МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *30* » *августа* 2023 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Защита информации в системах беспроводной связи
(наименование дисциплины)

10.05.02 Информационная безопасность, профиль «Защита информации в системах связи и управления»
(код и наименование ОПОП ВО)

Курск – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Сетевая аутентификация.

1) Что называют сетевой аутентификацией?

2) Что такое авторизация?

3) Перечислите объекты воздействия в информационных системах.

4) Что входит в задачи межсетевых экранов?

5) Что называют контролируемой зоной?

Тема 2. Функции межсетевых экранов, профили защиты.

1) Функции межсетевых экранов.
2) Фильтрация трафика.
3) Выполнение функций посредничества.
4) Дополнительные возможности МЭ.
5) Перечень профилей защиты межсетевых экранов.

Тема 3. Программные и аппаратные средства криптографической защиты.

1) Какие свойства присущи информации?

2) Дайте понятие объекта защиты информации.

3) Что относят к информационным процессам?

4) Что понимают под информационной системой?

5) Что называют информационными ресурсами?

Тема 4. Критерии оценки защищенности криптографических модулей.

1) Наиболее значимыми нормативными документами в области информационной безопасности являются?

2) Что включает в себя методика анализа защищённости?

3) Какие спецификации (шаблоны) для конфигурации наиболее распространенных системных программных средств известны?

4) Что определяют спецификации 1 и 2 уровней?

Тема 5. Построение VPN.

1) Каким образом сети VPN обеспечивают безопасную передачу пакетов?

2) Назовите виды VPN-соединений.

3) Перечислите достоинства и недостатки протоколов PPTP и L2TP.

4) Что такое RADIUS?

Тема 6. Аудит и мониторинг информационной.

1) Что такое аудит безопасности?

2) На какие вопросы отвечает аудит безопасности?

3) Какие функции выполняет мониторинг безопасности?

4) Для чего используется модели адаптивного управления безопасности сети?

Тема 7. Критерии выбора сканеров безопасности.

1) Для чего необходим сканер уязвимости?

2) Какие сканеры уязвимости Вы знаете?

3) Что включают в себя многофункциональные сканеры уязвимости?

4) Основные функции сканера Symantec Security Check?

5) Недостатки сканера Nessus?

Тема 8. Методы отражений вторжений.

1) Какие методы обнаружения Вам известны?

2) Преимущество способа обнаружения аномалий?

3) Какие атаки могут выполнять злоумышленники?

4) Могут ли сетевые системы обнаружения вторжений взаимодействовать с другими системами безопасности?

Критерии оценки:

9-12 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

5-8 баллов (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1-4 баллов (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может

привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 «Настройка межсетевого экрана в операционной системе Windows»

1) Что такое брандмауэр?
2) Какие бывают брандмауэры?
3) Что фиксирует журнал безопасности брандмауэра?
4) Перечислите основные требования к выбираемым средствам анализа защищенности.
5) Дайте общий обзор современных средств анализа защищенности.

Лабораторнаяработа № 2 «Фаервол Comodo Firewall»

1) Дайте определение межсетевого экрана.
2) Перечислите основные функции межсетевых экранов.
3) Перечислите основные схемы подключения межсетевых экранов.
4) Перечислите типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI.

Лабораторная работа № 3 «Антивирусная программа: Kaspersky Internet Security»

1) Дайте классификацию компьютерных вирусов.
2) В чем основное отличие вирусов-сценариев от файловых вирусов?
3) Существование каких вирусов зависит от конкретной программы?
4) В чем основное отличие троянской программы от вируса. Приведите пример троянской программы.

Лабораторная работа №4 «Анализ защищенности компьютерной сети с помощью программ GFI Languard, Network Security Scanner и XSPIDER»

1) В чем состоит концепция адаптивного управления безопасностью? Перечислите основные компоненты модели адаптивной безопасности.
2) Каков общий принцип работы средств анализа защищенности сетевых протоколов и сервисов?
3) Каков общий принцип работы средств анализа защищенности операционной системы?
4) Каковы методы анализа сетевой информации, используемые в средствах обнаружения сетевых атак?
5) Какова классификация систем обнаружения атак?
6) Перечислите основные компоненты системы обнаружения атак.
7) Каковы положительные и отрицательные стороны систем обнаружения атак на сетевом и операционном уровнях?

8) Дайте общий обзор современных средств обнаружения сетевых атак.

Критерии оценки:

6-5 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

Задание №1

Какая сетевая атака связана с превышением допустимых пределов функционирования сети ?

1. Отказ в обслуживании (DoS –атака).
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Угадывание ключа.

Задание №2

Какая сетевая атака является характерной именно для беспроводных сетей ?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).

3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №3
Основной защитой от фишинга являются:
1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №4
Под политикой безопасности организации понимают:
1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №5
Политика удаленного доступа – это:
1. Специализированная политика безопасности.
2. Базовая политика безопасности.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №6
Политики безопасности разделяют на уровни:
1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.

Нет разделения на уровни.

Задание №7

Под аутентификацией понимают:
1. Процедуру проверки подлинности заявленного пользователя, процесса, устройства.
2. Процедуру распознавания пользователя по его идентификатору.
3. Процедуру предоставления субъекту определенных полномочий и ресурсов в сети.
4. Регистрацию действий пользователя в сети.

Задание №8
Вероятность угадывания PIN –кода из 4 десятичных цифр за 3 попытки равна:
1. 0,0003.
2. 0,003
3. 0,00003.
4. 0,0004.

Задание №9
Различают следующие виды систем идентификации и аутентификации:
1. Электронные, биометрические и комбинированные.

2. Электронные и биометрические.
3. Электронные, биометрические и механические.
4. Электронные, биометрические и криптографические.

Задание №10
Какую функцию не может выполнять межсетевой экран?
1. Лечение файлов, зараженных вирусами.
2. Фильтрация трафика.
3. Трансляция сетевых адресов.
4. Регистрация событий.

Задание №11
Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности ?
1. Комплексный межсетевой экран.
2. Экранирующий маршрутизатор.
3. Шлюз сеансового уровня.
4. Прикладной шлюз.

Задание №12
Различают следующие варианты исполнения межсетевых экранов:
1. Программный и программно-аппаратный.
2. Программный и аппаратный.
3. Аппаратный и программно – аппаратный.
4. Существуют только программные межсетевые экраны.

Задание №13
Какая вредоносная программа не размножается, но способна удаленно управлять компьютером и воровать пароли ?
1. Троянская программа.
2. Червь.
3. Файловый вирус.
4. Макровирус.

Задание №14
Какая антивирусная программа не конфликтует с другими антивирусами, но не имеет функции автоматического обновления антивирусной базы?
1. Dr. Web Curelt.
2. Kaspersky Internet Security.
3. Eset NOD 32 Antivirus.
4. Avira AntiVir Personal.

Задание №15
Какой метод выявления вируса позволяет обнаруживать только известные вирусы?
1. Обнаружение, основанное на сигнатурах.
2. Обнаружение программ подозрительного поведения.
3. Обнаружение вирусов при помощи эмуляции работы программы.
4. Эвристический анализ.

Задание №16
В чем основное отличие системы анализа защищенности от системы обнаружения атак ?

1. Системы анализа защищенности исследуют сеть и ищут уязвимости в ней, системы обнаружения атак предназначены для противодействия сетевым атакам в реальном масштабе времени.

2. Системы анализа защищенности предназначены для противодействия сетевым атакам в реальном масштабе времени, системы обнаружения атак только моделируют сетевые атаки в целях поиска уязвимостей в защите сети.

3. Системы анализа защищенности и системы обнаружения атак – это одно и то же.

4. В отличии от систем обнаружения атак системы анализа защищенности только выдают предупреждения об обнаруженных атаках, но не противодействуют им в автоматическом режиме.

Задание №17

Какой метод анализа сетевой информации не требует знаний о возможных атаках и используемых ими уязвимостях?

1. Статистический метод.
2. Экспертные системы.
3. Нейронные сети.
4. Такого метода не существует.

Задание №18

Какие системы обнаружения атак (IDS) позволяют обнаруживать новые, ранее неизвестные виды сетевых атак?

1. IDS, которые для выявления атаки используют способ - обнаружение аномального поведения.
2. Пассивные IDS.
3. Активные IDS.
4. IDS, которые для выявления атаки используют способ - обнаружение злоупотреблений.

Задание №19

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа ?

1. 7.
2. 5.
3. 9.
4. 6.

Задание №20

Какой класс защищенности автоматизированных систем предъявляет наиболее высокие требования к информационной безопасности ?

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №21

Вторая группа классов защищенности автоматизированных систем включает автоматизированные системы:

1. В которых работают несколько пользователей и все они имеют одинаковые права доступа к информации.

2. В которых работают несколько пользователей и они имеют различные права доступа к информации.

3. В которых работает только один пользователь.

4. В которых работает один пользователь или несколько пользователей, имеющих одинаковые права доступа к информации.

Задание №22

Какой стандарт, используемый при проведении аудита, состоит из двух частей: “Практические рекомендации” и “Спецификации системы” ?

1. Стандарт BS7799
2. Стандарт ISO17799
3. Стандарт ISO/IEC15408
4. Стандарт SysTrust

Задание №23

Какой этап проведения аудита является первым ?

1. Инициирование и планирование процедуры аудита.
2. Сбор информации аудита.
3. Анализ данных аудита.
4. Оценка соответствия требованиям стандарта.

Задание №24

В каком методе анализа рисков рассчитываются минимальный и максимальный ущерб?

1. Оценка по верхним и нижним значениям.
2. Оценка рисков на этапе рассмотрения этапов вторжения.
3. Логарифмическая шкала.
4. Оценка на основе выявления слабого звена.

Задание №25

Какая программа предназначена для шифрования HTML – кода?

1. WebCrypt.
2. TrueCrypt.
3. PGP.
4. КРИПТОН Подпись.

Задание №26

Даны два Java – скрипта.

Первый Java – скрипт имеет вид:

```
<script language="JavaScript">

document.onselectstart=function(){return false}

document.onmousedown=function(){return false}

</script>
```

Второй Java – скрипт имеет вид:

```
<script language="JavaScript">
document.onselectstart=function(){return false}
```

```
document.oncontextmenu=function(){return false}
document.onmousedown=function(){return false}
</script>
```

Какой из рассмотренных Java – скриптов в целях защиты информации блокирует использование правой кнопку мыши ?

1. Второй
2. Первый
3. Первый и второй.
4. Ни один из рассмотренных Java – скриптов не блокирует правую кнопку мыши.

Задание №27

Какую из двух программ (Easy Watermark или Photoshop) можно использовать для защиты фотографии водяным знаком?

1. Можно использовать обе программы: Easy Watermark или Photoshop.
2. Только Easy Watermark.
3. Только Photoshop.
4. Ни одна из данных программ не позволяет установить на фотографию водяной знак.

Задание №28

Основная масса угроз приходится на:

1. Шпионские программы.
2. Троянские программы.
3. Черви.

Задание №29

Какой вид идентификации и аутентификации является наиболее распространённым:

1. Одноразовые пароли.
2. Постоянные пароли.
3. системыPKI.

Задание №30

Под какие системы вирусы распространяются наиболее динамично:

1. Windows.
2. Mac OS.
3. Android.
4. Linux.

Задание №31

Заключительный этап построения системы защиты:

1. Планирование.
2. Сопровождение.
3. Анализ уязвимых мест.
4. Отчётность.

Задание №32

Какие угрозы безопасности информации являются преднамеренными:

1. Открытие электронного письма, содержащего вирус.
2. Ошибка персонала.
3. Не авторизированный доступ.
4. Открытие сайта.

33. Выберите соответствие названий типов сетей устройств из приведен- ного перечня в зависимости от их масштаба:

а) муниципальная вычислительная сеть (Munitipal Area Network □ MAN);

б) территориальная вычислительная сеть (Wide Area Network □ WAN);

в) локальная вычислительная сеть □ ЛВС (Local Area Network □ LAN);

г) кампусная вычислительная сеть (Campus Area Network □ CAN); д) персональная вычислительная сеть (Personal Area Network □ PAN).

34. Укажите название утилиты, пересылающей набор тестовых пакетов на удаленный компьютер и получающей от него в случае его нормальной работы ответные пакеты

а) gong;

б) ping;

в) ring;

г) gang.

35. Выберите компоненты, входящие в состав сетевого адаптера: а) постоянное запоминающее устройство с BIOS;

б) разъем для подключения кабеля;

в) контроллер аппаратных прерываний IRQ; г) кварцевый элемент тактового генератора; д) СБИС контроллера сетевого адаптера;

е) панелька для BootROM;

ж) южный мост (Input-Output Controller Hub).

36. Выберите минимальное количество настроек, необходимых для орга- низации работы компьютера настройки в сети с сетевым протоколом TCP/IP:

а) установить IP-адрес компьютера;

б) установить основной шлюз подсети данного компьютера; в) установить маску подсети, в которую входит компьютер;

г) установить IP-адрес DNS-сервера локальной сети компьютера; д) установить IP-адрес почтового сервера домена;

е) установить IP-адрес прокси-сервера.

37. Выберите вариант, в котором правильно расположены в порядке воз- растания значений полосы пропускания следующие среды передачи данных □ коаксиальный медный кабель, кабель на основе медной ви- той пары, оптоволоконный кабель:

а) коаксиальный медный кабель, кабель на основе медной "витой пары", оптоволоконный кабель;

б) оптоволоконный кабель, коаксиальный медный кабель, кабель на основе медной "витой пары";

в) кабель на основе медной "витой пары", коаксиальный медный кабель, оптоволоконный кабель.

38. Выберите ресурсы, выделяемые операционной системой сетевому адаптеру:

а) MAC-адрес адаптера;

б) порт ввода-вывода (I/O port); в) полоса пропускания канала; г) запрос прерывания IRQ;

д) диапазон адресов памяти адаптера.

Укажите вводимую в окне командной строки команду, отображаю- щую IP-адрес компьютера, работающего под операционной системой Windows:

а) cmd;

б) net;

в) ipconfig; г) netstat.

39. Укажите преимущества использования компьютерных сетей:

а) возможность оперативной коммуникации между участниками се- ти и оперативного доступа к информации;

б) возможность совместного использования аппаратных ресурсов; в) возможность практически безграничного увеличения вычисли-

тельной производительности систем;

г) возможность организации совместной работы путем разделения прикладных программ и файлов;

д) упрощение конфигурирования и пользования операционными си- стемами и пользовательскими программами;

е) возможность централизованного управления данными и про- граммами.

40. Выберите соответствие названий и определений сетевых компонентов Windows, приведенных в списке:

а) клиент; б) протокол; в) служба; г) адаптер.

41. Драйвер сетевой платы, непосредственно взаимодействующий с сетевой платой, установленной в компьютере это…,

 Компонент, регламентирующий правила разбиения потока информации на пакеты и правила адресации компьютеров-участников сети,

 Компонент, позволяющий подключаться к серверам сети,

 Компонент, позволяющий выделять сетевые ресурсы на компьютере,на котором он установлен,

42. Выберите типы доступа для сетевых дисков и папок, определяемых в операционной системе Windows:

а) чтение;

б) чтение и выполнение; в) изменение;

г) запись;

д) полный доступ; е) просмотр;

ж) список содержимого папки.

43. Какой из сетевых компонентов Windows обеспечивает возможность предоставления ним сетевых ресурсов?

а) адаптер;

б) сетевой протокол; в) клиент;

г) служба.

44. Какой из сетевых компонентов Windows отвечает за адресацию узлов сети на сетевом уровне?

а) адаптер;

б) сетевой протокол; в) клиент;

г) служба.

45. Выберите правильную команду выделения на Вашем компьютере пап- ки C:\Data в общее пользование по сети с сетевым именем AllData: а) net share AllData =c:\data;

б) net share c:\data AllData; в) net use AllData = c:\data; г) net use c:\data AllData;

д) net view AllData =c:\data;

е) net view c:\data AllData.

46. Выберите команду подключения сетевого ресурса \\FS_stud\user и отображения его как сетевого диска Z:

а) net share Z: \\Fs_stud\user; б) net share \\Fs_stud\user Z: ; в) net use Z: \\Fs_stud\user;

г) net use \\Fs_stud\user Z: д) net view Z: \\Fs_stud\user е) net view \\Fs_stud\user Z:

47. Выберите команду, позволяющую вывести список сетевых имен рабо- тающих в данный момент компьютеров Вашей сети:

а) net computer

б) net view в) net config г) net name д) net group

48. Укажите, кто входит в группу пользователей Все в операционной си- стеме Windows:

а) все пользователи локальной сети; б) все пользователи сети предприятия;

в) все зарегистрированные в операционной системе пользователи.

49. Выберите права, которые отличают разрешение Изменение от разреше- ния Полный доступ:

а) добавлять файлы и подпапки;

б) изменять владельца сетевого ресурса; в) изменять данные в файлах;

г) изменять разрешения безопасности; д) удалять подпапки и файлы.

50. Выберите название протокола прикладного уровня, позволяющего од- новременно организовывать сетевой доступ к файловым ресурсам и принтерам в Windows и Linux:

а) HTTP б) FTP

в) CIFS/SMB.

51. Укажите номера битов MAC-адреса (нумерация начинается с нуля) для каждого из его полей:

а) Поле U/L уникальный в глобальном/локальном масштабе; б) Поле I/G индивидуальный/групповой;

в) Поле OUA организационно-уникального идентификатора порядкового номера сетевого контроллера, выпускаемого организацией;

г) Поле OUI организационно-уникального идентификатора кода организации, выпускающей сетевое оборудование.

52. Выберите максимальную на сегодняшний день стандартизованную скорость передачи данных по технологии Ethernet:

а) 10 Мбит/с;

б) 100 Мбит/с;

в) 1 Гбит/с;

г) 10 Гбит/с;

д) 40 Гбит/с;

е) 100 Гбит/с;

ж) 1 Тбит/с.

53. Укажите уровни модели взаимодействия открытых систем, на которых работает технология Ethernet:

а) сетевой;

б) канальный; в) прикладной;

г) транспортный;

д) представления данных; е) физический;

ж) сеансовый.

54. Укажите размеры максимального кадров Ethernet (не учитывая опцио- нальную возможность передачи гигантских кадров (Jambo Frame)):

а) 32 байта;

б) 64 байта;

в) 128 байт;

г) 256 байт;

д) 512 байт;

е) 1024 байта;

ж) 1518 байт;

з) 2000 байт.

55. Укажите размеры минимальных кадров Ethernet (не учитывая опцио- нальную возможность увеличения минимального размера кадра до 512 байт в полудуплексном режиме работы технологии Gigabit Ethernet):

а) 32 байта;
б) 64 байта;
в) 128 байт;
г) 256 байт;
д) 512 байт;
е) 1024 байта;
ж) 1518 байт;
з) 2000 байт.

Укажите размер MAC-адреса: а) 2 байта;
б) 3 байта;
в) 4 байта;
г) 6 байт;
д) 8 байт.

56. Определите тип приведенных MAC-адресов (однопунктовый, групповой, широковещательный):

а) 33:33:00:01:00:03 □ это…
б) 00:1c:f0:0d:66:11 □ это… в) ff:ff:ff:ff:ff:ff □ это…

57. Определите тип кадра Ethernet (DIX, Novell 802.3, 802.3/LLC, SNAP) по байтам заголовка канального уровня:

а) 00:4F:49:02:D8:6A:00:A0:C9:83:16:16:08:00;
б) 00:A0:C9:85:17:B2:00:4F:4E:00:E5:8F:00:54:E0:E0:03;
в) 00:4F:4E:00:CD:4A:00:60:8C:41:DF:C7:00:96:AA:AA:03:00:00
:00:08:00;
г) 00:00:F8:45:13:AC:00:00:C0:02:56:AB:00:78:FF:FF.

58. Выберите неизвестную в общем случае адресную информацию при отправке пакета утилиты ping по IP-адресу назначения:

а) MAC-адрес отправителя; б) MAC-адрес получателя; в) IP-адрес отправителя; г) IP-адрес получателя.

59. Укажите, откуда коммутатор Ethernet узнаѐт MAC-адреса подключѐнных к нему компьютеров, необходимые для заполнения его таблицы MAC-адресов:

а) выполняет последовательный опрос подключѐнных компьютеров; б) "подсматривает" адрес отправителя во входящих в него пакетах; в) опрашивает все компьютеры в широковещательном режиме.

60. Укажите, какие пакеты будет захватывать Wireshark при введѐнной команде фильтра ether proto 0x0806

а) только кадры Ethernet с любыми пакетами внутри; б) только кадры Ethernet с IP пакетами внутри;
в) только кадры Ethernet с ARP-пакетами внутри.

Укажите команды (enable, config t, interface имя_интерфейса), позволяющие осуществлять вход в различные режимы работы Cisco IOS:

а) войти в режим глобального конфигурирования можно коман- дой…;
б) войти в привилегированный режим можно командой…;
в) войти в режим конфигурирования интерфейса можно командой….

61. Хост имеет IP-адрес 192.168.1.47 и маску подсети 255.255.255.224. Укажите адрес подсети и широковещательный адрес подсети, в которую входит данный хост.

Укажите класс (A, B или C) следующих IP-адресов:

- 172.16.2.2;
- 10.15.234.28;
- 192.168.5.137.

62. В Вашей сети находится 31 компьютер. Укажите маску подсети, обеспечивающую выделение этих компьютеров в подсеть с минимально возможным числом IP-адресов

а) 255.255.255.248;
б) 255.255.255.240;
в) 255.255.255.224;
г) 255.255.255.192;
д) 255.255.255.128.

63. Выберите условие, при выполнении которого хост/маршрутизатор пересылает IP-дейтаграмму шлюзу:

а) IP-адрес отправителя и IP-адрес получателя принадлежат разным сетям/подсетям; б) IP-адрес отправителя и IP-адрес получателя принадлежат одной и той же сети/подсети;

64. Выберите правильное определение для максимальной единицы передачи (Maximum Transfer Unit, MTU):

а) MTU – это максимально допустимый размер заголовка IP-пакета; б) MTU – это максимально допустимый размер IP-пакета;

в) MTU – это максимально допустимое значение длины поля данных кадров канального уровня.

Выберите адрес, по которому не будут передаваться IP-дейтаграммы в Интернете:

а) 141.25.13.48; б) 172.31.204.1; в) 191.15.26.147.

65. Выберите логическую операцию, которая используется для определения адреса сети/подсети из IP-адреса получателя дейтаграммы:

а) IP-адрес получателя XOR маска сети/подсети; б) IP-адрес получателя OR маска сети/подсети; в) IP-адрес получателя AND маска сети/подсети.

Укажите маску суперсети с 2000 хостами, если адрес такой сети 212.14.17.0:

а) 255.255.255.0;
б) 255.255.254.0;
в) 255.255.252.0;
г) 255.255.248.0.

66. Укажите порядковый номер (от 1 до 5) для столбцов таблицы маршрутизации:

а) IP-адрес следующего по маршруту маршрутизатора = …; б) метрика маршрута = …;

в) адрес сети/подсети/хоста назначения = …;

г) IP-адрес исходящего порта текущего маршрутизатора = …; д) маска подсети назначения = ….

66. Выберите правильное утверждение об изменениях MAC- и IP-адресов в пересылаемых в составной сети сетевых пакетах при следовании их по маршруту:

а) MAC-адрес отправителя на каждом шаге изменяется, MAC-адрес получателя остаѐтся неизменным, IP-адреса остаются неизменными;

б) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса также остаются неизменными;

в) MAC-адрес отправителя и MAC-адрес получателя изменяются на каждом шаге изменяется, IP-адреса остаются неизменными;

г) MAC-адрес отправителя и MAC-адрес получателя остаются неизменными на каждом шаге, IP-адреса изменяются;

67. Укажите, какя информация служит указателем на первый фрагмент дейтаграммы:

а) нулевое значение флага MF More Fragments; б) нулевое значение поля Смещение фрагмента; в) нулевое значение поля Идентификатор пакета.

68. В пакете, пересылаемом в локальной сети порт отправителя = 80, порт получателя = 24561. Выберите из списка тип протокола и привязку портов к клиенту и серверу:

а) протокол UDP, отправитель сервер, получатель клиент; б) протокол UDP, отправитель клиент, получатель сервер; в) протокол TCP, отправитель сервер, получатель клиент; г) протокол TCP, отправитель клиент, получатель сервер.

69. Выберите, что характеризует порт транспортного уровня:

а) порт сетевого адаптера, через который хост работает с сетью; б) область памяти, связанную с сетевым приложением;

в) порт ввода-вывода, закреплѐнный за сетевым адаптером.

70. Выберите соответствия для названий стандартных служб и закреплѐн- ных за ними номеров портов: а) 80, б) 21, в) 67, г) 53, д) 25:

FTP …;

HTTP …;

DNS …;

DHCP …;

SMTP ….

71. Команда netstat -an вывела на экран следующие строки. Укажите, какие из них описывают сокеты установленного соединения:

а) TCP 0.0.0.0:135 0.0.0.0:0 LISTENING;

б) TCP 109.201.253.151:3603 74.125.39.104:80 ESTABLISHED;

в) TCP 109.201.253.151:54035 62.165.4.118:33016 TIME_WAIT;

г) TCP 109.201.253.151:54035 90.176.90.125:11740 SYN_RECEIVED.

72. Укажите десятичное значение, идентифицирующее UDP в поле Про- токол IP-заголовка:

а) 01;

б) 06;

в) 17.

73. Укажите поля, которые входят в псевдозаголовок, используемый при расчѐте контрольной суммы UDP или TCP:

а) MAC-адрес отправителя; б) MAC-адрес получателя;

в) IP-адрес отправителя; г) IP-адрес получателя; д) порт отправителя;

е) порт получателя;

ж) идентификатор протокола; з) длина пакета с заголовком.

74. Выберите, чему равняется максимальный размер сегмента для заго- ловка Ipv4 без опций и заголовка TCP длиной 28 байт:

а) 1452 байта;

б) 1460 байт;

в) 1472 байта;

г) 1500 байт.

75. TCP-пакет с полем данных 500 байт имеет десятичное значение SEQ#=15246, а десятичное значение ACK#=32412. Выберите, какими будут десятичные значения этих полей в ответе на данный пакет, если в нѐм пересылается 300 байт данных:

а) SEQ#=15746, ACK#=32712; б) SEQ#=32712, ACK#=15746; в) SEQ#=15747, ACK#=32713; г) SEQ#=15745, ACK#=32711

76. Из захваченных пакетов сеанса TCP извлечены три пакета с флагами: а) PSH, ACK;

б) SYN;

в) FYN, ACK; г) SYN, ACK.

77. Укажите, какие из них относятся к:

пакетам, устанавливающим соединение, …;

пакетам, передающим данные в сеансе, …;

пакетам, завершающим соединение, ….

78. Выберите название поля заголовка TCP, позволяющего регулировать поток данных с противоположной стороны соединения:

а) Длина заголовка; б) Окно;

в) Контрольная сумма; г) Указатель срочности.

79. **Защита соединений**На каком типе щифрования основан протокола IPSec

А) симметричном Б) асиметричном В) комбинированном Г) В нём не используется шифрование

80. Почему хэш вставляется в конце передаваемого по сети кадра

А) потому что он формируется аппаратно во время последовательной передачи и завершает кадр Б) потому что это позволяет минимизировать потери информации при случайных искажениях В) это упрощает разбор кадра при получении

Задания в открытой форме

1. Сетевое устройство, принимающее поток битов, поступающих из сети, на один из своих портов и передающее этот поток на все остальные порты это …

2. Находятся ли в одной подсети компьютеры с IP-адресами 172.16.2.65 и 172.16.2.94, если у них маска подсети 255.255.255.224?

3. Электронная плата, устанавливаемая в разъем системной платы компьютера и обеспечивающая подключение и прием-передачу данных по линиям компьютерной сети это …

4. Устройство, получающее сетевые пакеты на один из своих портов и передающее их на другой соответствующий порт, определяемый в зависимости от значения адреса сетевого уровня в заголовке пакета, это …

5. Устройство, принимающее кадры из сети на один из своих портов и передающее эти кадры на соответствующий другой порт, определяемый по MAC-адресу получателя в заголовке кадра, это …Сеть, обеспечивающая передачу данных в пределах страны или кон- тинента, это …

6. Определите, правильно ли следующее утверждение: в одноранговой сети под управлением Windows на каждом компьютере сети установлены и клиент для сетей Microsoft, и служба доступа к файлам и принтерам.

7. Сеть, объединяющая провайдеров услуг Интернет в одном городе,

это …

8. Сеть, объединяющая компьютеры компьютерного класса, это … Сеть, объединяющая коммуникационные устройства одного человека,

это …

9. Сеть, объединяющая университетские компьютеры и компьютеры, находящиеся в общежитиях и других зданиях студенческого городка, это …

Сеть, обеспечивающая передачу данных в пределах страны или кон- тинента, это …

10. Сеть, объединяющая провайдеров услуг Интернет в одном городе, это …

11. Режим, при котором передача и прием данных происходят одновре- менно, это …

12. Режим, при котором передача и прием данных происходят по очереди,это …

13. Режим, при котором происходит только передача или только прием данных, это …

14. Уровень, обеспечивающий проверку доступности передающей среды, адресацию интерфейсов сетевых устройств, реализацию механизмов опре- деления и коррекции ошибок передачи, это …

15. Уровень, обеспечивающий адресацию сетей, подсетей и рабочих станций, а также передачу пакетов данных из сети в сеть с выбором опти- мального маршрута к получателю, это …

16. Уровень, обеспечивающий передачу битов данных по передающей среде, это …

17. Уровень, обеспечивающий возможность одновременной передачи отправителем нескольких потоков данных, а также обеспечивающий гаран- тированную передачу данных, это …

18. Уровень, обеспечивающий преобразование формата данных, представляемых вышележащим уровнем, в некоторый общий формат представ- ления данных, а также шифрование и дешифрование данных, это …

19. Уровень, обеспечивающий определение активной стороны при передаче данных, а также синхронизацию соединения с возможностью уста- новки контрольных точек, это …

20. Уровень, предоставляющий пользовательским приложениям сетевые протоколы и службы для обеспечения передачи данных по сети, это …

Задания на установление соответствия

1. Установите соответствие между указанными в списке названиями и определениями режимов передачи данных:

а) полнодуплексный (Full Duplex)
б) полудуплексный (Half Duplex)
в) симплексный (Simplex)

2. Выберите соответствие между названиями и определениями уровней модели OSI:

1	Прикладной уровень	А	обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений
2	Сетевой уровень	Б	уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью
3	Уровень представления	В	предназначен для обеспечения надёжной передачи данных от отправителя к получателю
4	Канальный уровень	Г	определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.
5	Физический уровень	Д	предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля ошибок, которые могут возникнуть.
6	Сеансовый уровень	Е	предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.
7	Транспортный уровень	Ж	обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время

3. Установить соответствие топологии сети её характеристике

1	Общая шина	А	Каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети

2	Звезда	Б	В данной топологии все рабочие станции соединены друг с другом с помощью центрального концентратора
3	Кольцо	В	В основе топологии лежит общий кабель (магистраль), к которому подсоединяются все рабочие станции
4	Комбинированные решения	Г	Топология, в которой каждая рабочая станция соединяется только с двумя соседними

4. Установить соответствие названия ОС её назначению

1	NetWare	А	Серверная операционная система для поддержки виртуальных машин, включая виртуальные машины на Linux.
2	LANtastic	Б	Серверная операционная система с объектно-ориентированный интерфейсом OS/2 для создания мощного набора графических средств администратора.
3	Windows Server 2019	В	Сетевая операционная система и набор сетевых протоколов для взаимодействия с компьютерами-клиентами, подключёнными к сети
4	LAN server	Г	Сетевая операционная система для DOS, Windows,OS/2 с поддержкой технологии Ethernet, ARCNET и Token Ring

5. Установить соответствие между способами и видами информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

6. Установить соответствие названия протокола его назначению

1	FTP	А	Протокол передачи данных
2	SMTP	Б	Протокол передачи файлов
3	TCP/IP	В	Протокол передачи гипертекста
4	HTTP	Г	Протокол передачи почты

Задания на установление правильной последовательности

1.Расположите в правильном порядке уровни модели ISO взаимодей- ствия открытых систем (Open System Interconnect), пронумеровав уровни от нижнего до верхнего от 1 до 7:

1. транспортный
2. физический
3. канальный
4. сетевой
5. представления данных

6. прикладной
7. сеансовый

2. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

5. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

5. Установить этапы построения программы обеспечения безопасности:

1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

6. Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

7. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005

2. ISO/IEC 17799

3. ISO/IEC 15408

4. «Критерии оценки доверенных компьютерных систем»

8. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки

2. Анализ угроз и их последствий, определение слабостей в защите

3. Выбор, реализация и проверка защитных мер
4. Оценка остаточного риска
5. Идентификация активов и ценности ресурсов, нуждающихся в защите
6. Выбор анализируемых объектов и степени детальности их рассмотрения

9. Расположить этапы проведения аудита информационной безопасности:
1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных
3. Сбор исходных данных
4. Разработка регламента проведения аудита

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

Создать топологию, состоящую из маршрутизатора, к которому подключены 2 компьютера. Между ПК 1 и маршрутизатором подсеть 172.16.0.0, ПК 2 и маршрутизатором подсеть 192.168.0.0. Проверить

доступность компьютеров (ПК) с помощью команды ping. Создать Access list, запрещающий прохождений icmp-пакетов из подсети 192.168.0.0. Выполнить команду ping с ПК 1 на ПК 2 и с ПК2 на ПК 1.

Компетентностно-ориентированная задача № 2

Файловый архив емкостью 412 Мб скачивается 20 минут. Соответствует ли действительности заявленная скорость провайдера в 35 Мбит/с.

Компетентностно-ориентированная задача № 3

Определите информационный объём сообщения в байтах, если в греческом алфавите 24 буквы и сообщение на греческом языке, содержащее 150 символов, было записано в коде Unicode.

Компетентностно-ориентированная задача № 4

Сколько времени будет скачиваться архив емкостью 500 Мб при скорости 50 Мбит/с.

Компетентностно-ориентированная задача № 5

Для кодирования последовательности, состоящей из букв А, Б, В, Г и Д, используется неравномерный двоичный код.

Для букв А, Б, В и Г использованы кодовые слова:

А-111

Б-110

В-101

Г-100

Определите, каким кодовым словом может быть закодирована буква Д.

(Код должен удовлетворять свойству однозначного декодирования. Если можно использовать более одного кодового слова, указать кратчайшее).

Компетентностно-ориентированная задача № 6

Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Компетентностно-ориентированная задача № 7

Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в России в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Google и Яндекс.

Компетентностно-ориентированная задача № 8

Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в США в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Rambler и Google.

Компетентностно-ориентированная задача № 9

Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в ФРГ в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Google.

Компетентностно-ориентированная задача № 10

Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в России в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Rambler.

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

10-15 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода

(ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

6-9 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

1-5 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.