен обеспечивать информационную безопасности на уровне БД	ИД-1$_{ПК-9}$ Знать Методы обеспечения информационной безопасности на уровне БД
		ИД-2$_{ПК-9}$ Уметь анализировать угрозы информационной безопасности на уровне БД
		ИД-3$_{ПК-9}$ Владеть способами обеспечения информационной безопасности на уровне БД

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. Основные виды и источники атак на информацию. Раздел 2. Криптография	УК-1, ПК-9	Контрольная работа №1 Лабораторная работа №1

	Раздел 3. Сетевая безопасность		Лабораторная работа №2
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 4. ПО и информационная безопасность Раздел 5. Комплексная система безопасности		Контрольная работа №2 Лабораторная работа №3 Лабораторная работа №4
Промежуточная аттестация		Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1		УК-1, ПК-9	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$_{УК-1}$ Знать: методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа	Не знает	Знает методики сбора и обработки информации	Знает методики сбора и обработки информации; актуальные российские и зарубежные источники информации	Знает методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа
Второй этап	ИД-2$_{УК-1}$ Уметь: применять методики поиска, сбора и обработки информации: осуществлять критический анализ и синтез информации, полученной из разных источников	Не умеет	Умеет применять методики поиска, сбора и обработки информации	Умеет применять методики поиска, сбора и обработки информации: осуществлять критический анализ	Умеет применять методики поиска, сбора и обработки информации: осуществлять критический анализ и синтез информации, полученной из разных источников
Третий этап	ИД-3$_{УК-1}$ Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации: методикой системного подхода для решения поставленных задач	Не владеет	Владеет методами поиска, сбора и обработки, критического анализа	Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации	Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации: методикой системного подхода для решения поставленных задач
Первый этап	ИД-1$_{ПК-9}$	Не знает	Знает методы обеспечения информационной безопасности	Знать методику обеспечения	Знает методы обеспечения информационной

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	**3**	**4**	**5**
	Знать Методы обеспечения информационной безопасности на уровне БД			информационной безопасности	безопасности на уровне БД
Второй этап	ИД-2$_{ПК-9}$ Уметь анализировать угрозы информационной безопасности на уровне БД	Не умеет	Умеет анализировать угрозы	Умеет анализировать угрозы информационной безопасности	Уанализировать угрозы информационной безопасности на уровне БД
Третий этап	ИД-3$_{ПК-9}$ Владеть способами обеспечения информационной безопасности на уровне БД	Не владеет	Владеет навыками работы с ПО	Владеет способами обеспечения информационной безопасности	Владеет способами обеспечения информационной безопасности на уровне БД

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	A (отлично) – 88-100 баллов
4 (хорошо)	70–87	B (очень хорошо) – 80-87баллов
		C (хорошо) – 70-79 баллов
3 (удовлетворительно)	50–69	D (удовлетворительно) – 60-69 баллов
		E (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

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

5.2. Примерные вопросы к контрольной работе №2

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

5.3 Пример лабораторной работы №1

Лабораторная работа №1. Шифр простой перестановки

Задание на лабораторную работу

Реализовать программно алгоритм шифрования подстановкой степени *n*, среда разработки и язык программирования используется на усмотрение студента. При выполнении лабораторной работы необходимо предусмотреть выдачу на экран: исходного текста, ключа, шифрованного текста и расшифрованного текста.

5.4 Пример лабораторной работы №2

Лабораторная работа №2. Шифр Цезаря

Реализовать программно (среда разработки и язык программирования используется на усмотрение студента):
-алгоритм Цезаря степени *n*, при выполнении лабораторной работы необходимо предусмотреть выдачу на экран: исходного текста и зашифрованного текста.

-расшифруйте текст не зная значение сдвига:
1. т бврэфравэле ъащявюуардщжхъше бшбвхьре шбяюымчгхвбп юфшэ ш вюв цх ъыоз фып ишдаютрэшп ш фып арбишдаютъш
2. ё офмуцтжфдшмм зфиёсмщ ёфирис мхутпалтёдпмха зёд ёмзд ьмшфтё лдрисд м уифихцдстёод
3. рглдсозз жузерлп л угфтусфхугриррюп тулпзусп ылчуг кгпзрю веовзхфв ылчу щзкгув
4. рцохшфицёъое фйуё он чшёцкпюоы уёщр кл очшфцое уёчэошбзёкш укчрфсврф шбчеэ скш
5. щъзшмсарс р цлрх рп цщхцйхгэ щчцщциций пзбръг рхьцшфзюрр еъц щруцйгм фмъцлг, ъц мщъд цэшзхз лцтыфмхъз
6. рёкп кй усрургрд йвыкфэ кпцртовшкк яфр уфжевпретвцкб йвмнащвнуб д урмтэфкк уворер цвмфв пвнкщкб ужмтжфпрл кпцртовшкк

7. зт утгёписмг отруавцифтё офмуцтжфдшмг хтхцтгпд мхопвымципаст мл хмрётпасящ дпжтфмцртё
8. чщшв юоъцё ькнёце чфчшфош з шфт эшф жщрзб ёсъёзошё нёткуедшче жщрзёто шфиф мк ёсъёзошё уф чф чйзоифт
9. лштп цчхщпифпс ъофжт хз пшцхтгоълуху япычл щх хф ухнлщ чжшяпычхижщг щлсшщ цъщму цлчлзхчж стеюлр
10. втюъе щоъоыьйчшлфт илхизьыи ыйцецт щъшыьецт т лоъшиьчш ыйцецт нъолчтцт втюъйцт
11. есффхгрсеозрлз фссдьзрлв лол нобъг лк кгылчусегррсёс хзнфхг ргкюегзхфв жзылчусегрлз
12. з чотткшцоэубы ёсифцоштёы йсе нёюоъцфзро о цёчюоъцфзро чффжякуое очхфсвнщкшче фйоу о шфш мк рсдэ

5.5 Пример лабораторной работы №3

Лабораторная работа №3. Шифр Вижинера

Реализовать **программно** алгоритм шифрования Вижинера степени *n*, среда разработки и язык программирования используется на усмотрение студента. При выполнении лабораторной работы необходимо предусмотреть вы-дачу на экран: ключа исходного, шифрованного и расшифрованного текстов.

5.6. Пример лабораторной работы №4

Лабораторная работа №4. Лозунговый Шифр

Реализовать **программно** Лозунговый алгоритм шифрования, среда раз-работки и язык программирования используется на усмотрение студента. При выполнении лабораторной работы необходимо предусмотреть выдачу на экран: таблицу шифрозамен, шифрованного и расшифрованного текстов.

5.7 Пример тем курсовых работ.

Темы курсовых работ по дисциплине «**Защита информации**» курсовые работы не предусмотрены.

5.8 Вопросы к экзамену по дисциплине «**Защита информации**»

1. Современная ситуация в области информационной безопасности. Категории информационной безопасности.
2. Абстрактные модели защиты информации. Обзор наиболее распространенных методов «взлома» паролей.
3. Симметричные криптоалгоритмы.
4. Асимметричные криптоалгоритмы.
5. Другие системы и виды информации.
6. Криптографические протоколы.
7. Атакуемые сетевые компоненты (рабочие станции).
8. Атакуемые сетевые компоненты (сервера)ю
9. Уровни сетевых атак согласно модели OSI (Open System Interconnectoin) программные.
10. Уровни сетевых атак согласно модели OSI (Open System Interconnectoin) аппаратные.
11. Обзор современного ПО.
12. Ошибки, приводящие к возможности атак на информацию.
13. Основные положения по разработке ПО.
14. Классификация информационных объектов.
15. Политика ролей.

Вопросы к экзамену

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. Сокрытие 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

Ответы на вопросы к экзамену

№ вопроса	№ ответа	Содержание ответа
1	3	Шпионские программы
2	2	Постоянные пароли
3	3	Сопровождение
4	2	Неавторизованный доступ
5	1	Комплексный
6	2	Загрузочные
7	2	Атака на систему крупного предприятия
8	1, 4	Адекватность; Неисчерпаемость
9	3	Это попытка злоумышленника подбора пароля до его успешного получения
10	4	Сетевой уровень
11	5	P@ssw0rd
12	4	SYN Flood
13	4	Состояние защищенности информации, обрабатываемой средствами ВТ или АС, от внутренних и внешних угроз
14	2	Несанкционированное копирование информации
15	2	Сокрытие факта наличия секретной информации
16	3	Вирус не влияет на уровень безопасности системы

17	4	Паспортные данные
18	3	Объекты системы, процессы обработки информации, каналы связи, побочные электромагнитные излучения, управление системой защиты
19	1	Чтение, копирование, изменение, удаление
20	1	Хэш-функция