Государственное образовательное учреждение

«Приднестровский государственный университет имени Т.Г. Шевченко»

Рыбницкий филиал

Кафедра информатики и программной инженерии

«УТВЕРЖДАЮ»
Директор Рыбницкого филиала ПГУ им. Т.Г. Шевченко
профессор _____ И.А. Павлинов
«10» сентября 2021г.

РАБОЧАЯ ПРОГРАММА

на 2021/2022 учебный год

УЧЕБНОЙ ДИСЦИПЛИНЫ
«СЕТЕВЫЕ ТЕХНОЛОГИИ»

Направление подготовки:

2.09.03.04 «Программная инженерия»

Профиль подготовки:

«Разработка программно-информационных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения:
очная

Год набора **2018**

Рыбница 2021г.

Рабочая программа дисциплины «*Сетевые технологии*»/сост. А.Б. Глазов. – Рыбница: Рыбницкий филиал ПГУ им. Т.Г. Шевченко, 2021. – 18 с.

РАБОЧАЯ ПРОГРАММА ПРЕДНАЗНАЧЕНА ДЛЯ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ ПО ВЫБОРУ ВАРИАТИВНОЙ ЧАСТИ ДИСЦИПЛИН (МОДУЛЕЙ) СТУДЕНТАМ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ 2.09.03.04 – *«ПРОГРАММНАЯ* ИНЖЕНЕРИЯ», ПРОФИЛЬ ПОДГОТОВКИ *«РАЗРАБОТКА ПРОГРАММНО ИНФОРМАЦИОННЫХ СИСТЕМ».*

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 № 229 от 12 марта 2015 года.

Составитель _____ **А.Б. Глазов, ст. преподаватель**

1. *Цели и задачи освоения дисциплины*

Цель освоения учебной дисциплины «Сетевые технологии» – формирование компетенций, связанных с функционированием компьютерных сетей, принципами взаимодействия элементов сети на аппаратном и программном уровнях, построением сетей на основе типового оборудования и программного обеспечения.

Задачи освоения учебной дисциплины:

– изучение основных понятий, логических и физических принципов построения сетей ЭВМ и телекоммуникаций; принципов взаимодействия компьютеров и сетевого оборудования на аппаратном и программном уровне;

– изучение сетевых операционных систем и основ их взаимодействия с операционными системами отдельных компьютеров.

– изучение базовых протоколов различных уровней стека протоколов TCP/IP.

2. *Место дисциплины в структуре ООП ВО*

Дисциплина «Сетевые технологии» относится к дисциплине по выбору вариативной части дисциплин (модулей) (Б1.В.ДВ.08.01), читается студентам очной формы обучения по направлению 2.09.03.04 – «Программная инженерия» профиля подготовки «Разработка программно информационных систем».

Для освоения дисциплины «Сетевые технологии» обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: «Основы программирования», «Архитектура ЭВМ», «Периферийные устройства ЭВМ», «Машинно-зависимые языки программирования».

Освоение дисциплины «Сетевые технологии» является основой для последующего написания выпускной квалификационной работы бакалавра.

3. *Требования к результатам освоения дисциплины*

Изучение дисциплины направлено на формирование следующих компетенций:

Код компетенции	Формулировка компетенции
ПК-2	Владением навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных

В результате освоения дисциплины студент должен:

3.1. Знать:

– принципы функционирования вычислительных сетей и комплексов;

– основные решения по построению физического, канального, сетевого и транспортного уровней;

– методы и способы программной реализации сетевого взаимодействия в вычислительных сетях.

3.2. Уметь:

– на основе полученных знаний формулировать и решать задачи проектирования и модернизации локальной или корпоративной вычислительной сети, а также глобальной сети;

– конфигурировать сетевые устройства;

– оценивать трафик в сегментах сети;

– выбирать состав сетевого оборудования и программного обеспечения.

3.3. Владеть навыками:

– продемонстрировать соединения компонентов сетевого оборудования в единый комплекс;

– использования предоставляемого операционной системой пользовательского интерфейса конфигурирования сетевой операционной среды.

4. *Структура и содержание дисциплины*

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

Семестр	Количество часов						Форма итогового контроля
	Трудоем-кость, з.е./часы	В том числе					
		Аудиторных				Самост. работа	
		Всего	Лекций	Лаб. работы	Практич. занятия		
7	5/180	72	36	36	-	72	Экзамен Курсовая работа
Итого:	**5/180**	**72**	**36**	**36**	-	**72**	**Экзамен Курсовая работа**

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

№ раз-дела	Наименование модулей	Количество часов				
		Всего	Аудиторная работа			Внеауд работа (СР)
			Л	ПЗ	ЛР	
1	Основные понятия и определения	6	6	-	-	-
2	История развития криптографии как науки	20	4	-	-	16
3	Современные криптографические системы	56	8	-	16	32
4	Защита программного обеспечения	24	10	-	14	-
5	Сетевые технологии в рамках организации	24	4	-	-	20
6	Сетевые технологии на государственном уровне	14	4	-	6	4
Итого:		**144**	**36**	-	**36**	**72**

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
1	1	2	Цели и задачи дисциплины. Современные тенденции и основные проблемы построения компьютерных сетей. Основные сетевые термины.	–
2		2	Многоуровневый подход к построению компьютерных сетей, понятие протокола, стека протоколов, интерфейса. Многоуровневая модель TCP/IP стек коммуникационных протоколов.	–
3		2	Логическая и физическая структуризация сетей, сетевые топологии. Локальные и глобальные сети. Сетевые службы. Требования, предъявляемые к сетям ЭВМ.	–
4	2	2	Коммутация каналов, частотное и временное мультиплексирование. Коммутация пакетов, виртуальные каналы. Коммутация сообщений.	–
5		2	Структурированная кабельная система локальной вычислительной сети. Сетевые адаптеры. Концентраторы и их функции, управление концентраторами. Мосты локальных вычислительных сетей. Коммутаторы локальных сетей и их функции.	–

			Полнодуплексные режимы работы. Характеристики и дополнительные функции коммутаторов. Виртуальные локальные сети..	
6	3	2	Структура стандартов IEE802.X. Протокол LLC управления логическим каналом Технология Ethernet, метод доступа CSMA/CD, типы кадров технологии Ethernet, стандарты физической среды Ethernet. Методика расчета конфигурации сети Ethernet. Технологии Fast Ethernet и Gigabit Ethernet.	раздаточный материал
7		2	Принципы и протоколы маршрутизации. Реализация межсетевого взаимодействия средствами TCP/IP. Протокол IP. Адресация и маршрутизация в IP-сетях.	раздаточный материал
8		2	Статическая маршрутизация. Введение в динамические протоколы маршрутизации. Дистанционно-векторные протоколы маршрутизации.	–
9		2	Классовая и бесклассовая адресация. Технология масок подсетей переменной длины (VLSM). Технология бесклассовой междоменной маршрутизации (CIDR).	–
10	4	2	Характеристика протокола ARP. Основы использования ARP – таблиц. Динамические и статические ARP таблицы	раздаточный материал
11		2	Протоколы маршрутизации в IP-сетях. Характеристика этих протоколов по состоянию канала., числу хопов и другим признакам.	–
12		2	Организация локальной сети. Иерархическая модель. Уровни ядра, распределения и доступа иерархической модели. Принципы построения. Особенности коммутации. Сопоставление коммутаторов специфическим функциям LAN.	–
13		2	Протоколы транспортного уровня. Общее описание UDP протокола	–
14		2	Протоколы транспортного уровня. Протокол надежной доставки сообщений TCP	–
15	5	2	ICMP – протокол передачи управляющих пакетов в сети TCP/IP	раздаточный материал
16		2	Протокол прикладного уровня для отправки почтовых сообщений SMTP – общее описание и процесс работы	–
17	6	2	Протокол прикладного уровня для пересылки файлов TFTP, FTP назначение, основные команды и программное обеспечение	–
18		2	Протокол прикладного уровня HTTP для работы в Internet	–
Итого:		**36**		

Лабораторные работы

№ п/п	Номер раздела дисциплины	Объем часов	Тема практического занятия	Наименование лаборатор.	Учебно-наглядные пособия
1	3	4	Установка и знакомство с ОС Ubuntu Server, установка статического IP адреса.	аудитория № 30	методическое пособие
2		4	Установка web-сервера (LAMP), настройка Virtual Host для 2 сайтов (test.com , test.org)	аудитория № 30	методическое пособие
3		4	Установка ProFTP сервер, настройка доступа для 2 пользователей	аудитория № 30	методическое пособие

4		4	Установка файлового сервера Sumba сервера, настройка доступа для 3 папок.	аудитория № 30	методическое пособие
5	4	6	Установка и настройка корпоративного почтового сервера Postfix, связкой MySQL.	аудитория № 30	методическое пособие
6		2	Ubuntu Server в роли маршрутизатора.	аудитория № 30	методическое пособие
7		2	Настройка NAT	аудитория № 30	методическое пособие
8		2	Настройка Firewall	аудитория № 30	методическое пособие
9		2	Проброс портов.	аудитория № 30	методическое пособие
10	6	4	Установка и настройка DHCP сервера.	аудитория № 30	методическое пособие
11		2	Настройка DNS – клиента	аудитория № 30	методическое пособие
Итого:		**36**			

Самостоятельная работа студента

Раздел дисциплины	**№ п/п**	**Тема и вид СРС**	**Трудоемкость (в часах)**
2	1	Настройка сетевого окружения и параметров сети на компьютере	8
	2	Применение бесклассовой адресации для построения локальной сети с группами.	8
3	3	Работа с удаленным рабочим столом.	4
	4	Использование программы удаленного управления TeamViewer.	8
	5	Контроль трафика на локальном компьютере CommView	4
4	6	Системы защиты информации.	4
	7	Развитие теории и практики защиты информации.	4
	8	Сетевая защита.	8
5	9	Симметричные криптосистемы.	4
	10	Шифр простой перестановки, магический квадрат	4
	11	Перестановка «Магический квадрат»	4
	12	Асимметричные криптосистемы.	4
	13	Хакерские атаки, способы борьбы с ними.	4
6	*14*	Доктрина информационной безопасности ПМР.	4
Итого:			**72**

5. *Примерный перечень тем курсовых работ*

1. Сетевая игра в домино «Козел».
2. Сетевая игра в домино «Пятерка».
3. Сетевая игра в карты «Дурак».
4. Сетевая игра в карты «Blackjack».
5. Сетевая игра в кости.
6. Динамический анализ курсов валют.
7. Анализ изменения температуры по годам и регионам.
8. Анализ изменения влажности по годам и регионам.
9. Онлайн-анкетирование социальной тематике.
10. Простой голосовой чат.
11. Сетевой чат на Web Sockets.
12. Сайт для портфолио студента.

13. Удаленное управление компьютером.
14. SPA сайт с переменными темами оформления.
15. Простой аналог PHP Admin.
16. Сетевая игра в крестики-нолики.
17. Сайт по интерактивному обучению Pascal.
18. Реализация игры «Арканоид».
19. Разработка игры с сетевыми элементами.
20. Разработка сайта с использованием DBSN.
21. Сайт для организации работы поисковых систем.
22. Программа тестирование сервиса адаптации HTML-тегов для WordPress.

6. Образовательные технологии

Для повышения наглядности рассматриваемого материала применяются образовательные технологии, основанные на применении специализированных программных сред и технических средств работы с информацией. Например, лекции с мультимедийным сопровождением, с использованием электронных учебников.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
7	Л, ЛР	Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.	2
		Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения на всех уровнях. Мультимедийные программы предназначены как для аудиторной, так и самостоятельной работы студентов.	2
		Интернет-технологии – предоставляют широкие возможности для поиска информации и ведения научных исследований.	2
		Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.	2
		Технология тестирования – используется для контроля уровня усвоения знаний в рамках модуля на определённом этапе обучения. Данная технология позволяет преподавателю выявить и систематизировать аспекты, требующие дополнительной проработки.	2
		Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.	2
Итого:			24

В рамках данной дисциплины применяются инновационные методы, основанные на использовании современных достижений науки и информационных технологий в образовании. Они предполагают применение информационных образовательных технологий, а также учебно-методических материалов, соответствующих современному мировому уровню, в процессе преподавания дисциплины:

- использование мультимедийных учебников («Сетевые технологии»);
- использование обучающих Интернет-ресурсов;
- консультирование студентов с использованием электронной почты;
- использование программно-педагогических тестовых заданий для проверки знаний студентов.

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

Для оценки качества усвоения курса используются следующие формы контроля:

- **текущий** – контроль выполнения лабораторных работ, тестирование;

– **рубежный** предполагает использование тестовых материалов для контроля знаний;

– **итоговый** осуществляется посредством тестирования и экзамена.

Самостоятельная работа рассматривается как вид учебного труда студента, позволяющего целенаправленно формировать и развивать его самостоятельность как личностное качество при выполнении домашних заданий и проработке дополнительного учебного материала.

Самостоятельная работа организуется в двух формах:

– аудиторная (на практических занятиях, проводимых в счет лекционных часов в форме отчетов по решению индивидуальных заданий и на лабораторных занятиях при выполнении лабораторных работ);

– внеаудиторная работа: проработка лекций с целью самостоятельного выполнения индивидуальных заданий с примерами – 60 часов; подготовка к лабораторным занятиям, оформление отчётов по лабораторным работам – 12 часов.

№	Наименование работы	Число часов	Форма контроля
1	Проработка лекционного материала. Выполнение индивидуальных заданий	60	Отчет по индивидуальным заданиям.
2	Подготовка к лабораторным занятиям и оформление отчетов	12	Отчет. Допуск к лабораторным работам. Защита отчетов

Всего часов самостоятельной работы – 72.

Программа самостоятельной работы по дисциплине «Сетевые технологии» предполагает выполнение студентом в процессе обучения одного индивидуального задания из следующего списка индивидуальных заданий по компьютерным алгоритмам СЗИ:

1. Стандарт симметричного шифрования данных DES.
2. Блочный шифр IDEA.
3. Блочный шифр ГОСТ.
4. Блочный шифр CAST.
5. Блочный шифр BLOWFISH.
6. Блочный шифр RC5.
7. Блочный шифр LUCIFER.
8. Блочный шифр MADRYGA.
9. Блочный шифр NewDES.
10. Блочный шифр FEAL.
11. Блочный шифр REDOC.
12. Блочный шифр LOKI.
13. Блочный шифр KHUFU.
14. Блочный шифр RC2.
15. Блочный шифр MMB.
16. Блочный шифр CA-1.1.
17. Блочный шифр SKIPJACK.
18. Блочный шифр SAFER.
19. Блочный шифр 3-WAY.
20. Блочный шифр CRAB.
21. Блочный шифр SXAL8/MBAL.
22. Блочный шифр RC4.
23. Блочный шифр SEAL.
24. Асимметричный ранцевый криптоалгоритм.
25. Асимметричный алгоритм шифрования данных RSA.
26. Асимметричный алгоритм шифрования данных ElGamal.
27. Асимметричный алгоритм шифрования данных Pohlig-Hellman.
28. Асимметричный алгоритм шифрования данных Rabin.
29. Асимметричный алгоритм шифрования данных McEliece
30. Асимметричный алгоритм шифрования данных LUC.
31. Алгоритм цифровой подписи с открытым ключом DSA.
32. Алгоритм цифровой подписи с открытым ключом ГОСТ.
33. Однонаправленная хэш-функция Snefru.

34. Однонаправленная хэш-функция *N*-хэш.
35. Однонаправленная хэш-функция MD4.
36. Однонаправленная хэш-функция MD5.
37. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).
38. Однонаправленная хэш-функция RIPE-MD.
39. Однонаправленная хэш-функция HAVAL.

Образец теста для проведения итогового контроля по итогам освоения дисциплины, а также для контроля самостоятельной работы студента.

Тест №1

для среза текущих знаний

1) Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2) Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3) Атакой на КС называют:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4) Искусственные угрозы исходя из их мотивов разделяются на:

a) непреднамеренные и преднамеренные

b) косвенные и непосредственные

c) несанкционированные и сонкцианированные

5) К непреднамеренным угрозам относятся:

a) ошибки в разработке программных средств КС

b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

6) К умышленным угрозам относятся:

a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

c) ошибки пользователей КС;

7) Косвенными каналами утечки называют:

a) каналы, не связанные с физическим доступом к элементам КС

b) каналы, связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

8)К косвенным каналам утечки информации относятся:

a) использование подслушивающих (радиозакладных) устройств;

b) маскировка под других пользователей путем похищения их идентифицирующей

информации (паролей, карт и т.п.);

c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

9)Непосредственными каналами утечки называют:

a) каналы, связанные с физическим доступом к элементам КС.

b) каналы, не связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

10)К непосредственным каналам утески информации относятся:

a) обход средств разграничения доступа к информационным вследствие недостатков в их программном обеспечении и др.

b) перехват побочных электромагнитных излучений и (ПЭМИН).

c) дистанционное видеонаблюдение;

11) Избирательная политика безопасности подразумевает, что:

a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

b) все субъекты и объекты системы должны быть однозначно идентифицированы;

c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

12) Полномочная политика безопасности подразумевает, что:

a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

b) все субъекты и объекты системы должны быть идентифицированы;

c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) *правила (свойство избирательности).*

13) Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

14) Под <u>защитой информации</u> понимается

a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.

b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;

c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

15) Возможные каналы утечки информации по классификации разделяют:

a) человек, аппаратура, программа

b) человек, линия связи

c) коммутационное оборудование, человек

16)К группе каналов утечки информации в которой основным средством является <u>человек,</u> относятся следующие утечки:

a) расшифровка программой зашифрованной информации;

b) несанкционированный доступ программы к информации;

c) копирование программой информации с носителей.

17) К группе каналов утечки информации, в которой основным средством является <u>аппаратура,</u> относятся следующие утечки:

a) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;

b) хищение носителей информации (магнитных дисков, дискет, лент)

c) копирование программой информации с носителей

18) К группе каналов утечки информации в которой основным средством является <u>программа,</u> относятся следующие утечки:

a) несанкционированный доступ программы к информации
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

19) Идентификация объекта – это:
a) одна из функций подсистемы защиты.
b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи.
c) сфера действий пользователя и доступные ему ресурсы КС

20) Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:
a) авторизацией
b) аутентификацией
c) Идентификация

21) Авторизация – это:
a) предоставление полномочий
b) подтверждение подлинности
c) цифровая подпись

22) Аутентификация – это:
a) подтверждение подлинности
b) предоставление полномочий
c) цифровая подпись

23) Под компьютерным вирусом понимается:
a) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ.
b) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы.
c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

24) Трянские программы это:
a) программы, которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.
b) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.
c) программы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

ОТВЕТЫ

1	3	**6**	3	**11**	2	**16**	1	**21**	1
2	2	**7**	2	**12**	1	**17**	4	**22**	2
3	2	**8**	1	**13**	2	**18**	3	**23**	1
4	3	**9**	1	**14**	2	**19**	3	**24**	1
5	4	**10**	4	**15**	4	**20**	3		

Итоговый тест

1) К средствам активной защиты относятся:
a) искаженные программы (программы вирусы, искажение функций)
b) заказное проектирование
c) специальная аппаратура

2) К средствам пассивной защиты относятся:
a) частотный анализ
b) авторская эстетика
c) аппаратура защиты (ПЗУ, преобразователи)

3) К средствам собственной защиты относятся:
a) машинный код
b) сигнатура

c) корреляционный анализ

4) Под системой защиты от несанкционированного использования и копирования понимается:

a) комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.

b) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.

c) комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

5) Под надежностью системы защиты от несанкционированного копирования понимается:

a) способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.

b) способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений.

c) способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ

6) Методы, затрудняющие считывание скопированной информации основываются на

a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС

b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования дополнительных программных или аппаратно-программных средств.

7) Для защиты от несанкционированного использования программ могут применяться электронные ключи?

a) да

b) нет

c) не знаю

8) Любая криптографическая система основана на использовании:

a) криптографических ключей

b) разомкнутых линии

c) односторонних функций

9) В симметричной криптосистеме отправитель и получатель сообщения используют

a) один и тот же секретный ключ

b) разные секретных ключи

c) вообще не используют секретных ключей

10) Асимметричная криптосистема предполагает использование

a) двух ключей открытого и личного (секретного)

b) системы разграничения доступа

c) переносных носителей для хранения секретной информации

11) Под ключевой информацией понимают:

a) совокупность всех действующих в АСОИ ключей

b) совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.

c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации.

12)Какая из функций не входит в процесс управления ключами?

a) переадресация ключей

b) генерация ключей

c) распределение ключей

13) Модификация ключа – это

a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции.

b) генерирование нового ключа из последующего значения ключа с помощью

односторонней (однонаправленной) функции.

c) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней (двунаправленной) функции.

14) Под функцией хранения ключей понимают

a) организацию их безопасного хранения, учета и удаления.

b) организацию их генерации, учета и удаления.

c) организацию их безопасного хранения, учета и сопоставления.

15)В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа.

16) Файловые вирусы это:

a) вирусы, заражающие файлы с программами

b) вирусы, заражающие программы, хранящиеся в системных областях дисков.

c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

17) Резидентные вирусы это:

a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

b) вирусы, которые выполняются только в момент запуска зараженной программы.

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

18) Транзитные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

19) Вирусы-мутанты (MtE-вирусы) это

a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

20) Stealth-вирусы это

a) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных:

b) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

21) Загрузочные (бутовые) вирусы это:

a) вирусы, заражающие программы, хранящиеся в системных областях дисков.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

c) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

22) Основной проблемой создания высокоэффективной защиты от НСД является

a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.

b) использование дополнительных программных или аппаратно-программных средств.

c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

23)Аппаратно-программмные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.
b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.
c) проверяют на отсутствие закладок приборов, устройств.

24) Использование аппаратных средств снимает проблему:

a) обеспечения целостности системы.
b) разграничения прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
c) использования строго определенного множества программ.
a) за один цикл, и тем самым уменьшает длительность процесса идентификации.
b) внешней аутентификацией объекта, не принадлежащего системе.

ОТВЕТЫ

1	3	**6**	3	**11**	2	**16**	1	**21**	2
2	2	**7**	2	**12**	1	**17**	4	**22**	2
3	2	**8**	1	**13**	2	**18**	3	**23**	2
4	3	**9**	1	**14**	2	**19**	3	**24**	3
5	4	**10**	4	**15**	4	**20**	3		

Примерный перечень вопросов к экзамену:

1. Терминология и принципы организации сетей, основные понятия.
2. Основы работы Internet.
3. Стек протоколов OSI – общий обзор.
4. Стек протоколов TCP/IP начало.
5. Классификация сетей по размеру и по топологии, кольцо шина маркерный доступ.
6. Способы кодирования сигналов на физическом уровне.
7. Протокол Ethernet.
8. Сетевое оборудование.
9. Протокол ARP.
10. Прохождение IP пакета между сетями.
11. Классовая адресация IP сетей.
12. Бесклассовая адресация IP сетей.
13. Разбиение пула IP адресов на подсети.
14. Протокол UDP.
15. Протокол DHCP.
16. Протокол TFTP
17. Протокол TCP.
18. Протокол Telnet.
19. FTP клиент-сервер.
20. DNS сервера и система имен.
21. Введение в Python 3, установка.
22. Python функции.
23. Python: работа с массивами, число слов в тексте, список разных слов в тексте.
24. Python – средства работы с диском.
25. Сокеты на Python.
26. Запуск из Python внешнего приложения.
27. Python Генераторы Списков.
28. Python – основы работы в сети.
29. Применение Python для сетевых игр.
30. Python tcpserver.py, tcpclient.py.

31. Python udpserver.py, udpclient.py.
32. Чат на основе UDP протокола.
33. Python ftpclient, ftpserver.
34. Команда консольного режима Net.
35. Расчет оборудования компьютерной сети.
36. Запуск из Python внешнего приложения.
37. Python – основы работы в сети.
38. Запуск из Python внешнего приложения.
39. Python – основы работы в сети.
40. Способы передачи пакетов.
41. Запуск из Python внешнего приложения.
42. Python – основы работы в сети.
43. Программы TeamViewer, A3, Radmin.
44. Настройка сетевого подключения.
45. Консольные средства диагностики.
46. Методы управления трафиком.
47. Администрирование компьютерных сетей.
48. Практика по сниферам WireShark, ComView.
49. Обжимка кабеля сдача практики по расчету материалов для локальной сети.
50. Работа с Ethernet на канальном уровне. Простой снифер на Python.
51. Элементы протокола IP, IP adresa.
52. Элементы парсинга сайтов с Beautifulsoup.
53. Обзор Teamviewer, ICQ. Первичная настройка сети.
54. Утилиты консольной диагностики сети.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Винокуров Андрей. Криптография, ее истоки и место в современном обществе (Цикл статей по криптографии) – М.: ЗАО "Издательство БИНОМ", 2008. – 208 с.: ил.

2. Жельников Владимир. Криптография от папируса до компьютера. – М.: "Нолидж", 2008. – 384 с., ил.\.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с.

4. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с.

8.2. Дополнительная литература

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2002.

2. Безопасность информационных технологий. Выпуск 1. – М.: МИФИ. 2014.

3. Безопасность информационных технологий. Выпуск 3. – М.: МИФИ, 2005.

4. Вопросы защиты информации. – №1. – 2005.

5. Воронов М.В., Антонов Г.Н. К вопросу об устойчивости боевых систем. Военная мысль, 2011, 2. – с.75-76.

6. Герасименко В.А. Сетевые технологии в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 2014.

7. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

8. ГОСТ 34.10-94. Информационная технология. Криптографическая Сетевые технологии. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

9. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2012.

10. Мещеряков Р.В. Информационная безопасность. – Томск: ТПУ, 2004.

11. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. – М.: Прометей, 2009.

12. Насыпный В.В. Синтез систем обработки информации с защитой от программных закладок и вирусов. – М.: ВТИ, 2007.

13. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. – М.:ГТК РФ, 2012.

14. Термины и определения в области защиты от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2012.

8.3. Программное обеспечение и Интернет-ресурсы

1. Алефиренко В.М. Основы защиты информации (методические указания) – материалы сайта.

2. Ресурсный центр помощи студентам (методические указания) – материалы сайта: http://vstuhelp.narod.ru/met/zi.html

3. Электронный портал факультета электроники и вычислительной техники – материалы сайта: http://fevt.ru/load/78
http://www.twirpx.com/files/informatics/security/technical/ft.guideline/

8.4. Методические указания и материалы по видам занятий

Методические указания предоставляются студентам в виде теоретических предпосылок (в электронном виде) к практическим работам.

Отчеты по лабораторным работам следует оформлять в соответствии с общими требованиями и правилами оформления.

Программное обеспечение современных информационно-коммуникационных технологий:
Windows 7, средства просмотра Opera/Google Chrome, MS Office 2007.

9. *Материально-техническое обеспечение дисциплины*

Для осуществления образовательного процесса по дисциплине «Сетевые технологии» необходим компьютерный класс, а также лекционная аудитория, оборудованная мультимедийными средствами для демонстрации лекций-презентаций.

Карта обеспечения дисциплины учебными материалами:

№ п/п	Наименование	Вид	Форма доступа
1	Учебно-методическая литература по дисциплине «Сетевые технологии»	Электронный	Электронная библиотека, кафедра ИиПИ
2	Описание лабораторных работ	Электронный (Word)	Электронная библиотека, кафедра ИиПИ
3	Мультимедийные материалы	Сетевой	Медиатека кафедры ИиПИ
4	Электронная библиотека	Сетевой	Портал ПГУ им. Т.Г. Шевченко

Карта обеспечения дисциплины оборудованием:

№ п/п	Номер аудитории	Кол-во	Наименование	Форма использования
1	Аудитория № 30	10	Компьютеры типа Pentium III, объединенные локальной сетью. ОС Windows. Расширенный пакет Office. Глобальная сеть Internet.	Организация лабораторных работ, доступ к образовательным ресурсам во время самостоятельной работы студентов, работа с мультимедийными материалами на лабораторных занятиях

10. Методические рекомендации по организации изучения дисциплины

Рабочая учебная программа по дисциплине «Сетевые технологии» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО и учебного плана по направлению 2.09.03.04 «Программная инженерия» профилю подготовки «Разработка программно-информационных систем».

Методические рекомендации для студентов

Методические рекомендации для студентов содержат:

- тематику лабораторных работ;
- планы практических работ с указанием примерного списка аудиторных и домашних заданий.

Изучение дисциплины «Сетевые технологии» включает лекционные и лабораторные занятия. Лекции разбиты на основные разделы, каждый раздел может содержать несколько тем.

Курс сопровождают лабораторные работы. При подготовке к лабораторным занятиям студентам необходимо самостоятельно изучить рекомендуемую литературу, ответить на контрольные вопросы. В течение семестра каждый студент должен подготовить хотя бы один доклад на темы, предложенные преподавателем.

При подготовке к занятиям необходимо использовать литературу, имеющуюся в достаточном количестве в библиотеке вуза. В список рекомендуемой литературы входит основная и дополнительная литература. Список литературы приведен в карте обеспечения дисциплины учебно-методической литературой.

Текущий контроль усвоения знаний по дисциплине предполагает использование разных форм контроля, в том числе тестирование. Итоговый контроль может осуществляться в форме теста и экзамена. Вопросы к экзамену и образцы тестовых заданий приведены.

Методические указания по организации самостоятельной работы студентов

В курсе «Сетевые технологии» предусмотрен значительный объём самостоятельной работы студентов, который включает изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; подготовку к выполнению лабораторного практикума, самоконтроль знаний в форме тестирования; выполнение программированных заданий. Для приобщения обучаемых к поиску, к исследовательской работе, для развития их творческого потенциала следует по возможности избегать прямого руководства работой обучающихся при выполнении ими тех или иных заданий, чаще выступать в роли консультанта, эксперта, коллеги-исследователя.

Подготовка к выполнению лабораторных работ

Практикум способствуют повышению качества знаний студентов, это творческие задания, углубляющие знания студентов в их профессиональной деятельности.

Цель практикума – обеспечить текущий контроль над знаниями студентов; предоставить возможность: студентам – систематизировать и расширить знания, самостоятельно освоить пропущенный материал; преподавателю – оценить степень готовности студента к сдаче экзамена по дисциплине.

Для выполнения лабораторных работ по дисциплине «Сетевые технологии» необходим персональный компьютер с вышеперечисленными программами.

Выполнение практикума является необходимым условием для допуска к экзамену.

11. Технологическая карта дисциплины

Курс ____4____ группа ___РФ18ДР62ПИ___ семестр ____7____
Преподаватель – лектор Глазов Анатолий Борисович
Преподаватель, ведущий лабораторные занятия Глазов Анатолий Борисович
Кафедра_____информатики и программной инженерии _____

Наименование дисциплины / курса	Уровень//ступень образования (бакалавриат, специалитет, магистратура)	Статус дисциплины в рабочем учебном плане (А, Б, В, Г)	Количество зачетных единиц / кредитов
Сетевые технологии	бакалавриат	Б	5
Смежные дисциплины по учебному плану:			

Предшествующие: «Численные методы», «Основы программирования» «Организация и функционирование ЭВМ», «Архитектура ЭВМ», «Системный анализ», «Введение в алгоритмы».				
Последующие: написание выпускной квалификационной работы				
ВВОДНЫЙ МОДУЛЬ (входной рейтинг-контроль, проверка «остаточных» знаний по смежным дисциплинам)				
Тема, задание или мероприятие входного контроля	**Виды текущей аттестации**	**Аудиторная или внеаудиторная**	**Минимальное количество баллов**	**Максимальное количество баллов**
	Тестирование	Аудиторная	0	10
Итого:			0	**10**
БАЗОВЫЙ МОДУЛЬ (проверка знаний и умений по дисциплине)				
Тема, задание или мероприятие текущего контроля	**Виды текущей аттестации**	**Аудиторная или внеаудиторная**	**Мин. кол-во баллов**	**Макс. количество баллов**
Текущая работа	Лабораторные работы	Аудиторная	1	5
	Работа на лекциях	Аудиторная	3	5
	Присутствие на занятиях	Аудиторная	1	1
	Решение заданий	Аудиторная	3	5
	Самостоятельная работа	Внеаудиторная	3	5
Промежуточный рейтинг-контроль	Лабораторные работы	Аудиторная	1	5
Итого:			**12**	**21**
ДОПОЛНИТЕЛЬНЫЙ МОДУЛЬ				
Тема, задание или мероприятие дополнительного контроля	**Виды текущей аттестации**	**Аудиторная или внеаудиторная**	**Минимальное количество баллов**	**Максимальное количество баллов**
Промежуточный рейтинг-контроль	Тестирование	Аудиторная	5	10
Итого:			**5**	**10**
ИТОГОВЫЙ МОДУЛЬ				
	Тестирование	Аудиторная	10	15
Итого:			10	**15**

Необходимый минимум для получения итоговой оценки или допуска к промежуточной аттестации 12 баллов.

Составитель _____ А.Б. Глазов, ст. преподаватель

Зав. кафедрой информатики и программной инженерии _____ Л.А. Тягульская, доцент