СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08,2023 г.

УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И. В. Иванешко
«31» 08 2023 г.

Контрольно-оценочные средства для промежуточной аттестации по дисциплинам ОП.09 Информационные технологии, ОП.13 Основы информационной безопасности для специальности 11.02.18 Системы радиосвязи, мобильной связи и радиовещания

Комплексный дифференцированный зачет является промежуточной формой контроля, подводит итог освоения ОП.09 Информационные технологии и ОП.13 Основы информационной безопасности.

В результате освоения ОП.09 Информационные технологии и ОП.13 Основы информационной безопасности студент должен освоить следующие профессиональные компетенции:

ПК 2.3	Выполнять монтаж и первичную инсталляцию компьютерных сетей.
ПК 2.4	Инсталлировать и настраивать компьютерные платформы для организации услуг связи.
ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания.

А также общие компетенции:

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Результатом освоения ОП.09 Информационные технологии и ОП.13 Основы информационной безопасностиявляются освоенные умения и усвоенные знания.

В результате освоения ОП.09 Информационные технологии студент должен уметь:

У1 - обрабатывать текстовую и числовую информацию;

У2 - применять мультимедийные технологии обработки и представления информации;

У3 - обрабатывать экономическую и статистическую информацию, используя средства пакета прикладных программ.

У4 – применять информационные технологии в профессиональных задачах

В результате освоения ОП.09 Информационные технологии студент должен знать:

З1 - назначение и виды информационных технологий, технологии сбора, накопления, обработки, передачи и распространения информации;

З2 - состав, структуру, принципы реализации и функционирования информационных технологий;

З3 - базовые и прикладные информационные технологии;

З4 - инструментальные средства информационных технологий;

З5 – основные настройки информационных технологий.

В результате освоения ОП.13 Основы информационной безопасности студент должен уметь:

У1 - работать с различными операционными системами;

У2 - работать с протоколами доступа компьютерных сетей;

1

У3 - осуществлять конфигурирование сетей настраивать и осуществлять мониторинг локальных сетей;

У4 - подключать оборудование к точкам доступа;

У5 - производить настройку интеллектуальных параметров оборудования технологических мультисервисных сетей;

У6 -инсталлировать и настраивать компьютерные платформы для организации услуг связи;

У7 – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

У8 – определять оптимальные способы обеспечения информационной безопасности;

У8 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов.

В результате освоения ОП.13 Основы информационной безопасности студент должен знать:

З1 - принципы построения компьютерных сетей, топологические модели;

З2 - технологии с коммутацией пакетов, характеристики и функционирование локальных и глобальных (Интернет) вычислительных сетей, различных операционных систем;

З3 - конструктивное исполнения коммутаторов, маршрутизаторов и команд конфигурирования;

З4 - протоколы интеллектуальных функций коммутаторов 2-го и 3-го уровней;

З5- принципы организации передачи голоса и видеоинформации по сетям IP;

З6 - принципы построения сетей NGN, LTE, 5G;

З7 - возможности предоставления услуг связи средствами сетей высокоскоростного абонентского доступа;

З8 - действующие нормы на эксплуатационные показатели каналов и трактов;

З9 – принципы построения систем радиосвязи, мобильной связи и телерадиовещания;

З10 - международные стандарты информационной безопасности;

З11 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;

З12 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

З13 - классификацию угроз сетевой безопасности;

З14 - методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам.

Комплексный дифференцированный зачет по ОП.09 Информационные технологии, ОП.13 Основы информационной безопасности проводится в виде тестирования после того, как студентом выполнены и защищены все лабораторно-практические занятия.

На промежуточную аттестацию выделяется по 2 часа (последнее занятие в семестре) из общего количества часов на предмет.

Тест содержит 30 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока по 15 вопросов (первый блок – задания закрытого типа – 140 тестовых вопросов в совокупности по двум дисциплинам, второй блок – задания открытого типа – 105 теоретических вопросов с кратким ответом в совокупности по двум дисциплинам).

Время тестирования – 90 минут (по 2 минуты на каждый вопрос тестовых позиций и по 3 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 15 минут.

Критерии оценивания:

«5 баллов» - соответствует работа, содержащая 90-100% правильных ответов;

«4 балла» - соответствует работа, содержащая 70-89% правильных ответов;

«3 балла» - соответствует работа, содержащая 50-69% правильных ответов;

«2 балла» - соответствует работа, содержащая менее 50% правильных ответов.

Шкала оценивания образовательных результатов:

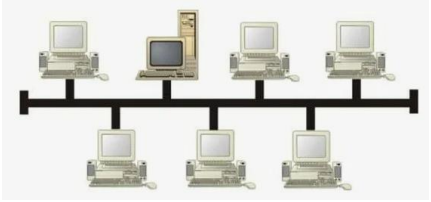
Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла

«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Блок заданий закрытого типа по ОП.09 Информационные технологии

Формируемые ОК 1-3, ОК 9, ПК 2.3 - 2.4

1) Какой кабель обеспечивает скорость передачи данных до 10Мбит/с?
   a. коаксиальный
   b. витая пара
   c. оптоволокно
   d. все вышеперечисленные
2) Какое определение для группы распространения из различных типов групп является верным?
   a. группа распространения назначает права доступа к ресурсам сети (администрирует)
   b. группа распространения не может заниматься администрированием, она занимается рассылкой сообщений группа
   c. распространения может содержать в себе пользователя любого домена, но администрировать эта группа может только в том домене, в котором группа создавалась
   d. группа распространения может содержать в себе пользователей из того домена, в котором она была создана, но администрировать они могут любой домен (если эти домены доверяют друг другу)
3) Какой из пользователей сервера имеет наибольшие права?
   a. системный администратор
   b. пользователь
   c. гость
   d. администратор
4) В чем заключается главная задача администрирования компьютерной сети?
   a. установка и настройка сети, поддержка ее дальнейшей работоспособности
   b. основной целью администрирования является приведение сети в соответствие с целями и задачами, для которых она предназначена
   c. создание и управление пользователями
   d. установка и конфигурация аппаратных устройств, установка программного обеспечения.
5) Что нужно иметь, чтобы соединить два компьютера по телефонным линиям?
   a. модем
   b. два модема
   c. телефон, модем и специальное ПО
   d. по модему на каждом компьютере и специальное ПО
6) Какие компоненты вычислительной сети необходимы для организации одноранговой локальной сети?
   a. модем, компьютер-сервер
   b. сетевая плата, сетевое ПО
   c. компьютер-сервер, рабочие станции
   d. линии связи, сетевая плата, сетевое ПО
7) Какая из приведенных схем соединения компьютеров представляет собой замкнутую цепочку?
   a. шина
   b. кольцо
   c. звезда
   d. полносвязная
8) Какая топология локальной сети представлена на картинке?



a. звезда
b. кольцо
c. линейная шина

9) Какой из перечисленных способов подключения к Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам?
   a. постоянное соединение по оптоволоконному каналу;
   b. удаленный доступ по телефонным каналам;
   c. постоянное соединение по выделенному каналу;
   d. терминальное соединение по коммутируемому телефонному каналу;
   e. временный доступ по телефонным каналам.
10) Какой минимальный набор средств необходимо иметь для подключения компьютера в уже существующую локальную сеть?
   a. модем, телефон и кабель
   b. звуковая карта и автоответчик
   c. сетевая карта, кабель
11) Как называется центральный компьютер, предоставляющий остальным компьютерам локальной сети сервисы и данные?
   a. рабочая станция
   b. последовательный порт связи
   c. сервер
12) Какой тип линий связи, используемых в глобальных сетях, менее надёжен?
   a. коммутируемые телефонные линии связи
   b. оптоволоконные линии связи
   c. цифровые линии связи
13) Чем оценивается качество передачи сигналов передачи данных?
   a. отсутствием искажения в принятой информации
   b. искажениями формы сигналов
   c. числом ошибок в принятой информации, т.е. верностью передачи
14) Какая топология компьютерной сети обладает самым высоким уровнем безопасности?
   a. Звезда
   b. Кольцо
   c. Шина
15) Для каких целей применяют коммутаторы или свитчи?
   a. для выбора маршрута
   b. для объединения компьютеров в единую сеть
   c. для усиления сигнала
16) Какие два типа линии связи существуют?
   a. Спутниковые и Глонасс
   b. Беспроводные и глобальные
   c. Беспроводные и проводные
17) У какой топологии компьютерной сети самый большой размер сети (до 20 км)?
   a. звезда
   b. шина
   c. кольцо
18) У какой топологии компьютерной сети самый маленький размер сети (до 200 м)?
   a. кольцо
   b. шина
   c. звезда
19) Сетевой администратор реализует политику, требующую надежных и сложных паролей. Какую цель защиты данных поддерживает эта политика?
   a. целостность данных

b. избыточность данных
c. конфиденциальность данных
d. качество данных

20) Компания обдумывает, использовать ли клиент/сервер или одноранговую сеть. Каковы три характеристики для одноранговой сети?
a. лучшая безопасность
b. лучшая производительность устройства при работе в качестве клиента и сервера
c. меньше затрат на внедрение
d. отсутствует централизованное администрирование
e. масштабируемость
f. легко создать

21) Какой термин описывает состояние сети, когда спрос на сетевые ресурсы превышает доступную мощность?
a. синхронизация
b. конвергенция
c. перегрузка
d. оптимизация

22) Какое устройство выполняет функцию определения пути, по которому сообщения должны проходить через объединенные сети?
a. маршрутизатор
b. брандмауэр
c. веб-сервер
d. DSL-модем

23) Какие два критерия используются для выбора сетевой среды из различных сетевых сред?
a. типы данных, которые должны быть приоритетными
b. расстояние, на которое выбранная среда может успешно передавать сигнал
c. оборудование, в которое будет установлена выбранная среда
d. количество промежуточных устройств, установленных в сети
e. стоимость конечных устройств, используемых в сети

24) Пользователь реализует безопасность в сети небольшого офиса. Какие два действия обеспечат минимальные требования безопасности для этой сети?
a. внедрение брандмауэра
b. установка антивирусного программного обеспечения
c. установка беспроводной сети
d. добавление специального устройства предотвращения вторжений
e. внедрение системы обнаружения вторжений

25) Какие два варианта подключения обеспечивают постоянное подключение к Интернету с высокой пропускной способностью для компьютеров в домашнем офисе?
a. сотовая связь
b. коммутируемая телефонная линия
c. DSL
d. спутниковый канал
e. кабель

26) Какие два варианта подключения к Интернету не требуют прокладки физических кабелей к зданию?
a. выделенная телефонная линия
b. DSL
c. сотовая связь
d. спутниковый канал
e. коммутируемая телефонная линия

27) Технический специалист добавляет новый ПК в локальную сеть. После распаковки компонентов и выполнения всех подключений техник запускает ПК. После загрузки ОС технический специалист открывает браузер и проверяет, может ли ПК подключиться к Интернету. Почему ПК смог подключиться к сети без дополнительной настройки?

a. ПК поставляется с предварительно настроенной информацией об IP-адресации на заводе
b. Виртуальный интерфейс ПК совместим с любой сетью
c. ПК использовал DNS для автоматического получения информации об IP-адресах с сервера
d. ПК был предварительно настроен на использование DHCP
e. ПК не требует никакой дополнительной информации для работы в сети

28) Сетевой администратор разрабатывает схему новой беспроводной сети. Какие три проблемы следует учитывать при построении беспроводной сети?
a. безопасность
b. помехи
c. коллизия пакетов
d. обширная кабельная разводка
e. зона покрытия
f. варианты мобильности

29) Как подразделяются компьютерные сети по территориальному охвату?
a. простые
b. локальные
c. глобальные
d. региональные
e. широкополосные

30) Каких двух видов бывают компьютерные сети по иерархической организации?
a. одноранговые
b. двухранговые
c. трехранговые
d. с выделенным сервером

31) По каким параметрам классифицируются компьютерные сети?
a. по территориальной распространенности;
b. по скорости передачи информации;
c. по типу среды передачи;
d. по способу организации взаимодействия;
e. по поддержки высокоуровневых сервисов

32) Как называется программно – аппаратный комплекс, соединяющий разнородные сети или сетевые устройства?
a. шлюз;
b. мост;
c. концентратор;
d. маршрутизатор;
e. коммутатор;
f. повторитель;
g. терминатор.

33) Как называется устройство сети, которое соединяет 2 отдельных сегмента и передает трафик между ними?
a. шлюз;
b. мост;
c. концентратор;
d. маршрутизатор;
e. коммутатор;
f. повторитель;
g. терминатор.

34) На чем основано действие антивирусной программы?
a. На удалении зараженных файлов;
b. На ожидании начала вирусной атаки;
c. На сравнении программных кодов с известными вирусами;
d. На определении заражённых файлов.

35) Что является компьютерным вирусом?
    a. Специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться";
    b. Программа проверки и лечения дисков;
    c. Любая программа, созданная на языках низкого уровня;
    d. Специальная программа для создания других программ.
36) Какой антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов?
    a. детектор;
    b. доктор;
    c. сканер;
    d. ревизор;
    e. сторож
37) Какой антивирус запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным?
    a. детектор;
    b. доктор;
    c. сканер;
    d. ревизор;
    e. сторож
38) Какими способами обеспечиваются основные уровни антивирусной защиты? (выберите три варианта)
    a. Поиск и уничтожение известных вирусов
    b. Поиск и уничтожение неизвестных вирусов
    c. Блокировка проявления вирусов
    d. Определения адреса отправителя вирусов
    e. Выявление создателей вирусов
39) Как может произойти заражение компьютерными вирусами?
    a. В процессе форматирования диска;
    b. В процессе работы с файлами;
    c. В процессе выключения компьютера;
    d. В процессе печати на принтере.
40) Какова схема работы компьютерных вирусов?
    a. заражение - размножение – атака
    b. размножение - заражение – атака
    c. атака - размножение – заражение
    d. размножение – заражение
41) Когда происходит заражение компьютерным вирусом?
    a. при загрузке операционной системы
    b. при включении питания
    c. при запуске инфицированной программы или при обращении к носителю, имеющему вредоносный код в системной области
    d. при загрузке непроверенного носителя информации
42) Какой антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние?
    a. детектор;
    b. доктор;
    c. сканер;
    d. ревизор;
    e. сторож
43) Как называется способ взаимодействия компьютеров и характер распространения сигналов по сети?
    a. физическая топология

b. логическая топология
c. сетевой протокол

44) На основе каких трех базовых топологий строятся сети?
a. шина
b. дерево
c. звезда
d. сеточная
e. гибридная
f. кольцо

45) Какая топология является самой распространенной в современных сетях?
a. шина
b. дерево
c. звезда

46) Что является основным недостатком топологии «шина»?
a. высокая стоимость сети
b. низкая надежность сети
c. большой расход кабеля
d. низкая помехозащищенность сети

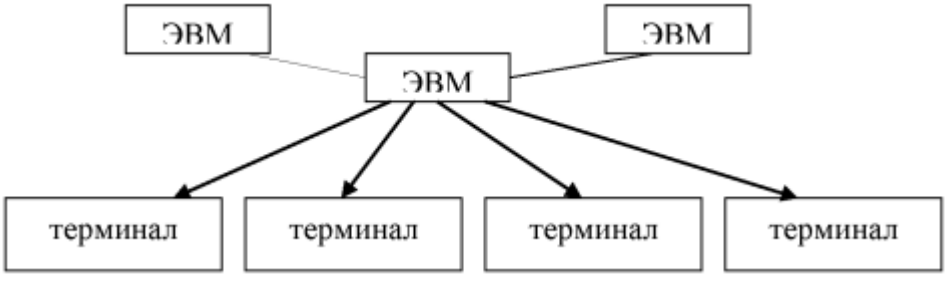
47) Что является основным недостатком топологии «кольцо»?
a. высокая стоимость сети
b. низкая надежность сети
c. большой расход кабеля
d. низкая помехозащищенность сети

48) Что является основным преимуществом топологии «звезда»?
a. низкая стоимость сети
b. малый расход кабеля
c. хорошая помехозащищенность сети
d. высокая надежность и управляемость сети

49) Какие характеристики используют для оценки качества сети?
a. скорость передачи данных по каналу связи
b. пропускную способность канала связи
c. достоверность передачи информации
d. время передачи

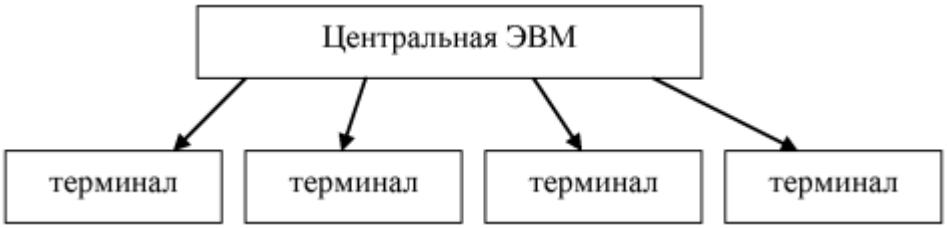
50) От каких параметров зависит скорость передачи данных?
a. типа канала связи
b. качества канала связи
c. типа используемых модемов
d. способа синхронизации

51) Какой принцип обработки данных изображен на рисунке?



a. Принцип централизованной обработки данных
b. Принцип распределенной обработки данных
c. Принцип центральной обработки данных
d. Принцип последовательной обработки данных

52) Какой принцип обработки данных изображен на рисунке?



a. Принцип централизованной обработки данных
b. Принцип центральной обработки данных
c. Принцип распределенной обработки данных
d. Принцип последовательной обработки данных

53) Что является главной составной частью системного программного обеспечения?
a. графический интерфейс
b. операционная система
c. операционная оболочка
d. система обслуживания

54) Для чего предназначено системное программное обеспечение?
a. для решения повседневных задач обработки информации
b. для эксплуатации и технического обслуживания ПК, управления и организации вычислительного процесса, для обработки информации
c. для разработки и эксплуатации программ на конкретном языке программирование.

55) Без какой части программного обеспечения пользователю было бы сложно работать с компьютером?
a. без сервисных программ
b. без операционной системы
c. без прикладного программного обеспечения

56) Для чего предназначена операционная система?
a. для организации взаимодействия пользователя с компьютером и выполнения всех других программ
b. для редактирования, сохранения текстовых документов
c. для монтажа видео, фото и звуковой информации
d. для вывода информации на экран или печатающее устройство

57) Где хранится операционная система?
a. на ВЗУ
b. в ОЗУ
c. в ПЗУ

58) Что не относится к системному программному обеспечению?
a. файловые менеджеры
b. операционная система
c. браузеры

59) Как называется совокупность программных средств, обеспечивающих совместную работу пользователя и аппаратных средств компьютера?
a. операционная система
b. компьютерная система
c. файловая система

60) Как называется комплекс программ, обеспечивающих совместное функционирование всех устройств компьютера и предоставляющих пользователю доступ к ресурсам компьютера?
a. Операционная система
b. Система управления
c. Сервисные программы

61) На какие три основных класса делится программное обеспечение?
a. системное, прикладное, инструментальное
b. операционное, системное, сервисное
c. системное, программное, прикладное

62) Какое высказывание о драйверах является правильным?

a. с их помощью осуществляется контроль за нормальным функционированием оборудования
b. обеспечивают диалог пользователя с компьютером на базе графического интерфейса
c. осуществляют сжатие программ и данных

63) Какую задачу не выполняет операционная система?
a. администрирование работы с файлами
b. поддержку работы аппаратного обеспечения компьютера
c. реализацию прикладного программного обеспечения

64) Для чего нужно инструментальное программное обеспечение?
a. для управления устройствами ввода и вывода компьютера
b. для разработки, корректировки или развития других прикладных или системных программ
c. решать какие-либо задачи в пределах данной проблемной области

65) Как называется утилита, обеспечивающая работу периферийных устройств?
a. драйвер
b. дефрагментатор
c. винчестер

	Блок заданий закрытого типа по ОП.13 Основы информационной безопасности Формируемые компетенции: ПК 3.1, ПК 3.2, ОК 01, ОК 02	
66.	Что такое информационная безопасность?	1.Состояние защищённости информационной среды. 2.Сохранность информационных ресурсов. 3.Защита конфиденциальности, целостности и доступности информации. 4.Все ответы не верны.
67.	Какие решения направлены на обеспечение информационной безопасности?	1.Высокопроизводительные системы защиты каналов. 2.Автоматизированные системы в защищенном исполнении. 3.Защита периметра информационной системы. 4.Все ответы верны.
68.	Что входит в комплексную систему защиты информации?	1. Средства управления учетными записями. 2. Средства управления событиями. 3. Средства защищенного доступа. 4. Средства контроля защищенности. 5. Средства разделения физической сети на несколько логических сетей.
69.	Что не относится к государственным органам РФ, контролирующим деятельность в области защиты информации?	1.Комитет Государственной думы по безопасности. 2.Совет безопасности России. 3.Федеральная служба по техническому и экспортному контролю. 4.Служба экономической безопасности.
70.	Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	1.Доступность 2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
71.	Что такое доступность информации?	1.Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия. 2.Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов. 3.Свойство системы, обеспечивать закрытый доступ к

		информации любых субъектов. 4.Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)
72.	Что такое целостность информации?	1.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 2.Свойство информации, заключающееся в возможности ее изменения любым субъектом 3.Свойство информации, заключающееся в возможности изменения только единственным пользователем 4.Свойство информации, заключающееся в ее существовании в виде единого набора файлов.
73.	Что такое конфиденциальность информации?	1.Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней. 2.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 3.Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора. 4.Свойство информации, заключающееся в ее шифровании. 5.Свойство информации, заключающееся в ее принадлежности к определенному набору.
74.	Какие документы относятся к актам федерального законодательства?	1.Международные стандарты. 2.Международные договоры РФ. 3.Приказы ФСБ. 4.Указы президента РФ.
75.	Что из перечисленного относится к угрозам информационной безопасности?	1.Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию. 2.Классификация информации. 3.Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.). 4.Сбои и отказы оборудования (технических средств) АС. 5.Ошибки эксплуатации. (пользователей, операторов и другого персонала). 6.Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов). 7.Последствия ошибок проектирования и разработки компонентов АС. (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.). 8.Иерархическое расположение данных.
76.	Какие угрозы безопасности информации являются преднамеренными?	1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты.

		7.Утрата паролей, ключей, пропусков. 8.Хищение носителей информации. 9.Незаконное получение паролей.
77.	Какие угрозы безопасности информации являются непреднамеренными?	1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты. 7.Утрата паролей, ключей, пропусков. 8.Хищение носителей информации.
78.	Что относится к правовым мерам защиты информации?	1.Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения. 2.Действия правоохранительных органов для защиты информационных ресурсов. 3.Организационно-административные меры для защиты информационных ресурсов. 4.Действия администраторов сети защиты информационных ресурсов.
79.	Какие принятыт виды правовой ответственности за нарушение законов в области информационной безопасности?	1.Уголовная 2.Административно-правовая. 3.Гражданско-правовая. 4.Дисциплинарная. 5.Материальная. 6.Условная. 7.Договорная.
80.	Что такое государственная тайна?	1.Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. 2.Сведения о состоянии окружающей среды. 3.Все сведения, которые хранятся в государственных базах данных. 4.Сведения о состоянии здоровья президента РФ. 5.Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне.
81.	Какие правовые документы решают вопросы информационной безопасности?	1.Уголовный кодекс РФ. 2.Конституция РФ. 3.Закон "Об информации, информатизации и защите информации". 4.Закон РФ "О государственной тайне". 5.Закон РФ "О коммерческой тайне". 6.Закон РФ "О лицензировании отдельных видов деятельности". 7.Закон РФ "Об образовании". 8.Закон РФ " Об электронной цифровой подписи ".
82.	Что относят к физическим средствам защиты информации?	1.Стены. 2. Заграждения. 3. Решетки. 4. Межсетевые экраны 5. Ударо- и взрывостойкое остекление. 6. Устройства хранения. 7. Замки (механические, электрические, электромеханические, гидравлические)
83.	Какую информацию запрещено относить к информации ограниченного доступа?	1.Информацию о чрезвычайных ситуациях. 2.Информацию о деятельности органов государственной власти.

		3.Документы открытых архивов и библиотек. 4.Все, перечисленное в остальных пунктах.
84.	Какой из перечисленных законодательных актов обладает наибольшей юридической силой в вопросах информационного права?	1.Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне". 2.ГК РФ. 3.Закон "Об информации, информатизации и защите информации". 4.Конституция РФ.
85.	Что понимается под средствами физического управления доступом?	1.Механические, электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации. 2.Силовые действия охраны организации против потенциальных нарушителей. 3.Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям. 4.Информационное обеспечение секретных задач.
86.	Какие задачи решает система физической защиты?	1. Предупреждение несанкционированного доступа, нерегламентированных воздействий. 2. Задержка нарушителей, их выявления на объекте. 3. Реагирование сотрудников службы безопасности. 4. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 5. Обеспечение целостности программно-аппаратной среды.
87.	Какие компоненты входят в комплекс защиты охраняемых объектов?	1. Сигнализация 2. Охрана 3. Датчики 4. Телевизионная система 5. Устройства несанкционированного доступа, нерегламентированных воздействий.
88.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1.Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 2.Обеспечение функций регистрации и учета событий безопасности. 3.Обеспечение неизменности (целостности) программно-аппаратной среды применяемых программных и программно-технических средств. 4. Задержка нарушителей, их выявление на объекте. 5. Реагирование сотрудников службы безопасности.
89.	Какие существуют виды угроз информационной безопасности (внешние и внутренние)?	1. Несанкционированный доступ 2. Угроза утечки информации 3. Мошенничество 4. Кибервойны и кибертерроризм 5. Угроза аутентификации пользователей. 6. Верификация.
90.	Какие из перечисленных средств относятся к средствам обнаружения угроз?	1. Охранная сигнализация. 2. Охранное телевидение. 3. Ударо- и взрывостойкое остекление. 4. Устройства хранения. 5. Электромеханические и гидравлические замки.
91.	Что из перечисленного является угрозами конфиденциальности информации?	1.Маскарад. 2.Карнавал. 3.Переадресовка. 4.Перехват данных. 5.Блокирование.

		6.Злоупотребления полномочиями.
92.	Что из перечисленного относится к инженерным средствам защиты?	1.Аутентификация. 2. Средства удаленного администрирования автоматизированных рабочих мест и серверов. 3.Ограждение периметра ПС и внутренних зон ограниченного доступа. 4. Контрольно-пропускные пункты (КПП) с соответствующим досмотровым оборудованием. 5. Въездные ворота, калитки, шлагбаумы.
93.	Какие существуют технические каналы утечки информации?	1.Визуально-оптические каналы утечки информации. 2.Акустические каналы утечки информации. 3.Электромагнитные каналы утечки информации (или каналы утечки информации по ПЭМИН). 4.Материально-вещественные каналы утечки информации. 5. Визуально-вещественные каналы утечкиинформации. 6. Все ответы верны.
94.	Для каких целей применяются средства активной защиты информации от утечки по каналам радиосвязи?	1. Для технического ограничения использования мобильных телефонов на контролируемых территориях. 2.Для защиты информации от утечки с использованием каналов сотовой связи (акустический и видеоконтроль, определение местоположения объекта, дистанционное управление различными устройствами). 3. Для защиты от утечки данных из-за несоблюдения режима коммерческой тайны.
95.	Какие функции безопасности применяются в архитектуре безопасности 4G LTE?	1.Безопасность сети доступа, для безопасного предоставления услуг пользователю; 2.Безопасность домена сети обслуживания, для безопасного обмена данными пользователя и сигнализации; 3.Безопасность домена пользователя, безопасный доступ к мобильному телефону (MS); 4.Безопасность домена приложений, установление безопасного подключения к уровню приложений. 5.Видимость и конфигурируемость безопасности, чтобы пользователи имели возможность проверять работоспособность функций безопасности. 6.Все ответы верны
96.	Как классифицируются технические каналы акустической (речевой) утечки информации в зависимости от физической природы возникновения информационных сигналов, среды их распространения?	1. Прямые акустические (воздушные). 2. Акустовибрационные. 3. Акустооптические (лазерные). 4. Акустоэлектрические. 5. Акустовизуальные. 6. Все ответы верны.
97.	Что из перечисленного является косвенными каналами утечки информации?	1.Пропажа, кража или утеря информационного накопителя, исследование неудаленной корзины. 2.Прослушивание, дистанционные снимки. 3.Перехват электромагнитных устройств. 4. Утечка данных из-за несоблюдения режима коммерческой тайны. 5.Непосредственное копирование данных.
98.	Что такое анализ защищенности ИТ-инфраструктуры?	1.Анализ защищенности – это неконтролируемое техническое воздействие, направленное на выявление минимального количества уязвимостей в исследуемой ИТ-инфраструктуре. 2.Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление максимального количества уязвимостей и недостатков в исследуемой ИТ-инфраструктуре.

		3.Анализ защищенности – это организационное воздействие, направленное на выявление потерь от угрозы информационной безопасности в исследуемой ИТ-инфраструктуре.
99.	Какие задачи решаются при проведении анализа защищенности?	1.Выполнение требований регуляторов. 2.Получение представления о текущем уровне защищенности системы. 3.Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты. 4.Получение подробной картины уязвимостей и недостатков исследуемой системы. 5.Все, перечисленное в остальных пунктах.
100.	Когда рекомендуется проводить работы по анализу защищенности?	1.При первичной установке информационной системы. 2.При публикации новой версии используемой ИС. 3.При внесении существенных изменений в систему или инфраструктуру. 4.По прошествии длительного периода времени с последней проверки. 5.Все, перечисленное в остальных пунктах.
101.	Какая угроза возникает всякий раз, когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу информационной системы?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Дезинформации. 5.Шпионажа.
102.	Какая угроза заключается в том, что информация становится известна неавторизованному пользователю?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Дезинформации. 5.Шпионажа.
103.	Какая угроза включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
104.	Сколько классов защищенности автоматизированных систем от несанкционированного доступа к информации выделено в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
105.	На сколько групп разделены классы автоматизированных систем согласно специфическим особенностям обработки информации в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 4 группы. 2. 7 групп. 3. 3 группы. 4. 2 группы. 5. 5 групп.
106.	К какой группе относятся АСОД, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.

107.	К какой группе относятся АСОД, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
108.	К какой группе относятся многопользовательские АСОД, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
109.	Зачем нужно шифрование радиосигналов?	1.Шифрование радиосигналов позволяет обеспечить конфиденциальность передаваемой информации. 2.Шифрование радиосигналов обеспечивает целостность передаваемой информации. 3.Шифрование радиосигналов позволяет достоверно установить идентичность отправителя и получателя информации. 4.Шифрование радиосигналов обеспечивает защиту от перехвата и вмешательства. 5.Все ответы верны
110.	Где применяется шифрование радиосвязи?	1.Военная связь 2.Коммерческая связь 3.Чрезвычайные ситуации 4.Государственная безопасность 5.Корпоративная безопасность 6.Все ответы верны
111.	Что такое имитостойкость?	1.Способность системы радиосвязи противостоять введению в нее неверной информации, а также навязыванию ложных рабочих режимов. 2.Способность системы радиосвязи противодействовать раскрытию злоумышленником смысла передаваемой информации. 3.Передача ложной информации, специально разработанной для введения злоумышленника в заблуждение, по каналам радиосвязи.
112.	Что из перечисленного является прямыми каналами утечки информации?	1. Прослушивание, дистанционные снимки. 2. Перехват электромагнитных устройств. 3. Человеческий фактор. 4. Утечка данных из-за несоблюдения режима коммерческой тайны. 5. Непосредственное копирование данных.
113.	Что такое криптостойкость?	1.Способность системы радиосвязи противостоять введению в нее неверной информации, а также навязыванию ложных рабочих режимов. 2.Способность системы радиосвязи противодействовать раскрытию злоумышленником смысла передаваемой информации. 3.Передача ложной информации, специально разработанной для введения злоумышленника в заблуждение, по каналам радиосвязи.
114.	Для чего нужна система контроля и управления доступом (СКУД)?	1.Контроль проникновения на охраняемую территорию лиц, цель которых нарушение нормальной работы организации путем саботажа или промышленный

		шпионаж. 2. Отслеживание количества людей, одновременно находящихся в помещении. 3.Учет рабочего времени персонала и фиксация опозданий, досрочных уходов с работы. 4.Организация пропускного режима, запрет доступа на охраняемую территорию посторонних лиц. 5.Все ответы верны.
115.	При каких режимах обработки информации средствами вычислительной техники возникают побочные электромагнитные излучения?	1. Вывод информации на экран монитора. 2. Ввод данных с клавиатуры. 3. Запись информации на накопители. 4. Чтение информации с накопителей. 5. Передача данных в каналы связи. 6. Вывод данных на периферийные печатные устройства - принтеры, плоттеры. 7. Запись данных от сканера на магнитный носитель. 8. Все ответы верны.
116.	Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	1. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ. 2. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС. 3. Перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ. 4. Съем информационных сигналов с линий электропитания ТСПИ. 5. Съем информационных сигналов с цепей заземления ТСПИ и ВТСС.
117.	Что из перечисленного относится к электрическим каналам утечки информации (КУИ)?	1.Съем наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников. 2. Съем информационных сигналов с линий электропитания ТСПИ. 3. Съем информационных сигналов с цепей заземления ТСПИ и ВТСС. 4. Съем информации путем установки в ТСПИ электронных устройств перехвата информации. 5. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ. 6. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС.
118.	Что из перечисленного является целями и задачами технической защиты информации?	1. Предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения. 2. Защита носителей информации от уничтожения в результате различных природных и техногенных воздействий. 3.Предотвращение утечки информации по различным техническим каналам. 4. Использование лицензионного ПО, или прошедших аттестацию программ по защите клиентов и личных данных. 5. Систематическое обновление программного обеспечения.
119.	Какие объекты относятся к критической информационной инфраструктуре (КИИ)?	1. Информационные системы. 2. Телекоммуникационные сети. 3. Автоматизированные системы управления технологическими процессами. 4. Все, перечисленное в остальных пунктах.
120.	Как называют единый территориально распределенный комплекс центров различного	1.Критическая информационная инфраструктура (КИИ). 2.Государственная система обнаружения, предупреждения и ликвидации последствий

	масштаба, обменивающихся информацией о кибератаках?	компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). 3.Межгосударственная нормативно-методическая комиссия (МНМК). 4.Система оперативно-розыскных мероприятий (СОРМ).
121.	Как называют документ, устанавливающий требования, спецификации, руководящие принципы, в соответствии с которыми могут использоваться материалы, процессы и услуги, которые подходят для этих целей?	1. Нормативно-методический документ. 2.Стандарт. 3.Руководящий документ. 4. Нормативно правовой акт.
122.	Какие из перечисленных функций являются основными функциями ФСТЭК?	1.Проведение единой технической политики и координация работ по защите информации 2.Организация и контроль над проведением работ по защите информации в организациях и учреждениях от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения. 3.Поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации. 4. Все, перечисленное в остальных пунктах.
123.	Что такое техническая защита информации?	1. Защита информации с помощью ее криптографического преобразования. 2.Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств. 3.Защита информации путем применения организационных мероприятий и средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
124.	Что такое физическая защита информации?	1. Защита информации с помощью ее криптографического преобразования. 2.Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств 3.Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
125.	Что такое криптографическая защита информации?	1. Защита информации с помощью ее криптографического преобразования. 2.Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств 3.Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
126.	Какие угрозы называют естественными угрозами безопасности информации?	1.Угрозы ИБ АС, вызванные деятельностью человека. 2.Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от

		человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, зависящими от человека.
127.	Какие угрозы называют искусственными угрозами безопасности информации?	1.Угрозы ИБ АС, вызванные деятельностью человека. 2.Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, независящими от человека.
128.	Что такое модель угроз информационной безопасности?	1. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 2. Описание существующих угроз ИБ, их актуальности, возможности реализации и последствий. 3.Угрозы ИБ АС, вызванные деятельностью человека.
129.	Что из перечисленного относится к угрозам для речевой информации?	1.Радиомикрофоны на основе мобильных телефонов 2.Средства негласной активации сотовых телефонов. 3.Телефонные перехватчики. 4.Диктофоны. 5.Все ответы верны
130.	Какие технические средства могут защитить от угрозы съема речевой информации с помощью радиомикрофона на основе мобильного телефона?	1.Индикаторы поля. 2.Акустические маскираторы. 3.Подавители систем сотовой связи. 4.Индикаторы инфракрасного излучения. 5.Виброакустические системы защиты.
131.	Какие технические средства могут защитить от угрозы съема речевой информации с помощью телефонных перехватчиков?	1.Индикаторы поля 2.Акустические маскираторы 3.Подавители систем сотовой связи 4.Скремблеры (шифраторы) 5.Маскираторы телефонных переговоров
132.	Какие виды средств защиты информации должны содержаться в информационных системах общего пользования?	1.СЗИ от неправомерных действий (в том числе средства криптографической защиты информации). 2.Средства обнаружения вредоносных программ (в том числе антивирусные средства). 3.Средства контроля доступа к информации (в том числе средства обнаружения компьютерных атак). 4.Средства фильтрации и блокирования сетевого трафика (в том числе средства межсетевого экранирования). 5. Все, перечисленное в остальных пунктах.
133.	Как условно разделяются ценные активы организации в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»?	1. Временные и финансовые. 2.Основные и вспомогательные. 3.Неопределенные и определенные.
134.	Что из перечисленного относится к основным активам организации?	1. Место функционирования организации - пределы контролируемой зоны, в которой функционирует информационная система. 2. Бизнес-процессы - совокупность различных видов деятельности, в результате которой создается услуга, представляющая интерес для потребителя. 3. Информация - сведения, являющиеся предметом собственности, подлежащие защите от нарушения конфиденциальности, целостности и доступности, в

		соответствии с требованиями правовых документов и требованиями владельца информации, вне зависимости от формы представления. 4.Сведения, компрометация которых никаким образом не повлияет на деятельность организации.
135.	Какие важные задачи решаются при создании системы физической защиты (СФЗ) объекта?	1.Установка режимов доступа, прием и обработка информации со считывателей. 2.Предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения активов организации. 3.Защита объекта от воздействия стихийных сил и прежде всего, пожара и воды.
136.	Какие мероприятия по управлению ИБ реализуют при размещении оборудования?	1.Оборудование необходимо размещать так, чтобы свести до минимума излишний доступ в места его расположения. 2.Средства обработки и хранения важной информации следует размещать так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием. 3.Должны быть сведены к минимуму риски потенциальных угроз ИБ, включая: воровство; пожар; взрыв; задымление; затопление; пыль; вибрацию; химические эффекты; помехи в электроснабжении; электромагнитное излучение. 4. Все ответы верны.
137.	Что из перечисленного относится к техническим средствам защиты от угроз конфиденциальности речевой информации?	1. Индикатор поля. 2.Инфракрасный микрофон 3. Акустическиймаскиратор. 4. Акустический сейф. 5. Индикатор электрических сигналов.
138.	Что из перечисленного относится к техническим средствам защиты от угроз конфиденциальности речевой информации?	1.Радиомикрофон на основе мобильного телефона. 2. Индикатор инфракрасного излучения. 3. Виброакустическая система защиты. 4. Скремблер (шифратор).
139.	Что из перечисленного НЕ относится к техническим средствам защиты от угроз конфиденциальности речевой информации?	1.Подавитель систем сотовой связи. 2.Маскиратор телефонных переговоров 3. Лазерный стетоскоп. 4. Инфракрасный микрофон.
140.	Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Какие мероприятия по управлению ИБ следует применять в этом случае?	1.Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать защищенным образом. 2.Использовать стандартные функции удаления. 3.Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного ПО. 4.Проводить оценку риской в отношении носителей данных, содержащих важную информацию, с целью определения целесообразности их разрушения, восстановления или выбраковки.

Блок заданий открытого типа по ОП.09 Информационные технологии
Формируемые ОК 1-3, ОК 9, ПК 2.3-2.4

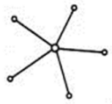
1. Как называется сеть, которая объединяет компьютеры, установленные в одном помещении или одном здании?

2. Как называется совокупность компьютеров и различных устройств, обеспечивающих информационный обмен между компьютерами в сети без использования каких-либо

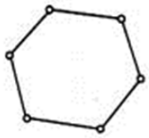
промежуточных носителей информации?

3. Какая топология локальной сети представлена на картинке?

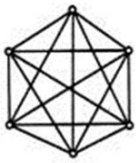
4. Как называются вирусы, способные обитать в файлах документов?
5. Как называется специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью "размножаться"?
6. Как называются вирусы, располагающиеся в служебных секторах носителей данных и поступающие в оперативную память только при загрузке компьютера?
7. Какая топология компьютерной сети изображена на рисунке?



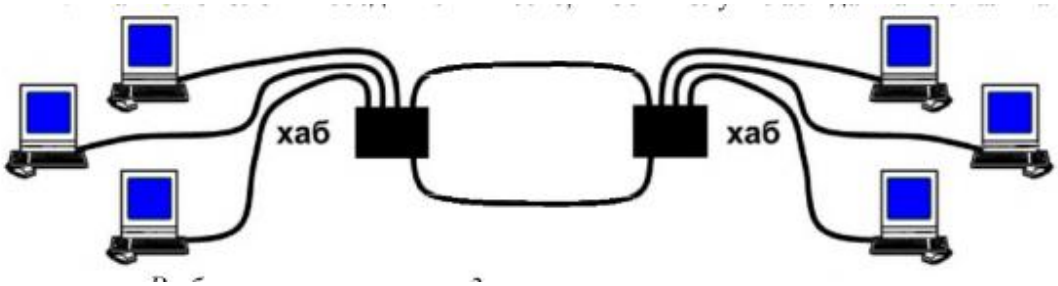
8. Какая топология компьютерной сети изображена на рисунке?



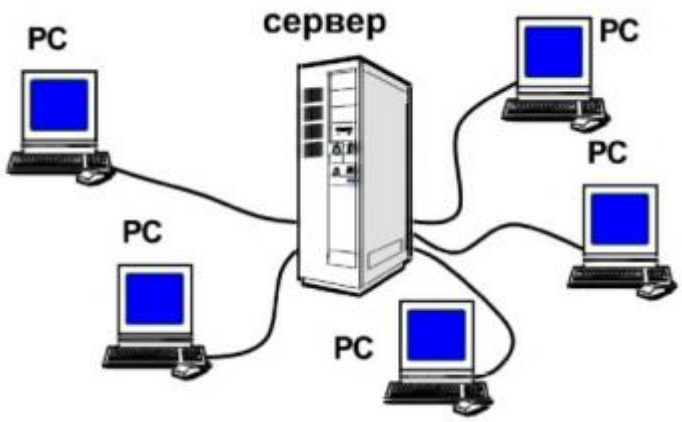
9. Какая топология компьютерной сети изображена на рисунке?



10. Какие топологии соединили вместе, чтобы получилась данная локальная сеть?

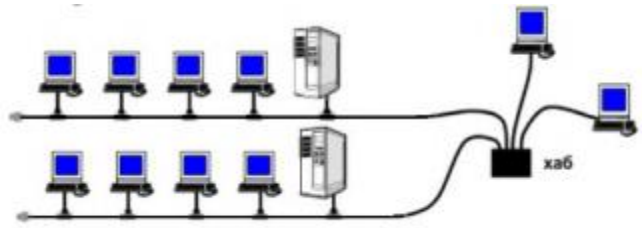


11. К какой топологии локальных сетей можно отнести данную компьютерную сеть?



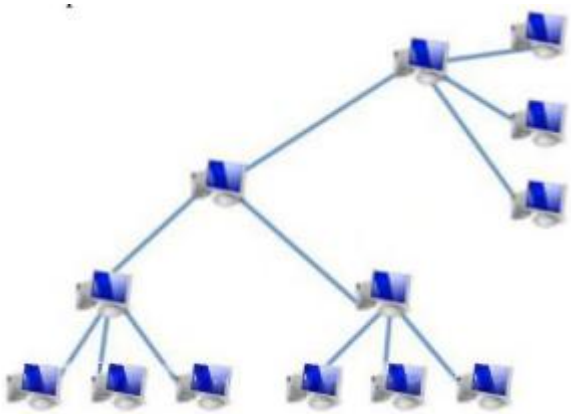
12. Укажите, какое устройство изображено на рисунке?

13. Какие топологии соединили вместе, чтобы получилась данная локальная сеть?

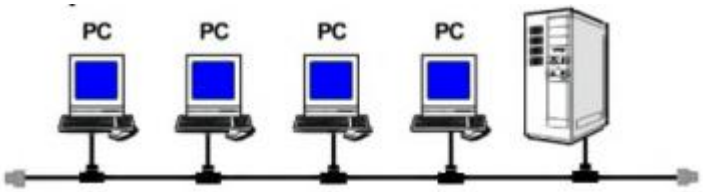


14. Как называется компьютер, который использует ресурсы сервера?

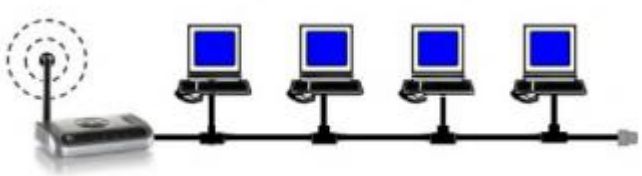
15. Какие две топологии использовались для построения локальной сети "снежинка", изображенной на рисунке?



16. Какая архитектура локальных сетей изображена на рисунке?



17. С помощью какой технологии. представленной на рисунке, выполнено подключение в данной локальной сети?



18. Как называется программно – аппаратный комплекс, соединяющий разнородные сети или сетевые устройства?

19. Как называется устройство сети, которое соединяет 2 отдельных сегмента и передает трафик между ними?

20. Как называется способ взаимодействия компьютеров и характер распространения сигналов по сети?

21. Без какой части программного обеспечения пользователю было бы сложно работать с компьютером?

22. Как называется совокупность программных средств, обеспечивающих совместную работу пользователя и аппаратных средств компьютера?

23. Как называется утилита, обеспечивающая работу периферийных устройств?

24. Какой компонент маршрутизатора имеет такие характеристики: держит операционную систему и микрокод, сохраняет свое содержимое при отключении питания или перезапуске и позволяет обновлять программное обеспечение без замены микросхем?

25. Что можно сделать, если размеры здания превышают установленную максимальную длину кабеля?

26. Какое сетевое устройство способно решить проблему чрезмерного широковещательного трафика?

27. Как называется устройство, которое сравнивает информацию из таблицы маршрутизации с IP-адресом пункта назначения, содержащимся в пакете данных, и переправляет пакет в нужную подсеть и узел?

28. Для чего используются межсетевые устройства?

29. Какое устройство принимает решение о дальнейшем перемещении пакета, выходит из информации о доступности канала и степенях его загрузки?

30. Какая характеристика кабелей имеют наибольшее значение для защиты передаваемой по нему информации от влияния внешнего электромагнитного излучения и снижения излучения самого кабеля?

Блок заданий открытого типа по ОП.13 Основы информационной безопасности
Формируемые компетенции: ПК 3.1, ПК 3.2, ОК 01, ОК 02

1. Какие компоненты входят в комплекс защиты охраняемых объектов?
2. Как определить класс защищенности системы?
3. Какие существуют виды инженерно-технических средств безопасности?
4. Какие существуют возможные способы организации утечки информации?
5.Что такое технические каналы утечки информации (ТКУИ)?
6. Каким образом классифицируются каналы утечки информации?
7.Что входит в структуру канала утечки информации?
8. Что такое конфиденциальность информации?
9. Что такое целостность информации?
10. Что такое доступность информации?
11. В чем заключается угроза раскрытия информации?
12. В чем заключается угроза целостности?
13. Когда возникает угроза отказа служб?
14. Что понимают под контролируемой зоной?
15. Что такое злонамеренные радиоэлектронные средства (ЗРЭС)?
16. Что называется каналом радиосвязи?
17. Какие бывают каналы связи?
18.Для каких целей предназначены системы радиосвязи?
19. Что понимают под термином «средство негласной активации сотового телефона»?
20. Что такое инфракрасный микрофон?
21. Как называют техническое средство, перехватывающее не акустическую, а вибрационную информацию (звуковые колебания, распространяющиеся по элементам конструкции здания)?
22.Как работает лазерный стетоскоп?
23. Какая деятельность называется защитой информации?
24. Как называется защита информации, заключающаяся в обеспечении безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств?
25.Как называется защита информации,применяющая организационные мероприятияи средства, создающие препятствия для проникновения неуполномоченных физических лиц к объекту защиты?
26.Что называют естественными угрозами безопасности информации?
27.Что называют искусственными угрозами безопасности информации?

28. Что понимают под моделью угроз информационной безопасности?
29. При построении модели угроз безопасности часто используют банк данных угроз безопасности информации ФСТЭК России. Где находится эта электронная база?
30. Какая структура определяет порядок и координирует действия обеспечения некриптографическими методами ИБ?
31. Какая структура определяет порядок и координирует действия обеспечения криптографическими методами ИБ?
32. Как называется совокупность требований в части защиты СВТ и АС?
33. Какие технические средства применяют для выявления радиозакладных устройств (РЗУ)?
34.Сколько определено ФСТЭК классов защищенности автоматизированных систем?
35. Как работает скремблер?
36.Что такое закладные устройства?
37. Что понимают под политикой информационной безопасности оператора связи?
38. Какой вид передачи информации называют радиосвязью?
39. Что понимают под радиовещанием?
40. Как называют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
41. Какую информацию о человеке можно отнести к персональным данным?
42.Что такое модель нарушителя информационной безопасности?
43.С какой целью проводится анализ защищенности?
44.Какой способ защиты информации заключается в создании на пути распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры?
45.Какой способ защиты информации предполагает преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется?
46.К каким способам защиты информации относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы?
47.К какому способу защиты информации относится разработка таких правил обращения с конфиденциальной информацией, которые позволили бы максимально затруднить получение этой информации злоумышленником?
48.Как называется способ защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности?
49. Что такое система виброакустической защиты?
50.Какие средства защиты информации относятся к формальным средствам?
51.Какие средства защиты информации относятся к неформальным средствам?
52. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, создающие препятствия на пути дестабилизирующих факторов?
53.К каким средствам защиты относятся различные электронные и электронно-механические устройства, встраиваемые в аппаратуру системы обработки данных, для решения задач защиты информации?
54.Какие средства защиты объединены в класс технических средств защиты информации?
55.К каким средствам защиты относятся специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем, с целью решении задач защиты информации?
56.К каким средствам защиты относятся организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей?
57. Для каких целей применяют индикатор поля?
58 Для каких целей применяют детектор радиоизлучающих устройств?
59. Для каких целей используют блокиратор сотовых телефонов?
60. Для каких целей используют индикатор электрических сигналов?
61.Какие средства защиты используются для проведения анализа защищенности?

62. Какова основная цель проведения анализа защищенности?
63.Зачем нужно проводить тестирование напроникновение (пентест) в рамках инструментального анализа защищенности?
64. По каким сценариям проводят тестирование на проникновение?
65.Что содержит реестр идентификации оборудования EIR?
66. Какие списки формирует реестр идентификации оборудования EIR?
67.Где производится аутентификация абонента, а точнее - SIM?
68.На какие группы подразделяются категории обрабатываемых персональных данных?
69.Как называют совокупность средств контроля и управления физическим доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью?
70. Что такое периметр безопасности?
71. Какой регулятор ИБ осуществляет организацию и контроль над проведением работ по защите информации от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами?
72. Какой регулятор ИБ осуществляет поддержание и развитие сегмента международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации?
73. Как называется единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?
74. Что входит в состав объектов критической информационной инфраструктуры?
75.Как называют сотрудников, которым доступна конфиденциальная информация организации, где они работают и которые могут использовать секреты в корыстных целях, провоцируя умышленные утечки информации?

Составили: преподаватели Грубник Е.М., Шаманова О.О.