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

Системы охраны и инженерной защиты информации
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, направленность (профиль) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Тема 1. Системы охраны и инженерной защиты информации

1. Меры информационной безопасности направлены на защиту
2. Что такое защита информации
3. Что понимается под информационной безопасностью

Тема 2. Угрозы информационной безопасности информации и объекты защиты

1. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?
2. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?
3. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно?
4. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

Тема 3. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков

1. Что надо определить перед выбором мер защиты информации?
2. Что такое демаскирующие признаки
3. Что называют прямыми демаскирующими признаками
4. Что называют косвенными демаскирующими признаками

Тема 4. Источники и носители информации

1. Что такое носитель информации?
2. Назовите основной носитель информации
3. Контейнер для файлов
4. Какая память содержит все знания, которые накопили люди за время своего существования и которыми могут воспользоваться ныне живущие люди

Тема 5. Принципы и способы добывания информации

1. Информацию, достаточную для решения поставленной задачи называют
2. Компьютер, рассматриваемый как универсальное обрабатывающее информацию устройство

3. Единицей измерения количества информации принято считать

Тема 6. Основы противодействия техническим средствам разведки

1. Какой государственный орган занимается рассмотрением и подготовкой законопроектов по вопросам безопасности государства и граждан?
2. Как называется основной орган внешней разведки Российской Федерации?
3. В каком документе описаны основные цели, функции и задачи ФСБ России?
4. Какой орган исполнительной власти осуществляет сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

Тема 7. Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы)

1. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?
2. В каком техническом канале утечки информации в качестве носителей используются фотоны?
3. В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?
4. Информативность канала оценивается по:

Тема 8. Каналы утечки речевой информации

1. Какими возможностями обладает нарушитель второго уровня?
2. Канал утечки информации представляет собой совокупность…
3. Является ли непреднамеренное прослушивание информации техническим каналом утечки информации?
4. К какому виду технических средств относится телевизор, установленный в защищаемом помещении и демонстрирующий изображение во время проведения конфиденциальных переговоров?

Тема 9. Каналы утечки информации при передаче по каналам связи

1. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?
2. Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?
3. Что должно включать в себя описание технического канала утечки информации?

Тема 10. Технические каналы утечки видовой информации

1. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?
2. В каком техническом канале утечки информации в качестве носителей используются фотоны?
3. В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?

Тема 11. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники

1. Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?
2. Какой термин соответствует деятельности, направленной на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?
3. Выделите тех, кто относится к внутренним потенциальным нарушителям:
4. Как называется модель нарушителя, которая представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, характеризующих результаты действий, и функциональных зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны?

Тема 12. Звукоизоляция помещений

1. Как называются методы защиты акустической информации, направленные на ослабление непосредственных акустических сигналов, циркулирующих в помещении?
2. Как называются методы защиты акустической информации, предусматривающие создание маскирующих помех?
3. Как называются методы защиты акустической информации, предусматривающие подавление технических средств разведки?

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 «Демаскирующие признаки объекта»

1. В состав комплексной защиты информации входят
2. атрибутами шифра являются
3. Утечка информации это

Лабораторная работа № 2 «Изучение существующих каналов утечки информации»

1. Как называется процесс изменения параметров сигнала в зависимости от передаваемой информации?
2. Если частота сигнала равна 20 Гц, то его период
3. Разность между максимальной и минимальной частотой в спектре сигнала называется

Лабораторная работа № 3 «Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации

СМР-700»

1. Как называется прибор, который обнаруживает закладку по превышению порогового значения по частоте?
2. акое расстояние до исследуемого объекта должно быть при контроле помещения с помощью радиочастотометра?
3. Прибор РИЧ-3 является:
4. Какую скорость сканирования каналов имеет сканирующий приемник Winradio 1000?
5. ое программное обеспечение в комплекте сканирующего приемника Winradio 1000 является основной программой управления работой приемника (устанавливает частоту настройки и режим работы приемника, задает параметры сканирования и отображает его результаты, обеспечивает ведение базы данных по результатам работы)?

Лабораторная работа № 4 «Изучение методики обследования помещения с помощью РЧ- зонда»

1. Внедренные устройства каких типов используют для съема и передачи
2. Перечислите основные канали перехвата конфиденциальной информации
3. Какие каналы передачи используются несанкционированными внедренными приборами
4. Напряженность поля физических полей нарастает по мере приближению к источнику, каков тип такой зависимости?

Лабораторная работа № 5 «Изучение методики обследования помещения с помощью ОНЧ- зонда и дополнительного входа»

1. При изменении уровня звука во времени не более чем на 5 дБА, имеет место шум, который называется
2. Шум, уровень звука которого изменяется ступенчато (на 5 дБА и более), причем длительность интервалов, в течение которых уровень остается постоянным, составляет 1с и более, называется
3. характеристикой постоянного шума на рабочих местах является
4. для какого шума дополнительно нормируется максимальный уровень звука

Лабораторная работа № 6 «Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков»

1. Транкинговая связь – это
2. Передача данных по одному коммутируемому каналу без помехоустойчивого кодирования обеспечит реализацию скорости
3. Сколько символов умещается в одном СМС, набранном на русском языке
4. Подключение к интернету с помощью прокси-сервера может помочь

Лабораторная работа № 7 «Изучение программно-аппаратного комплекса «VNK-012GL»»

1. Возможность за приемлемое время получить требуемую информационную услугу называется
2. Межсетевого экрана какого класса не существует
3. По каким критериям нельзя классифицировать угрозы

Лабораторная работа № 8 «Отделение полезного голоса от зашумляющего фона»

1. Голосовой аппарат — это
2. Нарушения голоса не входят в структуру дефекта при
3. Могут ли изменять свою форму и объем следующие надскладочные резонаторные полости

4. Характерной особенностью акустических характеристик псевдоголоса является

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.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1.Отражающая способность материала зависит от:
(1) плотности материала

(2) размера отражающей поверхности материала

(3) угла падения звука на поверхность

(4) скорости распространения звука

2.Звукопоглощение основано на:
(1) превращении кинетической энергии в потенциальную

(2) превращении потенциальной энергии в кинетическую

(3) превращении потенциальной энергии в свободную

(4) превращении кинетической энергии в свободную

3.К каким методам защиты акустической информации относится применение генератора шума:
(1) активные

(2) пассивные

(3) проактивные

(4) превентивные

4.Рассчитайте приблизительное значение ослабления акустического сигнала частотой f=1000 Гц в сплошной однородной стене массой 100 кг.
(1) 22.5 Дб

(2) 25.5 Дб

(3) 52.5 Дб

(4) 55.2 Дб

5.Рассчитайте приблизительное значение ослабления акустического сигнала частотой f=500 Гц в сплошной однородной стене массой 50 кг.
(1) 40.5 Дб

(2) 50.5 Дб

(3) 60.5 Дб

(4) 100 Дб

6.Рассчитайте приблизительное значение ослабления акустического сигнала частотой f=2000 Гц в сплошной однородной стене массой 1000 кг.
(1) 40.3 Дб

(2) 50.5 Дб

(3) 78.5 Дб

(4) 100.5 Дб

7.Какие места в помещении являются наиболее уязвимыми с точки зрения акустической разведки?
(1) окна

(2) кирпичные стены

(3) полы

(4) двери

8.На сколько децибел в среднем увеличивает звукоизоляцию применение уплотняющих прокладок на дверях?
(1) 5-10

(2) 10-15

(3) 15-20

(4) 20-40

9.Какой материал обеспечивает лучшее ослабление акустической волны с f=500 Гц?
(1) кирпичная стена

(2) войлок

(3) одинарное стекло

(4) деревянная обивка

10.Звукопоглощающие материалы делятся на:
(1) пористые

(2) сплошные

(3) составные

(4) простые

11.Как называются звукопоглощающие материалы, в которых звук поглощается только в результате вязкого трения в порах?
(1) пористые

(2) сплошные

(3) составные

(4) простые

12.Как называются звукопоглощающие материалы, в которых звук поглощается за счет трения и релаксационных потерь, связанных с деформацией нежесткого скелета?
(1) пористые

(2) сплошные

(3) составные

(4) простые

13.Как называется шум с тенденцией спада спектральной плотности 3 дБ на октаву в сторону вы¬соких частот?
(1) белый шум

(2) розовый шум

(3) речеподобная помеха

(4) серый шум

14.Как называется шум с огибающей ампли¬тудного спектра, подобной речево¬му сигналу?
(1) белый шум

(2) розовый шум

(3) речеподобная помеха

(4) серый шум

15.Какой из представленных ниже шумов наилучшим образом маскирует речевой сигнал?
(1) белый шум

(2) розовый шум

(3) речеподобная помеха

(4) серый шум

16.Для подавления диктофонов используют генераторы мощных шумовых сигналов … диапазона частот.
(1) миллимитрового

(2) сантиметрового

(3) дециметрового

(4) метрового

17.Какой средний радиус подавления диктофонов способен обеспечить генератор шума дециметрового диапазона?
(1) 0.5 м

(2) 1 м

(3) 5 м

(4) 10 м

18.Какие факторы останавливают применение подавителей мини-диктофонов?
(1) дороговизна

(2) низкая эффективность

(3) то, что их легко обнаружить с помощью визуального контроля

(4) маленькая зона подавления

19.Какой из приведенных ниже документов содержит требования и рекомендации в области технической защиты конфиденциальной информации?
(1) ФЗ «Об информации, информационных технологиях и о защите информации»

(2) ФЗ «О техническом регулировании»

(3) СТР-К

(4) Доктрина информационной безопасности Российской Федерации

20.Выберите рекомендации верные для защищаемых помещений (ЗП) в соответствии с СТР-К:
(1) ЗП должны располагаться на первом этаже

(2) ЗП не должны располагаться на первом этаже

(3) ЗП должны находиться максимально близко к границам контролируемой зоны

(4) ЗП должны быть удалены от границ контролируемой зоны

(5) Ограждающие конструкции ЗП не должны быть смежными с помещениями других организаций

(6) В ЗП не должно быть окон

21.Запись и воспроизведение конфиденциальной речевой информации аппаратурой звукозаписи разрешается проводить:
(1) повсеместно, если информация не относится к государственной тайне

(2) только в защищаемом помещении

(3) не ближе, чем 10 м от границы контролируемой зоны

22.Как называется модель нарушителя, которая отражает систему принятых руководством объекта защиты взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия?
(1) количественная

(2) математическая

(3) косвенная

(4) содержательная

23.Какая модель нарушителя используется для количественных оценок уязвимости объекта и эффективности охраны?
(1) количественная
(2) математическая
(3) косвенная

(4) содержательная

24.Какие уязвимости присущи протоколу telnet?
(1) аутентификация на базе открытого текста

(2) отсутствие механизма предотвращения перегрузок буфера

(3) отсутствие аутентификации сообщений об изменении параметров маршрута

(4) отсутствие поддержки аутентификации заголовков сообщений

25.Какие уязвимости присущи протоколу UDP?
(1) аутентификация на базе открытого текста

(2) отсутствие механизма предотвращения перегрузок буфера

(3) отсутствие аутентификации сообщений об изменении параметров маршрута

(4) отсутствие поддержки аутентификации заголовков сообщений

26.Какие уязвимости присущи протоколу RIP?
(1) аутентификация на базе открытого текста

(2) отсутствие механизма предотвращения перегрузок буфера

(3) отсутствие аутентификации сообщений об изменении параметров маршрута

(4) отсутствие поддержки аутентификации заголовков сообщений

27.Какой вид атаки направлен на получение конфиденциальной информации путем прослушивания сети?
(1) анализ сетевого трафика

(2) сканирование сети

(3) навязывание ложного маршрута

(4) внедрение ложного объекта

28.Какой протокол прикладного уровня производит аутентификацию на базе открытого текста?

(1) IP

(2) TCP

(3) FTP

(4) HTTPS

29.Целью какой атаки является нарушение доступности информации для законных субъектов информационного обмена?
(1) анализ сетевого трафика

(2) сканирование сети

(3) отказ в обслуживании

(4) внедрение ложного объекта

30.Какой тип атаки реализует sniffer?
(1) анализ сетевого трафика

(2) сканирование сети

(3) подмена доверенного объекта в сети

(4) отказ в обслуживании

31.Целью какой атаки является выявление работающих в сети служб, используемых протоколов, открытых портов и т.п.?
(1) анализ сетевого трафика

(2) сканирование сети

(3) подмена доверенного объекта в сети

(4) отказ в обслуживании

32.Как называется атака на систему, целью которой является довести её до отказа?
(1) анализ сетевого трафика

(2) сканирование сети

(3) подмена доверенного объекта в сети

(4) отказ в обслуживании

(5) атака на уровне приложений

33.Как называется атака, при которой злоумышленник получает доступ к системе от имени пользователя приложения?
(1) анализ сетевого трафика

(2) сканирование сети

(3) подмена доверенного объекта в сети

(4) отказ в обслуживании

(5) атака на уровне приложений

34.Какой способ является самым надежным при борьбе с атаками типа “анализ трафика”?
(1) анти-снифферы

(2) одноразовые пароли

(3) криптография

(4) коммутируемая инфраструктура

35.Какой метод борьбы со снифферами помогает сузить зону возможного перехвата информации?
(1) анти-снифферы

(2) одноразовые пароли

(3) криптография

(4) коммутируемая инфраструктура

36.Как называется атака, при которой злоумышленник выдает себя за легитимного участника сети, воспользовавшись внутренним IP-адресом?
(1) сканирование сети

(2) подмена доверенного объекта в сети

(3) отказ в обслуживании

(4) атака на уровне приложений

37.Подмена доверенного объекта в сети по-другому называется:
(1) спуфинг

(2) снифинг

(3) скриминг

(4) фишинг

38.Какие устройства разбивают сеть на сегменты, образующие отдельные домены коллизий?
(1) концентраторы

(2) коммутаторы

(3) межсетевые экраны

(4) маршрутизаторы

39.Как называется DOS-атака, которая использует ping-пакеты в широковещательном режиме?
(1) Smurf

(2) ICMP flood

(3) UDP flood

(4) TCP flood

40.Какие программы позволяют реализовать DOS-атаки нескольких типов одновременно?
(1) Trinoo

(2) TFN

(3) TFN2K

(4) Smurf

41.В какое программное обеспечение встроена функция автомодификации?
(1) Trinoo

(2) TFN

(3) TFN2K

(4) Stacheldracht

42.Что является носителем информации в оптическом канале утечки информации?
(1) акустическая волна

(2) электрическое поле

(3) электромагнитное поле

(4) световая волна

43.К какому техническому каналу утечки информации относится несанкционированное распространение за пределы контролируемой зоны вещественных носителей с защищаемой информацией?
(1) оптический

(2) акустический

(3) материально-вещественный

(4) радиоэлектронный

44.В каком техническом канале утечки информации носителем является упругая акустическая волна?
(1) оптический

(2) акустический

(3) материально-вещественный

(4) радиоэлектронный

45.Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?
(1) ограниченная зона

(2) пограничная зона

(3) контролируемая зона

(4) зона 1

46.Как называется пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения?
(1) ограниченная зона

(2) зона 2

(3) контролируемая зона

(4) зона 1

47.Выберите верное утверждение:
(1) зона 1 меньше зоны 2

(2) зона 1 больше зоны 2

(3) зона 1 меньше контролируемой зоны

(4) зона 2 меньше контролируемой зоны

48.Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?
(1) электромагнитный

(2) электрический

(3) индукционный

49.Как называется технический канал утечки информации, заключающийся в перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи?
(1) электромагнитный

(2) электрический

(3) индукционный

50.Как называется технический канал утечки информации, при котором производится бесконтактный съем информации с кабельных линий связи?
(1) электромагнитный

(2) электрический

(3) индукционный

51.В каких технических каналах утечки акустической информации средой распространения информативного сигнала являются конструкции зданий, стены, потолки и другие твердые тела?
(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

52.В каких технических каналах утечки акустической информации основным средством съема информации является микрофон?
(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

53.В каких технических каналах утечки акустической информации основным средством съема информации является стетоскоп?
(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

54.В каких технических каналах утечки акустической информации основным средством съема информации является лазер?
(1) воздушные

(2) вибрационные

(3) электроакустические

(4) оптико-электронные

55.Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС под давлением звуковой волны может измениться взаимное расположение элементов схем, проводов и т.п.?
(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

56.Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС есть элементы, обладающие "микрофонным эффектом"?

(1) воздушные
(2) вибрационные

(3) электроакустические

(4) параметрические

57.Как называются электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях?
(1) вспомогательные электромагнитные излучения

(2) вторичные электромагнитные излучения

(3) побочные электромагнитные излучения

(4) недекларированные электромагнитные излучения

58.Что значит буква "Н" в аббревиатуре ПЭМИН?
(1) наводки

(2) недекларированные

(3) нарушители

(4) нераспознанные

59.Выделите верное утверждение.
(1) зона 2 должна быть больше контролируемой зоны

(2) зона 2 должна быть меньше зоны 1

(3) зона 2 должна быть меньше контролируемой зоны

(4) зона 2 должна быть равна контролируемой зоне

60.Выделите способы получения видовой информации:
(1) наблюдение за объектами

(2) перехват ПЭМИН

(3) перехват излучений на частотах работы ВЧ-генераторов

(4) съемка объектов

61.К какому типу технических каналов утечки относится перехват информации путем высокочастотного облучения технических средств?
(1) электромагнитные

(2) параметрические

(3) электрические

62.Какой тип технических каналов утечки образуется за счет просачивания информационных сигналов в цепи заземления и электропитания ОТСС?
(1) электромагнитные

(2) параметрические

(3) электрические

63.Выберите из списка технические каналы утечки информации:
(1) Непреднамеренный просмотр информации

(2) Акустоэлектрический канал утечки информации

(3) Канал утечки информации, обусловленный наводками

(4) Внедрение вредоносных программных средств

(5) Просмотр информации с экрана дисплея с использованием специальных электронных устройств съема

64.При обработке информации ограниченного доступа необходимо исключить нарушение её:
(1) Целостности

(2) Полноты

(3) Защищенности

(4) Конфиденциальности

(5) Важности

(6) Доступности

(7) Значимости

(8) Секретности

65.На объекте информатизации защите подлежит:
(1) Информация, представленная в виде баз данных

(2) Носители информации

(3) Речевая информация

(4) Информация, представленная в виде информативных электрических сигналов

66.Угроза безопасности информации представляет собой совокупность:
(1) Канала утечки информации и нарушителя

(2) Условий возникновения угрозы источника угрозы

(3) Факторов внешней среды и источника информации

(4) Факторов, воздействующие на информацию и условий возникновения угрозы

67.По какому параметру классифицируются нарушители правил разграничения доступа?
(1) Уровень технической оснащенности

(2) Уровень защищенности АС

(3) Уровень возможностей, предоставляемых штатными средствами АС

(4) Уровень доступных ресурсов

68.Необходимо ли при формировании угроз безопасности информации учитывать внешние факторы, воздействующие на информацию?
(1) Да

(2) Нет

69.Выберите из нижеперечисленного каналы утечки информации без использования технических средств:
(1) Канал утечки информации, обусловленный наводками

(2) Непреднамеренный просмотр информации

(3) Непреднамеренное прослушивание информации

(4) Канал утечки информации, передаваемой по оптическим линиям связи

70.Какое количество уровней классификации нарушителей правил разграничения доступа?
(1) 4

(2) 6

(3) 8

(4) 12

71.Вспомогательные технические средства и системы (ВТСС) это:
(1) Технические средства, предназначенные для передачи информации ограниченного доступа

(2) Технические средства, устанавливаемые с целью защиты информации ограниченного доступа

(3) Технические средства, не предназначенные для обработки информации, но размещенные в том же помещении, где и объект информатизации

(4) Технические средства, размещаемые в защищаемом помещении и предназначенные для обработки акустической информации ограниченного доступа

72.Что является необходимым условием получения нарушителем видовой информации:
(1) Наличие доступа внутрь контролируемой зоны

(2) Наличие специальной аппаратуры получения видовой информации

(3) Благоприятные погодные условия

(4) Наличие прямой видимости между источником и приемником видовой информации

73.Укажите способы распространения информации при ее утечке каналу, обусловленному наводками:
(1) Цепь электропитания

(2) Цепь заземления

(3) Информативное электромагнитное поле

(4) Воздушное пространство

74.Угрозы несанкционированного доступа к информации включают в себя:
(1) Угроза проникновения в операционную среду компьютера

(2) Угроза хищения носителей защищаемой информации

(3) Угроза внедрения программных закладок

(4) Угроза преднамеренного просмотра информации

75.При формировании требований к системе защиты информации объекта информатизации необходимо:
(1) Провести аттестацию объекта информатизации

(2) Определить границу контролируемой зоны

(3) Провести классификацию автоматизированной системы (объекта информатизации)

(4) Определить угрозы безопасности информации

76.Выберите из списка технические каналы утечки речевой информации:
(1) Специально внедренные в предметы интерьера защищаемого помещения программные средства негласного получения информации

(2) Акустоэлектрический канал утечки информации

(3) Несанкционированный доступ к информации

(4) Наводки на цепи электропитания

Задания в открытой форме

1. Каналы, в которых утечка информации носит случайный разовый характер, называются…
2. Каналы, в которых утечка информации носит достаточно регулярный характер, называются…
3. Ультразвуковому диапазону соответствуют акустические волны:
4. Что такое φ в формуле $s(t) = Asin(2\pi ft + \varphi)$?
5. Если частота сигнала равна 20 Гц, то его период…
6. Разность между максимальной и минимальной частотой в спектре сигнала называется…
7. Десятичный логарифм отношения максимальной мгновенной мощности сигнала к минимальной называется…
8. Если минимальная частота сигнала 30 КГц, а максимальная – 300 КГц, то ширина спектра сигнала будет равна…
9. В общем случае сигнал можно представить следующими параметрами…
10. Произведение значений длительности передачи сигнала, его динамического диапазона и диапазона частот называется…
11. Опасные сигналы подразделяют на два вида…
12. К основным показателям ТКУИ относятся…
13. Срок действия лицензии…
14. Причинами отказа в получении лицензии могут быть…
15. Следствием наличия уязвимостей в информационной системе является…
16. Совокупность содержащейся в базах данных информации, и информационных технологий и технических средств, обеспечивающих ее обработку, называется…
17. Персональные данные это…
18. До начала обработки персональных данных оператор обязан…
19. Выберите случаи обработки персональных данных, когда оператор не обязан получать письменное согласие субъекта на обработку…
20. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на…

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Идентификация	А	Может быть охарактеризован тем, какой пользователь обращается
2	Аутентификация	Б	Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – за счѐт этого каждый субъект или объект системы должен быть однозначно идентифицируем.
3	Запрос на доступ к ресурсу	В	Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа к ресурсу)

2. Установите взаимно однозначное соответствие функции памяти

1	Proximity	А	Чтение/Запись
2	Стандарт ISO/IEC 14443	Б	Чтение/Запись
3	Стандарт ISO/IEC 15693	В	Только чтение

3. Установите взаимно однозначное соответствие

1	аутентификации Kerberos	А	Принимает от пользователей запросы на аутентификацию
2	аутентификации RADIUS	Б	Был разработан специально для того, чтобы обеспечить надежную аутентификацию пользователей
3	Клиент RADIUS	В	рассматривается как механизм аутентификации и авторизации удалѐнных

			пользователей в условиях распределѐнной сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учѐту для служб удалѐнного доступа
4	Сервер RADIUS	Г	Заключается в централизованной обработке информации, предоставленной клиентами

4. Установите взаимно однозначное соответствие методы реализации систем одноразовых паролей

1	Метод "запрос-ответ"	А	В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей
2	Метод "только ответ"	Б	В начале процедуры аутентификации пользователь отправляет на сервер свой логин. В ответ на это последний генерирует некую случайную строку и посылает ее обратно.
3	Метод "синхронизация по времени"	В	При этом в процессе создания строки используется значение предыдущего запроса
4	Метод "синхронизация по событию"	Г	При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд).

5. Установите взаимно однозначное соответствие

1	Ядро безопасности	А	Является одним из элементов ядра системы и предназначена для

			управления регистрацией в журнале событий, связанных с работой системы защиты
2	Ядро системы защиты	Б	локализованная, чѐтко ограниченная, изолированная совокупность программных и аппаратных механизмов, правильно реализующих функцию диспетчера доступа
3	Подсистема регистрации	В	Предоставляет средства для настройки защитных механизмов системы
4	Подсистема управления	Г	Представляет собой программу, которая автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера

6. Установите взаимно однозначное соответствие

1	Замкнутая программная среда	А	Предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты СЗИ загружены и функционируют. Функциональный контроль осуществляется перед входом пользователя в систему
2	Функциональный контроль	Б	Предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах
3	Подсистема контроля аппаратной конфигурации компьютера	В	Позволяет сформировать для любого пользователя компьютера программную

			среду, определив индивидуальный перечень программ, разрешенных для запуска
4	СЗИ «Страж NT 2.0»	Г	Предназначена для своевременного обнаружения изменений в аппаратной конфигурации компьютера и реагирования на эти изменения и поддержания в актуальном состоянии списка устройств компьютера.

7. Установите взаимно однозначное соответствие

1	Пофайловое шифрование	А	Если зашифрован весь диск целиком, то операционная система не сможет запуститься, пока какой-либо механизм не расшифрует файлы загрузки
2	Шифрование каталогов	Б	Пользователь сам выбирает файлы, которые следует зашифровать
3	Шифрование виртуальных дисков	В	Пользователь создает папки, все данные в которых шифруются автоматически
4	Защита процесса загрузки	Г	Концепция виртуальных дисков реализована в некоторых утилитах компрессии, например Stacker или Microsoft DriveSpace

8. Установите взаимно однозначное соответствие

1	Контроль входа на компьютер	А	Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные.
2	Контроль целостности файлов операционной системы	Б	При включении ПК устройство требует от пользователя ввести

			персональную информацию (например, вставить дискету с ключами)
3	Блок управления	В	Через него осуществляется основной обмен данными между устройством и компьютером.
4	Контроллер системной шины ПК	Г	основной модуль шифратора, который управляет работой всех остальных

9.Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками контактного типа, установленными на инженерно-технических коммуникациях
2) Акусто-вибрационный (через ограждающие кострукции)	b) Специализированные высокочувствительные микрофоны, установленные в воздуховодах или смежных помещениях
3) Акусто-электрический (через соединительные линии ВТСС)	c) Аппаратура высокочастотного облучения, установленная за пределами КЗ
4) Акусто-электромагнитный (параметрический)	d) Аппаратура «высокочастотного навязывания», подключенная к соединительным линиям ВТСС

10.Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками микрофонного типа при условии неконтролируемого доступа к ним посторонних лиц
2) Акусто-оптический (через оконные стекла)	b) Лазерные акустические локационные системы, находящиеся за пределами КЗ
3) Акусто-электрический (через	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие

соединительные линии ВТСС)	«микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

11.Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	4) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.
5) 4 уровень	6) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

12.Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных

	технических устройств).

13.Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.
4) Незначительный риск	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

14.Установить соответствие:

1) Правовая защита	a) Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
2) Организационная защита	b) Это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
3) Инженерно-техническая защита	c) Это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

15.Установить соответствие:

1) OLE-automation или просто Automation	a) Технология, организующая доступ к данным разных компьютеров с учетом балансировки нагрузки сети.
2) ActiveX	b) Технология, обеспечивающая безопасность и стабильную работу распределенных приложений при больших объемах передаваемых данных.
3) MIDAS	c) Технология предназначена для создания программного обеспечения как сосредоточенного на одном компьютере, так и распределенного в сети.
4) MTS (Microsoft Transaction Server)	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

16.Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

17.Установить соответствие:

1) Программно-аппаратные (технические) методы	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

18. Установить соответствие:

1) Превентивные	a) Меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
2) Восстановительные	b) Меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
3) Обнаруживающие	c) Меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.
4) Подавляющие	d) Меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.

5) Корректирующие	e) Меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам.

19. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.
2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.
3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

20.Установить соответствие средства обеспечения информационной безопасности:

1) Организационные	a) Сюда входит весь перечень программного обеспечения, который поможет обеспечить должную информационную безопасность ресурса
2) Программные	b) Сюда входят сами приборы и устройства, которые обеспечивают защиту информации.
3) Аппаратные	c) Сюда входят: обеспечение качественного помещения для размещения серверов, качественное оборудование, продуманная кабельная система, организация правового статуса ресурса или компании и др.

Задания на установление правильной последовательности

1. Установить этапы построения программы обеспечения безопасности:
1) Формирование политики безопасности организации
2) Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
3) Регулярный контроль пошаговой реализации плана безопасности
4) Установление уровня безопасности
5) Определение ценности технологических и информационных активов организации

2. Установить иерархию последовательно:
1) Компонент
2) Семейства
3) Элемент
4) Компонент

3. Установить этапы системы управления:
1) Планирование.
2) Внедрение.
3) Мониторинг и анализ.
4) Совершенствование.

4. Установите этапы PDCA:
1) Планирование
2) Проверка
3) Действие
4) Выполнение

5. Установите этапы этапы создания СУИБ:
1) Внедрение и функционирование системы управления информационной безопасности.
2) Проведение мониторинга и анализа системы управления информационной безопасности.
3) Разработка системы управления информационной безопасности.
4) Поддержка и улучшение системы управления информационной безопасности.

6. Установить этапы разработки:
1) Проектирование
2) Реализация
3) Внедрение
4) Анализ и планирование требований пользователей

7. Установить этапы разработки программной документации:
1) Разработка технического проекта.
2) Комплексное внедрение программной документации.
3) Подготовка технического специального задания.
4) Составление подробного эскизного варианта проекта.
5) Оформление рабочего документа.

8. Основные этапы разработки системы управления информационной безопасностью:
1) Обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);
2) Контроль выполнения и эффективности выбранных мер.
3) Оценка защищенности информационной системы;
4) Оценка информационных рисков;
5) Инвентаризация активов;
6) Внедрение выбранных мер обработки рисков;
7) Категорирование активов;

9. Установить предпочтительную последовательность этапов внедрения межсетевого экрана:
1) Конфигурирование
2) Планирование
3) Тестирование
4) Развертывание
5) Управление

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

11. Выберите правильную последовательность этапов разработки профиля защиты.
1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований
12. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование

4. Предпроектный этап

13.Установить этапы реализации в ОС механизмов безопасности в порядке их внедрения:
1. Создание кольцевой системы защиты процессора
2. Реализация аутентификации пользователя
3. Реализация многозадачности
4. Создание виртуальных контейнеров для запуска приложений

14. Расположить этапы процесса комплекса превентивных мер
1.подача и рассмотрение заявки;
2. предварительное ознакомление специалистов с аттестуемыми объектами;
3.разработка программы и методики испытаний;
4. запрос и получение специалистами необходимой технической документации;
5. проведение испытаний;
6. оформление, регистрация и выдача аттестата (сертификата соответствия) на оборудование и помещения.

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

16.Выберите правильную последовательность этапов процесса управления рисками:
1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
2) Анализ угроз и их последствий, определение слабостей в защите;
3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;
4) Выбор, реализация и проверка защитных мер;
5) Оценка остаточного риска;
6) Выбор анализируемых объектов и степени детальности их рассмотрения;

17.Выберите правильную последовательность этапов обеспечения информационной:
1) Оценка стоимости;
2) Реализация политики;
3) Квалифицированная подготовка специалистов;
4) Аудит;
5) Разработка политики безопасности;

18.Выберите последовательность уровней безопасности информации:
1) Административный уровень
2) Процедурный уровень
3) Программно-технический уровень
4) Законодательный уровень

19.Выберите правильную последовательность этапов оценки угроз безопасности информации:
1) Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
2) Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
3) Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
4) Оценка способов реализации (возникновения) угроз безопасности информации;
5) Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
6) Оценка сценариев реализации угроз безопасности информации в системах и сетях.

20.Выберите правильную последовательность этапов построения политики безопасности:
1) Выбор и установка средств защиты;
2) Организация обслуживания по вопросам информационной безопасности;
3) Создание системы периодического контроля информационной безопасности
4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
5) Подготовка персонала работе со средствами защиты.

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
Используя интернет, выбрать такую конфигурацию компьютера, который будет эффективно справляться с профессиональными задачами, связанными с вашей профессиональной деятельностью. Подобрать основные и дополнительные устройства. Рассчитать стоимость

Компетентностно-ориентированная задача №2
Опишите технологический процесс обработки информации. Перечислите и охарактеризуйте технологические процессы процесса обработки информации. Какие режимы обработки информации вам известны? Перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Компетентностно-ориентированная задача №3
Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу.
Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Компетентностно-ориентированная задача №4
Опишите параметры локальной политики безопасности операционной системы Windows, параметры и значения параметров Политики учетной

записи, параметры и значения параметров Политики паролей. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.

Компетентностно-ориентированная задача №5
Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера. Предложите стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Компетентностно-ориентированная задача №6
Опишите параметры и значения параметров Политики аудита. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале? Включите аудит успеха и отказа всех параметров.

Компетентностно-ориентированная задача №7
Опишите причины возникновения остаточной информации. Приведите примеры устройств уничтожения информации с магнитных носителей. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей. Охарактеризуйте программные методы уничтожения информации. Обоснуйте выбор устройства уничтожения информации с магнитных носителей.

Компетентностно-ориентированная задача №8
Опишите разделы реестра Windows. В каких разделах реестра хранится информация о выбранной политике безопасности? Опишите возможности программы REGEDIT.EXE. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

Компетентностно-ориентированная задача №9
С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 120 узлов

Компетентностно-ориентированная задача №10
Сеть может передавать данные в двух режимах: с помощью дейтаграмм и по виртуальным каналам. Какие соображения вы бы приняли во внимание при

выборе того или иного режима для передачи ваших данных, если главным критерием выбора для вас является скорость и надежность доставки?

Компетентностно-ориентированная задача №15

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

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.