МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Мониторинг безопасности телекоммуникационных сетей
(наименование учебной дисциплины)

10.05.02 Информационная безопасность, профиль «Управление безопасностью телекоммуникационных систем и сетей»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ.

Тема 1. Введение. Анализ современного состояния сетевой безопасности

1. Как проходила эволюция угроз?
2. Какие происходили сдвиги в потребительском восприятии угроз сетевой безопасности?
3. Какова актуальность технологий предотвращения утечек?
4. Какие существуют наиболее эффективные методы защиты?
5. Что представляет собой шифрование и многофакторная аутентификация?
6. Чем характеризуются BGP и утечки информации?

Тема 2. Назначение сетевых пакетов и их структура

1. Какова необходимость упаковки информации?
2. Как оформляют заголовки пактов?
3. Что представляет формат данных в пакте?
4. Какие существуют методы управления обменом данными?
5. Как происходит управление обменом данными в системах с различной топологией?
6. Для чего нужна адресация пакетов?

Тема 3. Анализ сетевого трафика

1. Что такое APM-решения?
2. Каковы признаки комплексного подхода к анализу трафика?
3. Какие существуют методы анализа сетевого трафика?
5. В чем заключается особенность парадигмы сетевого мониторинга?
6. Что представляют собой решения в области анализа трафика?

Тема 4. Программные утилиты для мониторинга сети

1. Каково назначение лицензирования средств мониторинга сети?
2. Что входит в состав лицензирования средств мониторинга сети?
3. Что представляет собой функционал лицензирования средств мониторинга сети?
4. Какие есть особенности лицензирования средств мониторинга сети?
5. Охарактеризуйте состояние рынка средств мониторинга сети?
6. Какие существуют виды собираемой информации в сетевых мониторах?

Тема 5. Контроль трафика с помощью виртуальных частных сетей

1. Дайте определение виртуальных частных сетей?
2. В чем состоит принцип действия VPN?

3. Что входит в процесс создания туннеля?

4. В чем особенность процесса инкапсуляции?

5. Что представляет собой туннелирование на уровне 2?

6. Как можно охарактеризовать туннелирование IPSec?

Тема 6. Угрозы информации в беспроводных сетях

1. Какие существуют особенности беспроводных сетей?

2. Что такое периметр беспроводных сетей?

3. Что представляют собой риски для информации в беспроводных сетях?

4. Какие есть особенности уязвимости устройств беспроводной связи?

5. Как происходят ошибки конфигурации точек беспроводного доступа?

6. Что представляют собой ошибки конфигурации клиентов беспроводных сетей?

Тема 7. Получение информации от сетевых сервисов

1. Как происходит сканирование портов?

2. Как можно получить информацию от DNS-сервера.

3. Что такое перебор имен и перебор обратных записей?

4. Как получают информацию с использованием SNMP?

5. В чем особенность получения информации с использованием NetBIOS?

6. Что представляет собой работа с электронной почтой?

Тема 8. Системы мониторинга сетей связи

1. Что такое контроль точек взаимодействия сетей?

2. Что представляет собой управление сетью?

3. Каковы возможности современных систем контроля сетей связи?

4. Как происходит учет разговорного трафика?

5. Какие существуют функциональные возможности систем мониторинга сетей связи?

6. Для чего необходим анализ качества функционирования сети?

Тема 9. Системы обнаружения вторжений. Автоматическая валидация уязвимостей с помощью нечетких множеств и нейронных сетей

1. Как происходит проверка конфигураций и поиск уязвимости ИС?

2. Какие есть принципы работы систем обнаружения вторжений?

3. Что входит в состав системы обнаружения вторжений?

4. Чем представлена классификация систем обнаружения вторжений?

5. Как происходит размещение компонентов системы обнаружения вторжений в сети?

6. Как происходит постановка задачи нечеткой классификации уязвимостей при использовании нейросетей?

Критерии оценки:

2 балла 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.

1 балл 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 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 «Средства устранения неисправностей в TCP/IP»

1. Что представляет собой удалённый ресурс? Примеры.
2. Какие способы подключения удалённых ресурсов вам известны?
3. Что такое общий ресурс? Приведите примеры.
4. Как создать общий ресурс?
5. Как подключить удалённый принтер, используя командную строку?
6. Как просмотреть список удалённых ресурсов узла?
7. Как удалить подключенный ранее сетевой диск?
8. Как добавить в список разрешений заданного пользователя?

Лабораторная работа №2 «Протокол управления транспортом»

1. Каково назначение портов транспортного уровня и приведите примеры портов?
2. Каков диапазон портов, закреплѐнный за стандартными серверными службами?
3. Какие примеры портов служб, обычно использующих UDP и портов служб, обычно использующих TCP?
4. В чем сходство и отличие функций протоколов UDP и TCP?
5. Что называют адресом сокет?
6. Какая команда позволяет отобразить пары сокетов, образующих коммуникации?
7. Опишите заголовок UDP?
8. Как вычисляется контрольная сумма заголовка?

Лабораторная работа №3 «Контроль сетевой активности через VPN»

1. Что такое виртуальная частная сеть?
2. Какие средства существуют в операционных систем для организации контроля сетевой активности пользователей?
3. Какие функции у приложения Traffic Inspector?
4. Какую сетевую активность можно наблюдать с помощью VPN – туннеля?
5. Можно ли из внешней сети обнаружить активность приложения Traffic Inspector?
6. Как настроить VPN подключения к серверу?
7. Как назначить правила отдельным пользователям и их группам?
8. Как проверить работу правил и корректность настроек?

Лабораторная работа №4 «Беспроводные технологии Bluetooth»

1. Что такое технология Bluetooth?

2. Какие технические особенности технологии Bluetooth можно выделить?

3. Какие средства безопасности предусмотрены в технологии Bluetooth?

4. Сколько основных угроз и какие возможны при Bluetooth-связи?

5. Сколько основных рекомендаций и какие следует выполнять при Bluetooth-связи?

6. Каково назначение беспроводных технологий Bluetooth?

7. Какие 6 основных рекомендаций по безопасному использованию у технологии Bluetooth?

8. Назовите методы защиты терминала беспроводной связи Bluetooth в системе Android?

Лабораторная работа №5 «Сетевые утилиты и их использование»

1. Для чего предназначена утилита ipconfig (IP configuration)?
2. Для чего предназначена утилита ping (Packet Internet Groper)?
3. Для чего предназначена утилита tracert?
4. Что такое сервис Whois?
5. Каковы параметры утилиты ping?
6. Как произвести трассировку двух работоспособных узлов?
7. Какие существуют типы адресов?
8. Для чего предназначена служба DNS?

Критерии оценки:

3 балла (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.

2 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.

1 балл (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.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1 «Назначение пакетов и их структура, адресация пакетов»

1. Каково назначение локальной сети?
2. Для чего необходим сетевой адрес?
3. Как происходит адресация пакетов?
4. Как происходит передача пакетов в сети между двумя абонентами?
5. Какие существуют методы управления обменом?
6. За что отвечает сетевой уровень модели OSI?
7. Как определить диапазон адресов в подсети?
8. Как определить размер подсети?

Лабораторная работа №2 «Анализаторы сетевых протоколов»

1. Для решения каких задач используется анализатор сетевых протоколов?
2. Что представляет собой анализатор протоколов?
3. Какие общие свойства имеют анализаторы протоколов?
4. Что представляют собой программные анализаторы протоколов?
5. Каков интерфейс анализатора сетевых протоколов Wireshark?
6. Приведите примеры анализаторов сетевых протоколов?
7. Какие существуют типы аппаратных анализаторов?
8. В каких случаях применяются аппаратные анализаторы ЛВС?

Лабораторная работа №3 «Исследование работы телефонной сети на базе АТС Panasonic»

1. Сколько видов звонкового сигнала предусмотрено в мини АТС?
2. Как работает режим приема звонка другими абонентами?
3. Какие преимущества дает использование системного телефонного аппарата?
4. Для чего служит режим программирования абонента?
5. Приведите примеры ситуаций когда можно использовать каждый из режимов переназначения звонков.
6. Какие вы знаете типы телефонных аппаратов и чем они отличаются друг от друга?
7. Какие комбинации телефонных аппаратов могут быть при конференц-связи?
8. Какие различия между режимами удержания линии?

Критерии оценки:

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

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

2. На сколько уровней модель OSI разделяет коммуникационные функции:

(1) семь

(2) восемь

(3) пять

3. Какие задачи выполняют уровни OSI в процессе передачи данных по сети:

(1) уровни выполняют одинаковые задачи, постоянно повторяя передающие сигналы по сети

(2) каждый уровень выполняет свою определенную задачу

(3) первых три уровня выполняют одинаковые задачи, последующие выполняют определенные задачи

4. Выбрать правильное расположение уровней модели OSI от 7 до 1:

(1) прикладной, канальный, представления, сеансовый, транспортный, сетевой, физический

(2) представления, прикладной, сеансовый, транспортный, сетевой, канальный, физический

(3) прикладной, представления, сеансовый, транспортный, сетевой, канальный, физический

5. Верно ли утверждение: «Каждый уровень модели выполняет свою функции. Чем выше уровень, тем более сложную задачу он решает»:

(1) верно

(2) не верно

6. На базе протоколов, обеспечивающих механизм взаимодействия программ и процессов на различных машинах, строится:

(1) горизонтальная модель

(2) вертикальная модель

(3) сетевая модель

7. Какой уровень представляет собой набор интерфейсов, позволяющим получить доступ к сетевым службам:

(1) представления

(2) прикладной

(3) сеансовый

8. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

(1) представления

(2) прикладной

(3) канальный

9. Какой уровень обеспечивает битовые протоколы передачи информации:

(1) физический

(2) канальный

(3) транспортный

10. Основными элементами модели OSI являются:

(1) уровни, прикладные процессы и физические средства соединения

(2) уровни и прикладные процессы

(3) уровни

11. Единицей информации канального уровня являются:

(1) сообщения

(2) потоки

(3) кадры

12. Согласно этому протоколу передаваемое сообщение разбивается на пакеты на отправляющем сервере и восстанавливается в исходном виде на принимающем сервере:

(1) TCP

(2) IP

(3) WWW

13. Доставку каждого отдельного пакета до места назначения выполняет протокол:

(1) TCP

(2) IP

(3) HTTPS

14. Какие функции выполняет протокол IP

(1) маршрутизация

(2) коррекция ошибок

(3) установка соединения

15. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

(1) сетевой

(2) представительский

(3) транспортный

16. Подтверждение подлинности взаимодействующих объектов обеспечивает:

(1) аутентификация

(2) конфиденциальность

(3) контроль доступа

17. Защиту от несанкционированного использования ресурсов обеспечивает:

(1) контроль доступа

(2) конфиденциальность

(3) аутентификация

18. Цифровая подпись – это:

(1) способ введения электронной метки для файла данных

(2) сведения о пользователе помещаемые в файл

3) файл, подтверждающий ваши права

(4) идентификатор документа

19. К механизмам безопасности относят:

(1) алгоритмы симметричного шифрования

(2) невозможность отказа от полученного сообщения

(3) целостность сообщения

(4) хэш-функции

20. Совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующих функции защиты и обеспечения безопасности это:

(1) политика безопасности (Security Policy)

(2) ядро безопасности (Trusted Computing Base, TCB)

(3) модель безопасности (Security Model)

(4) идентификация (Identification)

21. Специальный нормативный документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. В ходе квалификационного анализа служит описанием информационного продукта:

(1) профиль защиты

(2) проект защиты

(3) задачи защиты

(4) круг защиты

22. Потенциальные угрозы, определяющие задачи защиты информации в сетях:

(1) прослушивание каналов

(2) внедрение сетевых вирусов

(3) умышленное уничтожение или искажение информации

(4) выход из строя операционной системы

23. Что представляет собой запись и последующий анализ всего проходящего потока сообщений

(1) прослушивание каналов

(2) контроль доступа

(3) аутентификация

(4) аудит

24. К сервисам безопасности относят:

(1) идентификация/аутентификация

(2) протоколирование/аудит

(3) шифрование

(4) аудит

25. Какое управление доступом, осуществляемое на основании заданного администратором множества разрешенных отношений доступа.

(1) мандатное управление доступом (Mandatory Access Control)

(2) дискреционное управление доступом (Discretionary Access Control)

(3) прямое взаимодействие (Trusted Path)

(4) идентификация (Identification)

26. Что представляет собой управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов:

(1) дискреционное управление доступом (Discretionary Access Control)

(2) мандатное управление доступом (Mandatory Access Control)

(3) модель безопасности (Security Model)

(4) идентификация (Identification)

27. Что представляет собой предотвращение пассивных атак для передаваемых или хранимых данных:

(1) конфиденциальность

(2) контроль доступа

(3) аутентификация

28. Активные угрозы становятся видимыми на уровне (модели OSI):

(1) транспортном

(2) физическом

(3) канальном

(4) сетевом

29. Что представляет собой совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности:

(1) модель безопасности (Security Model)

(2) ядро безопасности (Trusted Computing Base, TCB)

(3) политика безопасности (Security Policy)

(4) прямое взаимодействие (Trusted Path)

30. Что представляет собой принцип организации информационного взаимодействия, гарантирующий, что передаваемая информация НЕ подвергнется перехвату или искажению:

(1) мандатное управление доступом (Mandatory Access Control)

(2) политика безопасности (Security Policy)

(3) прямое взаимодействие (Trusted Path)

(4) идентификация (Identification)

31. Основными источниками угроз информационной безопасности являются все указанное в списке:

(1) хищение жестких дисков, подключение к сети, инсайдерство

(2) перехват данных, хищение данных, изменение архитектуры системы

(3) хищение данных, подкуп системных администраторов, нарушение регламента работы

32. Виды информационной безопасности:

(1) персональная, корпоративная, государственная

(2) клиентская, серверная, сетевая

(3) локальная, глобальная, смешанная

33. Цели информационной безопасности – своевременное обнаружение, предупреждение:

(1) несанкционированного доступа, воздействия в сети

(2) инсайдерства в организации

(3) чрезвычайных ситуаций

34. Основные объекты информационной безопасности:

(1) компьютерные сети, базы данных

(2) информационные системы, психологическое состояние пользователей

(3) бизнес-ориентированные, коммерческие системы

35. Основными рисками информационной безопасности являются:

(1) искажение, уменьшение объема, перекодировка информации

(2) техническое вмешательство, выведение из строя оборудования сети

(3) потеря, искажение, утечка информации

36. К основным принципам обеспечения информационной безопасности относится:

(1) экономической эффективности системы безопасности

(2) многоплатформенной реализации системы

(3) усиления защищенности всех звеньев системы

37. К основным функциям системы безопасности можно отнести все перечисленное:

(1) установление регламента, аудит системы, выявление рисков

(2) установка новых офисных приложений, смена хостинг-компании

(3) внедрение аутентификации, проверки контактных данных пользователей

38. Принципом информационной безопасности является принцип недопущения:

(1) неоправданных ограничений при работе в сети (системе)

(2) рисков безопасности сети, системы

(3) презумпции секретности

39. Принципом политики информационной безопасности является принцип:

(1) невозможности миновать защитные средства сети (системы)

(2) усиления основного звена сети, системы

(3) полного блокирования доступа при риск-ситуациях

40. Принципом политики информационной безопасности является принцип:

(1) усиления защищенности самого незащищенного звена сети (системы)

(2) перехода в безопасное состояние работы сети, системы

(3) полного доступа пользователей ко всем ресурсам сети, системы

41. Принципом политики информационной безопасности является принцип:

(1) разделения доступа (обязанностей, привилегий) клиентам сети (системы)

(2) одноуровневой защиты сети, системы

(3) совместимых, однотипных программно-технических средств сети, системы

42. К основным типам средств воздействия на компьютерную сеть относится:

(1) компьютерный сбой

(2) логические закладки («мины»)

(3) аварийное отключение питания

43. Когда получен спам по e-mail с приложенным файлом, следует:

(1) прочитать приложение, если оно не содержит ничего ценного – удалить

(2) сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

(3) удалить письмо с приложением, не раскрывая (не читая) его

44. Принцип Кирхгофа:

(1) секретность ключа определена секретностью открытого сообщения

(2) секретность информации определена скоростью передачи данных

(3) секретность закрытого сообщения определяется секретностью ключа

45. ЭЦП – это:

(1) электронно-цифровой преобразователь

(2) электронно-цифровая подпись

(3) электронно-цифровой процессор

46. Наиболее распространены угрозы информационной безопасности корпоративной системы:

(1) покупка нелицензионного ПО

(2) ошибки эксплуатации и неумышленного изменения режима работы системы

(3) сознательного внедрения сетевых вирусов

47. Наиболее распространены угрозы информационной безопасности сети:

(1) распределенный доступ клиент, отказ оборудования

(2) моральный износ сети, инсайдерство

(3) сбой (отказ) оборудования, нелегальное копирование данных

48. Наиболее распространены средства воздействия на сеть офиса:

(1) слабый трафик, информационный обман, вирусы в интернет

(2) вирусы в сети, логические мины (закладки), информационный перехват

(3) компьютерные сбои, изменение администрирования, топологии

49. Утечкой информации в системе называется ситуация, характеризуемая:

(1) потерей данных в системе

(2) изменением формы информации

(3) изменением содержания информации

50. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

(1) целостность

(2) доступность

(3) актуальность

51. Угроза информационной системе (компьютерной сети) – это:

(1) вероятное событие

(2) детерминированное (всегда определенное) событие

(3) событие, происходящее периодически

52. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

(1) регламентированной

(2) правовой

(3) защищаемой

53. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

(1) программные, технические, организационные, технологические

(2) серверные, клиентские, спутниковые, наземные

(3) личные, корпоративные, социальные, национальные

54. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

(1) владелец сети

(2) администратор сети

(3) пользователь сети

55. Политика безопасности в системе (сети) – это комплекс:

(1) руководств, требований обеспечения необходимого уровня безопасности

(2) инструкций, алгоритмов поведения пользователя в сети

(3) нормы информационного права, соблюдаемые в сети

56. Наиболее важным при реализации защитных мер политики безопасности является:

(1) аудит, анализ затрат на проведение защитных мер

(2) аудит, анализ безопасности

(3) аудит, анализ уязвимостей, риск-ситуаций

57. Что такое компьютерный вирус?

(1) прикладная программа

(2) системная программа

(3) программа, выполняющая на компьютере несанкционированные действия

(4) база данных.

58. Основные типы компьютерных вирусов:

(1) аппаратные, программные, загрузочные

(2) программные, загрузочные, макровирусы

(3) файловые, программные, макровирусы

59. Этапы действия программного вируса:

(1) размножение, вирусная атака

(2) запись в файл, размножение

(3) запись в файл, размножение, уничтожение программы

60. В чем заключается размножение программного вируса?

(1) программа-вирус один раз копируется в теле другой программы

(2) вирусный код неоднократно копируется в теле другой программы

61. Что называется вирусной атакой?

(1) неоднократное копирование кода вируса в код программы

(2) отключение компьютера в результате попадания вируса

(3) нарушение работы программы, уничтожение данных, форматирование жесткого диска

62. Какие существуют методы реализации антивирусной защиты?

(1) аппаратные и программные

(2) программные и административные

(3) только программные

63. Какие существуют основные средства защиты данных?

(1) резервное копирование наиболее ценных данных

(2) аппаратные средства

(3) программные средства

64. Какие существуют вспомогательные средства защиты?

(1) аппаратные средства

(2) программные средства

(3) административные методы и антивирусные программы

65. На чем основано действие антивирусной программы?

(1) на ожидании начала вирусной атаки

(2) на сравнении программных кодов с известными вирусами

(3) на удалении зараженных файлов

66. Какие программы относятся к антивирусным:

(1) AVP, DrWeb, Norton AntiVirus

(2) MS-DOS, MS Word, AVP

(3) MS Word, MS Excel, Norton Commander

67. Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами:

(1) руткит

(2) бэкап

(3) камбэк

68. Компьютерные вирусы:

(1) файлы, которые невозможно удалить

(2) программы, способные к саморазмножению (самокопированию)

(3) файлы, имеющие определенное расширение

69. DDos — программы:

(1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

(2) оба варианта верны

(3) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

70. Отличительными способностями компьютерного вируса являются:

(1) способность к самостоятельному запуску и многократному копированию кода

(2) значительный объем программного кода

(3) легкость распознавания

71. DoS — программы:

(1) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

(2) оба варианта верны

(3) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера

72. Компьютерные вирусы:

(1) являются следствием ошибок в операционной системе

(2) пишутся людьми специально для нанесения ущерба пользователем ПК

(3) возникают в связи со сбоями в аппаратных средствах компьютера

73. Троянские программы бывают:

(1) сетевые программы

(2) программы передачи данных

(3) программы – шпионы

74. Основная масса угроз информационной безопасности приходится на:

(1) троянские программы

(2) шпионские программы

(3) черви

75. Троянская программа, троянец:

(1) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей

(2) являются вредоносными программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы

(3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам

76. Информационная безопасность зависит от:

(1) компьютеров, поддерживающей инфраструктуры

(2) пользователей

(3) информации

77. Сетевые черви бывают:

(1) Web-черви

(2) черви операционной системы

(3) черви MS Office

78. Таргетированная атака – это:

(1) атака на сетевое оборудование

(2) атака на компьютерную систему крупного предприятия

(3) атака на конкретный компьютер пользователя

79. Сетевые черви бывают:

(1) почтовые черви

(2) черви операционной системы

(3) черви MS Office

80. Stuxnet – это:

(1) троянская программа

(2) макровирус

(3) промышленный вирус

81. По «среде обитания» вирусы можно разделить на:

(1) загрузочные

(2) очень опасные

(3) опасные

82. Какие вирусы активизируются в самом начале работы с операционной системой:

(1) загрузочные вирусы

(2) троянцы

(3) черви

83. По «среде обитания» вирусы можно разделить на:

(1) не опасные

(2) очень опасные

(3) файловые

84. Какие угрозы безопасности данных являются преднамеренными:

(1) ошибки персонала

(2) открытие электронного письма, содержащего вирус

(3) не авторизованный доступ

85. По «среде обитания» вирусы можно разделить на:

(1) опасные

(2) не опасные

(3) макровирусы

86. Под какие системы распространение вирусов происходит наиболее динамично:

(1) Windows

(2) Mac OS

(3) Android

87. Макровирусы:

(1) существуют для интегрированного офисного приложения Microsoft Office

(2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске

(3) заражают загрузочный сектор гибкого или жёсткого диска

88. Какой вид идентификации и аутентификации получил наибольшее распространение:

(1) системы PKI

(2) постоянные пароли

(3) одноразовые пароли

89. Файловые вирусы:

(1) заражают загрузочный сектор гибкого или жёсткого диска

(2) существуют для интегрированного офисного приложения Microsoft Office

(3) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске

90. Для периодической проверки компьютера на наличие вирусов используется:

(1) компиляция

(2) антивирусное сканирование

(3) дефрагментация диска

91. Антивирусный сканер запускается:

(1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия

(2) оба варианта верны

(3) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера

92. Как называется вирус, попадающий на компьютер при работе с электронной почтой:

(1) текстовый

(2) сетевой

(3) файловый

93. Антивирусный монитор запускается:

(1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера

(2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютер

(3) оба варианта верны

94. К категории компьютерных вирусов не относятся:

(1) загрузочные вирусы

(2) файловые вирусы

(3) type-вирусы

95. Выберите тип вредоносных программ:

(1) шпионское, рекламное программное обеспечение

(2) Microsoft Office

(3) операционная система Linux

96. Выберите тип вредоносных программ:

(1) Microsoft Office

(2) вирусы, черви, троянские и хакерские программы

(3) операционная система Windows

97. Как называют схему страницы, на которой представлены элементы, имеющиеся на страницах сайта:

(1) матрица

(2) шаблон

(3) фундамент

98. Чтобы отличать теги от текста, их заключают в:

(1) круглые скобки

(2) угловые скобки

(3) фигурные скобки

99. Проектированием структуры web-сайта занимается:

(1) web-программист

(2) провайдер

(3) web-дизайнер

100. Сайт можно создать, воспользовавшись:

(1) языком программирования Си

(2) языком программирования Паскаль

(3) языком разметки гипертекста HTML

Задания в открытой форме

1) В настоящее время угрозы и вредоносный код разрабатываются с целью – ……..….

2) Основным средством предотвращения утечек из корпоративных информационных систем являются – ……..…

3) Что такое неотчуждаемый аутентифицирующий признак - ……..…

4) Это процесс формирования кадра из данных прикладного уровня ……...

5) VPN работают на уровне модели OSI на ……

6) … – уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

7) … – разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

8) … – программные средства контроля доступа в систему, используемые для защиты уязвимой информации и программных средств.

9) … – процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

10) … – процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

11) … – предоставление определенному лицу или группе лиц прав на выполнение определенных действий.
12) … – всестороннее обследова-ние, позволяющее оценить текущее состояние информационной безопасно-сти организации и спланировать дальнейшие шаги по повышению уровня защищенности.
13) … – основная функция систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находя-щимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.
14) … – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.
15) … – компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.
16) … – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.
17) … – вторжение в операционную систему удаленного компьютера.
18) … – степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации.
19) … – возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.
20) … – стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере.
21) … – отключения ответа в беспроводных точках доступа на широковещательный запрос ESSID (Broadcast ESSID) позволяет предотвратить сканирование беспроводной сети злоумышленником.

Задание на установление соответствия

1. Установите соответствие между названием и описанием

1	Сервер	А	согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
2	Рабочая станция	Б	специальный компьютер, который предназначен для удаленного запуска

			приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
3	Сетевая технология	В	это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею
4	Информационно-коммуникационная технология	Г	это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами

2. Установите соответствие между названием и описанием

1	Локальная сеть	А	объединение компьютеров, расположенных на большом расстоянии друг от друга
2	Региональная сеть	Б	объединение локальных сетей в пределах одной корпорации для решения общих задач
3	Корпоративная сеть	В	объединение компьютеров в пределах одного города, области, страны
4	Глобальная сеть	Г	объединение компьютеров, расположенных на небольшом расстоянии друг от друга

3. Установите соответствие между названием и описанием

1	Прикладной уровень	А	Отвечает за поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время
2	Уровень представления	Б	Верхний (7-й) уровень модели, обеспечивает взаимодействие сети и пользователя.
3	Сеансовый уровень	В	4-й уровень модели, предназначен для доставки данных без ошибок, потерь и дублирования в той последовательности, как они были переданы.
4	Транспортный уровень	Г	Этот уровень отвечает за преобразование протоколов и кодирование/декодирование данных

4. Установите соответствие между названием и описанием

1	Сетевой уровень	А	Этот уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и контроле за ошибками, которые могут возникнуть.

2	Канальный уровень	Б	3-й уровень сетевой модели OSI, предназначен для определения пути передачи данных
3	Физический уровень	В	Самый нижний уровень модели, предназначен непосредственно для передачи потока данных.

5. Установите соответствие между названием и описанием

1	TCP	А	используется либо при пересылке коротких сообщений, когда накладные расходы на установление сеанса и проверку успешной доставки данных оказываются выше расходов на повторную (в случае неудачи) пересылку сообщения
2	UDP	Б	это транспортный механизм, предоставляющий поток данных, с предварительной установкой соединения, за счёт этого дающий уверенность в безошибочности получаемых данных, осуществляет повторный запрос данных в случае потери пакетов и устраняет дублирование при получении двух копий одного пакета
3	Порт	В	параметр протоколов TCP и UDP, определяющий пункт назначения для данных, принимаемых по сети

6. Соответствие комбинаций клавиш, действиям в приложении ВМ VirtualBox

1	RCTRL	А	Осуществить сброс
2	RCTRL+DEL	Б	Переслать ВМ сигнал нажатия клавиш CTRL+ALT+DEL
3	RCTRL+R	В	Перейти в хостовый компьютер

7. Установите соответствие между названием и описанием

1	WinPCAP	А	средство ограничения объемов потребления процессорного времени.
2	Многозадачные ОС	Б	среда моделирования ЭВМ.
3	Dynamips	В	средство ограничения объемов потребления процессорного времени.
4	Cpulimit	Г	поддерживают одновременную работу на ЭВМ нескольких пользователей за различными терминалами
5	VirtualBox	Д	графический анализатор сетевого трафика. Позволяет наглядно отобразить подробнейшую информацию о сетевом трафике.

8. Установите соответствие между названием и описанием

1	Канал связи	А	это путь для передачи данных от одной системы к другой
2	Логический канал	Б	это поток сообщений в сети передачи данных
3	Трафик	В	путь или средство, по которому передаются сигналы

9. Установите соответствие между названием и описанием

1	Общий ресурс	А	логическое объединение компьютеров. Как правило, объединение в группы используется для упрощения администрирования сети. При этом несколько компьютеров выступают как единое целое – группа
2	Рабочая станция	Б	это специализированный компьютер, предоставляющий свои ресурсы в использование клиентам сети (как правило, это рабочие станции) и управляющий сетью
3	Сервер	В	это объект (папка, диск, принтер и др.) который могут использовать несколько пользователей одновременно, причем им не обязательно находится за тем компьютером, на котором физически расположен данный ресурс
4	Рабочая группа	Г	это компьютер, подключенный к сети и предназначенный для выполнения задач пользователя

10. Установите соответствие между описанием и названием

1	Коммутация с промежуточным хранением	А	Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.
2	Сквозная коммутация	Б	Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).
3	Бесфрагментная	В	Коммутатор читает всю информацию

	или гибридная коммутация		в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

11. Установите соответствие между названием и описанием

1	Сетевая плата	А	служит для подключения отдельно стоящей ВУ к ГВС.
2	Модем	Б	обеспечивает физическую связь нескольких ЛВС и маршрутизацию пакетов между ЛВС, а также поддержку различных технологий и топологий организации сети
3	Маршрутизатор	В	служит для подключения отдельно стоящей ВУ к ЛВС.
4	Периферийное оборудование	Г	это оборудование, расширяющее функциональные возможности ВУ

12. Установите соответствие между названием и описанием

1	Wireshark	А	системный драйвер и библиотека функций, позволяющая получить доступ к сетевым интерфейсам физического компьютера и передаваемой/получаемой информации по ним.
2	WinPCAP	Б	среда моделирования сетевых устройств, реализованных на базе процессоров с MIPS архитектурой.
3	SolarWinds Response	В	среда для анализа сетевого трафика. Используется для графического отображения информации.
4	SuperPUTTY	Г	система виртуальных терминалов. Позволяет подключаться к сетевым устройствам для управления ими.

13. Установите соответствие между командами linux и их описанием

1	man	А	Выводит краткое описание программы
2	whatis	Б	Показывает инструкцию к программам и командам Linux
3	whereis	В	Показывает к какому типу относится файл

4	file	Г	Показывает полный путь к исполняемому файлу и другим файлам программы

14. Установите соответствие между командами linux и их описанием

1	help	А	Команда показывает действительный идентификатор пользователя (UID)
2	whoami	Б	Вся необходимая информация о команде будет доступна
3	TAB	В	Это сочетание клавиш помогает запустить обратный поиск по всем параметрам, связанным с указанной командой
4	Ctrl + R	Г	Показывает варианты автозавершения команды

15. Установите соответствие между названием серверов и их описанием

1	Веб-сервер	А	программа, поддерживающая определенную сетевую логику в полноценном приложении
2	Сервер приложения	Б	компьютерная программа, нон-стоп обрабатывающая запросы пользователей и показывающая им HTML-страницы. Проще говоря, это любое устройство, на базе которого работает сайт
3	Прокси-сервер	В	получает письма, отправляет и хранит их на встроенных жестких дисках
4	Почтовый	Г	шлюз между пользователем и ресурсом, к которому он пытается подключиться.

16. Установите соответствие между названием серверов и их описанием

1	Файловый	А	утилита-гипервизор, определяющая себя как отдельный компьютер, но таковой не являющаяся
2	Виртуальный	Б	хранилище любых документов, медиа-контента и всего, что можно хранить и чем можно делиться
3	Сервер сетевой политики	В	отвечает за безопасное хранение одной или нескольких баз данных.
4	Сервер баз данных (SQL)	Г	шлюз безопасности, через которой подключаются сотрудники одной компании, чтобы начальство могло контролировать их поведение в интернете,

			смотреть загружаемые файлы и тому подобное

17. Установите соответствие между названием и описанием

1	Управляемость	А	Срок жизни современных ИБП составляет 10–15 лет, если своевременно выполнять операцию подзарядки батарей
2	Масштабируемость	Б	с любой рабочей станции сети с помощью программы клиента можно наблюдать за состоянием ИБП и получать от него сигналы предупреждения
3	Долговечность	В	возможность увеличить мощность ИБП

18. Установите соответствие между названием и описанием

1	Информационно-вычислительная система	А	должностное лицо, ответственное за работоспособность и надлежащее функционирование всех частей ИВС.
2	Пользователь ИВС	Б	комплекс программных и аппаратных средств для обеспечения автоматизации производства и других сфер жизнедеятельности человека, включающий в качестве составных частей серверное и сетеобразующее оборудование.
3	Администратор ИВС	В	физическое лицо, имеющее доступ к определенным ресурсам ИВС, идентифицируемое бюджетом пользователя

19. Установите соответствие между названием и описанием

1	netstat -a	А	получение основной статистики по всем протоколам (ethernet, IPv4, IPv6, TCP, UDP).
2	netstat -n –b	Б	получение информации обо всех активных соединениях и процессах инициировавших их.
3	netstat -e -s	В	получение информации обо всех установленных соединениях и открытых на прослушивание портах.

20. Установите соответствие между протоколом и портом

1	HTTP	А	53

2	DHCP	Б	20
3	DNS	В	80
4	FTP	Г	67

Задания на установление правильной последовательности

1. Установить последовательность команд на маршрутизаторе, позволяющие выставить VLAN на интерфейсе.

1) int f1/1.

2) conf t.

3) switchport access vlan 3.

4) write memory.

5) exit, exit.

2. Установить этапы загрузки операционной системы:

1. Исполнение команд базовой системы ввода-вывода
2. Загрузка интерфейса ввода пароля
3. Формирование таблиц размещения данных в памяти
4. Чтение информации из главной загрузочной записи
5. Проверка аппаратной конфигурации

3. Установить последовательность определения Администратор сети-

1. для управления компьютерами
2. человек, обладающий всеми полномочиями
3. пользователями и ресурсами в сети

4. Установить последовательность определения Компьютерная сеть-

1. в сети без использования каких-либо
2. промежуточных носителей информации
3. беспечивающих информационный обмен между компьютерами
4. совокупность компьютеров и различных устройств

5. Установить последовательность команд на маршрутизаторе, что бы создать VLAN?

1. conf t
2. vlan database
3. vlan 3
4. write memory

6. Установите последовательность, чтобы сделать сетевые файлы или папки доступными при работе в автономном режиме

1. Установите флажок Создать на рабочем столе ярлык для папки с автономными файлами и нажмите кнопку Готово. Файлы копируются на компьютер, а на рабочем столе появляется папка «Ярлык к автономным файлам».

2. Щелкните правой кнопкой мышки нужный файл или папку и выберите пункт Создать доступной автономно. Откроется мастер автономных файлов. Нажмите кнопку Далее;

3. Откройте место на сетевом диске, которое содержит нужный файл или папку;

4. Установите флажок Автоматически синхронизировать автономные файлы при входе в систему и при выходе из нее и нажмите кнопку Далее;

7. Установите последовательность команд на роутере, чтобы выставить IP на интерфейсе?

1. cont t
2. ip address 1.0.0.0 255.0.0.0
3. interface f0/0
4. no shutdown
5. exit
6. write memory

8. Установите этапы процессной модели:

1. Проверка.
2. Планирование.
3. Реализация
4. Действие.

9. Установите последовательность

1. Тонкий клиент
2. Сервер баз данных
3. Сервер приложений

10. Установить этапы разработки:

1. Проектирование
2. Реализация
3. Внедрение
4. Анализ и планирование требований пользователей

11. Определить вариант организации локальной сети установить последовательность

1. Панель управления
2. Пуск
3. Центр управления сетями и общим доступом

12. Что нужно делать, для добавления ПК в GNS3?
1. Скачать образ операционной системы.
2. Создать виртуальную машину.
3. Установить ОС на виртуальную машину
4. В настройках GNS3 выбрать среду ЭВМ и выбрать путь к ней.
5. В настройках GNS3 выбрать нужную нам виртуальную машину.

13. Установите порядок от верхнего к нижнему уровней модели OSI
1. Прикладной
2. Презентационный
3. Сетевой
4. Сеансовый
5. Физический
6. Канальный
7. Транспортный

14. Перечисление типов VLAN, которые могут быть реализованы в коммутаторах в последовательности
1. на основе портов
2. на основе портов и протоколов IEEE 802.1v
3. на основе MAC-адресов
4. на основе стандарта IEEE 802.1Q
5. ассиметричные

15. ВС делятся на системы установить последовательность
1. распределенные
2. территориально-сосредоточенные
3. структурно-одноуровневые
4. многоуровневые

16. Установите последовательность вычислительной системы
1. По методам управления элементами ВС
2. По типу построения
3. По названию
4. По типу используемых ЭВМ или процессоров
5. По принципу закрепления вычислительных функций за отдельными ЭВМ
6. По степени территориальной разобщенности вычислительных модулей ВС

17.Последовательность слов для понятия Компьютерная сеть – это

1. Обеспечивающего передачу
2. Устройства связи
3. Связанных с помощью
4. Данных между ними
5. Группа компьютеров

18. Расположить параметры для группировки данных в журнале брандмауэра информации об атаке:
1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

19. Установите последовательность
1. Сервер баз данных
2. Тонкий клиент
3. Сервер приложений

20. Установить последовательность уровней
1. Канальный уровень
2. Сетевой уровень
3. Транспортный уровень
4. Физический уровень

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
Для адреса 198.146.70.176/19 найти следующее: сетевой адрес, широковещательный адрес, маску подсети.

Компетентностно-ориентированная задача № 2
Для адреса 60.190.185.79 с маской 255.255.248.0 определить максимальное количество возможных хостов.

Компетентностно-ориентированная задача № 3
Администратору поручено выбрать сеть, которая бы удовлетворяла следующим требованиям: Количество подсетей — не менее 27. Количество хостов в каждой подсети — не менее 200. Какую маску выберет администратор?

Компетентностно-ориентированная задача № 4
К какой сети принадлежит IP адрес 192.168.23.61/28

Компетентностно-ориентированная задача № 5
Адреса 34.23.89.190 и 34.23.101.190 принадлежат одной подсети. Определить минимально возможную подсеть для данных адресов, а также их маску.

Компетентностно-ориентированная задача № 6
Что такое ip-адрес, составьте схему из 2 ПК и роутера, проверьте работоспособность схемы, каждая часть схемы должна быть связанной друг с другом(пинговаться).

Компетентностно-ориентированная задача № 7
Что такое маска подсети, зачем она нужна, найти 2-ю и 4-ю подсети в классовой сети 175.100.0.0 при использовании маски 255.255.224.0.

Компетентностно-ориентированная задача № 8
Для адреса 52.92.25.205/19 найти следующее: Сетевой адрес, Широковещательный адрес, Маску подсети.

Компетентностно-ориентированная задача № 9
Даны адреса 23.149.22.3/28 и 23.149.55.1/26 с масками 255.255.255.240 и 255.255.255.192 соответственно. Вашей задачей является определить последние подсети при использовании указанных масок. Также определите следующие параметры этих найденных подсетей: сетевой адрес, широковещательный адрес, маску подсети, количество хостов в каждой подсети.

Компетентностно-ориентированная задача № 10
Найти общий суммаризированный адрес для адресов 187.63.224.12/21, 187.63.1.85/21, 187.63.131.100/22, 187.63.148.71/20.

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):

6-5 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.

4-3 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).

2-1 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.