

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Таныгин Максим Олегович  
Должность: Заведующий кафедрой  
Дата подписания: 21.09.2023 00:37:15  
Уникальный программный ключ:  
c581cd75563a552725439b81ebe71cb37bca10f0

МИНОБРНАУКИ РОССИИ

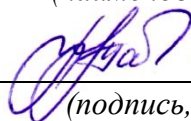
Юго-Западный государственный университет

УТВЕРЖДАЮ:

Заведующий кафедрой

информационной безопасности

*(наименование ф-та полностью)*



М.О. Таныгин

*(подпись, инициалы, фамилия)*

« 30 » августа 2023 г.

ОЦЕНОЧНЫЕ СРЕДСТВА

для текущего контроля успеваемости и промежуточной аттестации  
обучающихся по дисциплине

Информационная безопасность инфокоммуникаций

*(наименование учебной дисциплины)*

11.04.02 Инфокоммуникационные технологии и системы связи,  
направленность (профиль) «Проектирование устройств, систем и сетей  
телекоммуникаций»

*(код и наименование ОПОП ВО)*

# 1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

## 1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

### Тема 1. Введение.

1. Основные информационные процессы.
2. Классификация информации.
3. Угрозы информационной безопасности.
4. Основные виды телекоммуникационных систем (ТКС).

### Тема 2. Основные понятия информационной безопасности ТКС.

1. Уровни обеспечения информационной безопасности ТКС.
2. Основные программно-технические меры обеспечения информационной безопасности ТКС.
3. Понятие НДС.
4. Основные угрозы безопасности и их классификация.
5. Основные положения доктрины информационной безопасности РФ.

### Тема 3. Информационная безопасность систем передачи речевой информации.

1. Методы скремблирования.
2. Системы телефонной связи и их классификация.
3. Аналоговые цифровые системы телефонной связи с коммутацией каналов.
4. Аппаратные и программно-аппаратные методы защиты.
5. Организационные и организационно-технические, аппаратные и программно-аппаратные методы защиты.

### Тема 4. Информационная безопасность систем волоконно-оптической связи (ВОЛС).

1. Особенности оптических систем связи.
2. Уязвимости и каналы утечки информации.
3. Методы НДС.
4. Аппаратные и программные методы защиты.

### Тема 5. Инфокоммуникационная безопасность систем сотовой связи.

1. Архитектура сети GSM.
2. Угрозы информационной безопасности в системах сотовой связи GSM.
3. Методы и средства обеспечения безопасности в системах GSM.
4. Какие действия могут нанести урон безопасности в сети?
5. Что является самым распространённым основанием для возникновения угроз информационной безопасности?

**Критерии оценки:**

**4-3балла** (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

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

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

## **1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ**

**Практическая работа № 1 «Общие вопросы обработки сигналов в программе Adobe Audition»**

1. Что такое дискретизация аналогового сигнала?
2. Что такое АИМ-сигнал?
3. Как происходит кодирование АИМ-сигнала?
4. Объяснить метод преобразования (оцифровки) аналогового сигнала в цифровой
5. Что такое информация?
6. На сколько категорий и каких подразделяются все виды информации (кратко охарактеризовать каждую).

**Практическая работа № 2 «Маскировка речевого сигнала путем его зашумления»**

1. Чем описывается область слухового восприятия человека?
2. Основные величины и их соотношения, характеризующие разборчивость речи.
3. Очередность проведения инструментальной проверки.

4. Опишите модель структуры речевого сигнала.

**Практическая работа № 3** «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»

1. Перечислите виды сигналов сигнализации двухпроводной аналоговой абонентской линии и их функции.

2. Поясните принцип организации шлейфной сигнализации?

3. Сформулируйте, достоинства и недостатки при организации шлейфного способа сигнализации?

4. Перечислите виды информационных акустических сигналов, их частоты и каденции используемые в отечественных аналоговых телефонных сетях при шлейфном способе сигнализации.

5. Поясните особенности в использовании основных стандартных акустических сигналов местных телефонных сетей различных стран.

6. Перечислите основные параметры абонентских линий городских АТС.

**Практическая работа №4** «Обработка тональных сигналов набора номера»

1. Сколько базовых частот в тональном наборе номера?

2. Чем отличается тональный и импульсный набор?

3. Как сделать тональный режим?

4. Как работает DTMF?

5. Что такое тональный режим набора номера?

**Практическая работа №5** «Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android»

1. Для чего нужны меры по обеспечению безопасности мобильного терминала от НСД?

2. Какая информация должна быть защищена от НСД?

3. Как производится настройка параметров блокировки экрана?

4. Как зашифровать устройство?

5. Как ввести пароль и обеспечить его видимость при вводе?

6. Для чего нужны сертификаты безопасности?

#### **Критерии оценки:**

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

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

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

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

## **2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ**

### **2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ**

#### **Задания в закрытой форме**

1. Какая сетевая атака связана с превышением допустимых пределов функционирования сети:

- (1) отказ в обслуживании (DoS – атака)
- (2) подслушивание (Sniffing)
- (3) атака Man in – the – Middle (человек в середине)
- (4) угадывание ключа

2. На сколько уровней модель OSI разделяет коммуникационные функции:

- (1) семь
- (2) восемь
- (3) пять

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

- (1) уровни выполняют одинаковые задачи, постоянно повторяя передающие сигналы по сети
- (2) каждый уровень выполняет свою определенную задачу
- (3) первых три уровня выполняют одинаковые задачи, последующие выполняют определенные задачи

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

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

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

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

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

(1) верно

(2) не верно

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

(1) горизонтальная модель

(2) вертикальная модель

(3) сетевая модель

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

(1) представления

(2) прикладной

(3) сеансовый

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

(1) представления

(2) прикладной

(3) канальный

9. Какой уровень обеспечивает битовые протоколы передачи информации:

(1) физический

(2) канальный

(3) транспортный

10. Основными элементами модели OSI являются:

(1) уровни, прикладные процессы и физические средства соединения

(2) уровни и прикладные процессы

(3) уровни

11. Единицей информации канального уровня являются:

(1) сообщения

(2) потоки

(3) кадры

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

- (1) TCP
- (2) IP
- (3) WWW

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

- (1) TCP
- (2) IP
- (3) HTTPS

14. Какие функции выполняет протокол IP

- (1) маршрутизация
- (2) коррекция ошибок
- (3) установка соединения

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

- (1) сетевой
- (2) представительский
- (3) транспортный

16. Подтверждение подлинности взаимодействующих объектов обеспечивает:

- (1) аутентификация
- (2) конфиденциальность
- (3) контроль доступа

17. Защиту от несанкционированного использования ресурсов обеспечивает:

- (1) контроль доступа
- (2) конфиденциальность
- (3) аутентификация

18. Цифровая подпись – это:

- (1) способ введения электронной метки для файла данных
- (2) сведения о пользователе помещаемые в файл
- (3) файл, подтверждающий ваши права
- (4) идентификатор документа

19. К механизмам безопасности относят:

- (1) алгоритмы симметричного шифрования
- (2) невозможность отказа от полученного сообщения

- (3) целостность сообщения
- (4) хэш-функции

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

- (1) политика безопасности (Security Policy)
- (2) ядро безопасности (Trusted Computing Base, TCB)
- (3) модель безопасности (Security Model)
- (4) идентификация (Identification)

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

- (1) профиль защиты
- (2) проект защиты
- (3) задачи защиты
- (4) круг защиты

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

- (1) прослушивание каналов
- (2) внедрение сетевых вирусов
- (3) умышленное уничтожение или искажение информации
- (4) выход из строя операционной системы

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

- (1) прослушивание каналов
- (2) контроль доступа
- (3) аутентификация
- (4) аудит

24. К сервисам безопасности относят:

- (1) идентификация/аутентификация
- (2) протоколирование/аудит
- (3) шифрование
- (4) аудит

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

- (1) мандатное управление доступом (Mandatory Access Control)
- (2) дискреционное управление доступом (Discretionary Access Control)



- (3) прямое взаимодействие (Trusted Path)
- (4) идентификация (Identification)

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

- (1) дискреционное управление доступом (Discretionary Access Control)
- (2) мандатное управление доступом (Mandatory Access Control)
- (3) модель безопасности (Security Model)
- (4) идентификация (Identification)

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

- (1) конфиденциальность
- (2) контроль доступа
- (3) аутентификация

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

- (1) транспортном
- (2) физическом
- (3) канальном
- (4) сетевом

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

- (1) модель безопасности (Security Model)
- (2) ядро безопасности (Trusted Computing Base, TCB)
- (3) политика безопасности (Security Policy)
- (4) прямое взаимодействие (Trusted Path)

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

- (1) мандатное управление доступом (Mandatory Access Control)
- (2) политика безопасности (Security Policy)
- (3) прямое взаимодействие (Trusted Path)
- (4) идентификация (Identification)

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

- (1) хищение жестких дисков, подключение к сети, инсайдерство
- (2) перехват данных, хищение данных, изменение архитектуры системы
- (3) хищение данных, подкуп системных администраторов, нарушение регламента работы

32. Виды информационной безопасности:

- (1) персональная, корпоративная, государственная
- (2) клиентская, серверная, сетевая
- (3) локальная, глобальная, смешанная

33. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- (1) несанкционированного доступа, воздействия в сети
- (2) инсайдерства в организации
- (3) чрезвычайных ситуаций

34. Основные объекты информационной безопасности:

- (1) компьютерные сети, базы данных
- (2) информационные системы, психологическое состояние пользователей
- (3) бизнес-ориентированные, коммерческие системы

35. Основными рисками информационной безопасности являются:

- (1) искажение, уменьшение объема, перекодировка информации
- (2) техническое вмешательство, выведение из строя оборудования сети
- (3) потеря, искажение, утечка информации

36. К основным принципам обеспечения информационной безопасности относится:

- (1) экономической эффективности системы безопасности
- (2) многоплатформенной реализации системы
- (3) усиления защищенности всех звеньев системы

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

- (1) установление регламента, аудит системы, выявление рисков
- (2) установка новых офисных приложений, смена хостинг-компании
- (3) внедрение аутентификации, проверки контактных данных пользователей

38. Принципом информационной безопасности является принцип недопущения:

- (1) неоправданных ограничений при работе в сети (системе)
- (2) рисков безопасности сети, системы
- (3) презумпции секретности

39. Принципом политики информационной безопасности является принцип:

- (1) невозможности миновать защитные средства сети (системы)

- (2) усиления основного звена сети, системы
- (3) полного блокирования доступа при риск-ситуациях

40. Принципом политики информационной безопасности является принцип:

- (1) усиления защищенности самого незащищенного звена сети (системы)
- (2) перехода в безопасное состояние работы сети, системы
- (3) полного доступа пользователей ко всем ресурсам сети, системы

41. Принципом политики информационной безопасности является принцип:

- (1) разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- (2) одноуровневой защиты сети, системы
- (3) совместимых, однотипных программно-технических средств сети, системы

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

- (1) компьютерный сбой
- (2) логические закладки («мины»)
- (3) аварийное отключение питания

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

- (1) прочитать приложение, если оно не содержит ничего ценного – удалить
- (2) сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- (3) удалить письмо с приложением, не раскрывая (не читая) его

44. Принцип Кирхгофа:

- (1) секретность ключа определена секретностью открытого сообщения
- (2) секретность информации определена скоростью передачи данных
- (3) секретность закрытого сообщения определяется секретностью ключа

45. ЭЦП – это:

- (1) электронно-цифровой преобразователь
- (2) электронно-цифровая подпись
- (3) электронно-цифровой процессор

46. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- (1) покупка нелегального ПО
- (2) ошибки эксплуатации и неумышленного изменения режима работы системы

(3) сознательного внедрения сетевых вирусов

47. Наиболее распространены угрозы информационной безопасности сети:

- (1) распределенный доступ клиент, отказ оборудования
- (2) моральный износ сети, инсайдерство
- (3) сбой (отказ) оборудования, нелегальное копирование данных

48. Наиболее распространены средства воздействия на сеть офиса:

- (1) слабый трафик, информационный обман, вирусы в интернет
- (2) вирусы в сети, логические мины (закладки), информационный перехват
- (3) компьютерные сбои, изменение администрирования, топологии

49. Утечкой информации в системе называется ситуация, характеризующаяся:

- (1) потерей данных в системе
- (2) изменением формы информации
- (3) изменением содержания информации

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

- (1) целостность
- (2) доступность
- (3) актуальность

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

- (1) вероятное событие
- (2) детерминированное (всегда определенное) событие
- (3) событие, происходящее периодически

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

- (1) регламентированной
- (2) правовой
- (3) защищаемой

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

- (1) программные, технические, организационные, технологические
- (2) серверные, клиентские, спутниковые, наземные
- (3) личные, корпоративные, социальные, национальные

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

- (1) владелец сети
- (2) администратор сети
- (3) пользователь сети

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

- (1) руководств, требований обеспечения необходимого уровня безопасности
- (2) инструкций, алгоритмов поведения пользователя в сети
- (3) нормы информационного права, соблюдаемые в сети

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

- (1) аудит, анализ затрат на проведение защитных мер
- (2) аудит, анализ безопасности
- (3) аудит, анализ уязвимостей, риск-ситуаций

57. Что такое компьютерный вирус?

- (1) прикладная программа
- (2) системная программа
- (3) программа, выполняющая на компьютере несанкционированные действия
- (4) база данных.

58. Основные типы компьютерных вирусов:

- (1) аппаратные, программные, загрузочные
- (2) программные, загрузочные, макровирусы
- (3) файловые, программные, макровирусы

59. Этапы действия программного вируса:

- (1) размножение, вирусная атака
- (2) запись в файл, размножение
- (3) запись в файл, размножение, уничтожение программы

60. В чем заключается размножение программного вируса?

- (1) программа-вирус один раз копируется в теле другой программы
- (2) вирусный код неоднократно копируется в теле другой программы

61. Что называется вирусной атакой?

- (1) неоднократное копирование кода вируса в код программы
- (2) отключение компьютера в результате попадания вируса
- (3) нарушение работы программы, уничтожение данных, форматирование жесткого диска

62. Какие существуют методы реализации антивирусной защиты?

- (1) аппаратные и программные

- (2) программные и административные
- (3) только программные

63. Какие существуют основные средства защиты данных?

- (1) резервное копирование наиболее ценных данных
- (2) аппаратные средства
- (3) программные средства

64. Какие существуют вспомогательные средства защиты?

- (1) аппаратные средства
- (2) программные средства
- (3) административные методы и антивирусные программы

65. На чем основано действие антивирусной программы?

- (1) на ожидании начала вирусной атаки
- (2) на сравнении программных кодов с известными вирусами
- (3) на удалении зараженных файлов

66. Какие программы относятся к антивирусным:

- (1) AVP, DrWeb, Norton AntiVirus
- (2) MS-DOS, MS Word, AVP
- (3) MS Word, MS Excel, Norton Commander

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

- (1) руткит
- (2) бэкап
- (3) камбэк

68. Компьютерные вирусы:

- (1) файлы, которые невозможно удалить
- (2) программы, способные к саморазмножению (самокопированию)
- (3) файлы, имеющие определенное расширение

69. DDos — программы:

- (1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера
- (2) оба варианта верны
- (3) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров

70. Отличительными способностями компьютерного вируса являются:

(1) способность к самостоятельному запуску и многократному копированию кода

(2) значительный объем программного кода

(3) легкость распознавания

71. DoS — программы:

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

(2) оба варианта верны

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

72. Компьютерные вирусы:

(1) являются следствием ошибок в операционной системе

(2) пишутся людьми специально для нанесения ущерба пользователем

ПК

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

73. Троянские программы бывают:

(1) сетевые программы

(2) программы передачи данных

(3) программы шпионы

74. Основная масса угроз информационной безопасности приходится на:

(1) троянские программы

(2) шпионские программы

(3) черви

75. Троянская программа, троянец:

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

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

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

76. Информационная безопасность зависит от:

(1) компьютеров, поддерживающей инфраструктуры

(2) пользователей

(3) информации

77. Сетевые черви бывают:

- (1) Web-черви
- (2) черви операционной системы
- (3) черви MS Office

78. Таргетированная атака – это:

- (1) атака на сетевое оборудование
- (2) атака на компьютерную систему крупного предприятия
- (3) атака на конкретный компьютер пользователя

79. Сетевые черви бывают:

- (1) почтовые черви
- (2) черви операционной системы
- (3) черви MS Office

80. Stuxnet – это:

- (1) троянская программа
- (2) макровирус
- (3) промышленный вирус

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

- (1) загрузочные
- (2) очень опасные
- (3) опасные

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

- (1) загрузочные вирусы
- (2) троянцы
- (3) черви

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

- (1) не опасные
- (2) очень опасные
- (3) файловые

84. Какие угрозы безопасности данных являются преднамеренными:

- (1) ошибки персонала
- (2) открытие электронного письма, содержащего вирус
- (3) не авторизованный доступ

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

- (1) опасные
- (2) не опасные
- (3) макровирусы



86. Под какие системы распространение вирусов происходит наиболее динамично:

- (1) Windows
- (2) Mac OS
- (3) Android

87. Макровирусы:

- (1) существуют для интегрированного офисного приложения Microsoft Office
- (2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске
- (3) заражают загрузочный сектор гибкого или жёсткого диска

88. Какой вид идентификации и аутентификации получил наибольшее распространение:

- (1) системы PKI
- (2) постоянные пароли
- (3) одноразовые пароли

89. Файловые вирусы:

- (1) заражают загрузочный сектор гибкого или жёсткого диска
- (2) существуют для интегрированного офисного приложения Microsoft Office
- (3) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске

90. Для периодической проверки компьютера на наличие вирусов используется:

- (1) компиляция
- (2) антивирусное сканирование
- (3) дефрагментация диска

91. Антивирусный сканер запускается:

- (1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия
- (2) оба варианта верны
- (3) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера

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

- (1) текстовый

- (2) сетевой
- (3) файловый

93. Антивирусный монитор запускается:

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

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

- (3) оба варианта верны

94. К категории компьютерных вирусов не относятся:

- (1) загрузочные вирусы
- (2) файловые вирусы
- (3) тупе-вирусы

95. Выберите тип вредоносных программ:

- (1) шпионское, рекламное программное обеспечение
- (2) Microsoft Office
- (3) операционная система Linux

96. Выберите тип вредоносных программ:

- (1) Microsoft Office
- (2) вирусы, черви, троянские и хакерские программы
- (3) операционная система Windows

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

- (1) матрица
- (2) шаблон
- (3) фундамент

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

- (1) круглые скобки
- (2) угловые скобки
- (3) фигурные скобки

99. Проектированием структуры web-сайта занимается:

- (1) web-программист
- (2) провайдер
- (3) web-дизайнер

100. Сайт можно создать, воспользовавшись:

- (1) языком программирования Си
- (2) языком программирования Паскаль
- (3) языком разметки гипертекста HTML

### Задания в открытой форме

1. Конфиденциальностью информации называется.....
2. К коммерческой тайне относится информация.....
3. Информационной безопасностью предприятия является.....
4. В состав системы защиты информации входят обеспечивающие подсистемы.....
5. Под угрозой безопасности информации понимается.....
6. Причинами информационных угроз являются.....
7. Основные компьютерные вирусы.....
8. К основным законам информационной безопасности РФ относятся законы.....
9. Основными принципами политики безопасности являются.....
10. Политика безопасности верхнего уровня включает.....
11. Удаленный доступ к сервису организован.....
12. Политика управления паролями включает.....
13. Системный подход к защите информации базируется на принципах.....
14. В состав организационно-технических мер входит.....
15. Межсетевые экраны применяют для.....
16. Технические средства противодействия классифицируются.....
17. В состав службы безопасности входят подразделения.....
18. К мерам по защите информации в интернете относятся.....
19. Для защиты электронной почты используется.....
20. Для защиты от вирусов можно использовать.....
21. К антивирусным программам относятся.....
22. План защиты включает.....
23. Ответственным за определение уровня классификации информации является.....
24. Политики безопасности – это.....
25. К посторонним лицам - нарушителям информационной безопасности относятся.....

### Задания на установление соответствия

1. Установить соответствие между элементами и функциями

1	Диаграммы деятельности	А	IDEF0
2	Бизнес-моделирование	Б	Active Diagram
3	Проектирование модели	В	Class-diagram

	данных		
4	Моделирование потоков данных	Г	DFD-модель
5	Описание объектов программы	Д	IDEF1x

2. Установить соответствие между способами и видами информации

1	Диаграмма передачи управления	А	IDEF0
2	Бизнес-моделирование	Б	Component Diagram
3	Проектирование модели данных	В	Sequence diagram
4	Моделирование потоков данных	Г	DFD-модель

3. Установить соответствие

1	Методология построения модели потоков данных	А	IDEF3
2	Бизнес-моделирование	Б	Component Diagram
3	Проектирование модели данных	В	Диаграмма компонентов

4. Установить соответствие мер защиты информации:

1	Выделение функций ИС	А	Диаграммы Use-case
2	Последовательность передачи активности между объектами системы	Б	Component Diagram
3	Описание объектов системы	В	Диаграммы Sequences
4	Последовательность деятельности в системе	Г	Class Diagram

5. Установить соответствие между каналами связи

1	Технического проектирования	А	Получение корректного программного кода
2	Анализ требований	Б	Разработка основных моделей функционирования
3	Эскизное проектирование	В	Сбор и систематизация требований
4	Тестирование и отладка	Г	Выделение целей и задач проектирования,
5	Внедрение	Д	Обучение персонала

6. Установить соответствие между элементами и функциями

1	Компоновка программных модулей ИС	А	Activity Diagram
2	Описание объектов системы	Б	Class Diagram
3	Размещение модулей ИС	В	Sequences Diagram
4	Последовательность деятельности в системе	Г	Package Diagram
5	Схема размещения программных пакетов	Д	Deployment diagrams

7. Установить соответствие между видами технических каналов утечки информации

1	Технического проектирования	А	Технического задания
2	Сопровождение	Б	Разработки рабочей документации
3	Анализ предметной области ИС	В	Скорректированная рабочая документация
4	Тестирование и отладки	Г	Инструкции по эксплуатации
5	Внедрение	Д	Акт приема сдачи работ

8. Установите соответствие между методологиями риска

1	Выделение функций ИС	А	Диаграммы Use-case
2	Последовательность передачи активности между объектами системы	Б	Component Diagram
3	Описание объектов системы	В	Диаграммы Sequences
4	Последовательность деятельности в системе	Г	Class Diagram
5	Схема размещения программных пакетов	Д	Диаграммы Activity

9. Установите соответствие между международной организацией по стандартизации ISO

1	Сбор и систематизация данных об объекте проектирования	А	IDEF0
2	Бизнес-моделирование	Б	Component Diagram

3	Проектирование модели данных	В	Модель Захмана
4	Моделирование потоков данных	Г	DFD-модель
5	Схема размещения программных пакетов	Д	IDEF1x

10. Установить соответствие:

1) Угроза целостности	а) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	б) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) Ущерб	с) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	д) Это угроза изменения информации.

11. Установить соответствие классификации угроз

1) Угроза безопасности	а) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	б) Это угроза раскрытия информации.
3) Атака	с) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	д) Это действие по использованию уязвимости; реализация угрозы.

12. Установить соответствие

1) Нарушитель	а) намеренно идущий на нарушение из корыстных побуждений.
2) Злоумышленник	б) лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового, и использующее для этого различные возможности, методы и средства.
3) Взломщик	с) Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам.

13. Установить соответствие между классификацией АС и их характеристикой.

1	1 Д	А	Один пользователь, носители одного уровня, конфиденциальная информация.
2	2 Б	Б	Два пользователь, доступ ко всей информации, конфиденциальная информация.
3	3 Б	В	Два пользователь, не все пользователи имеют право доступа ко всей информации, конфиденциальная информация.

14. Установить соответствие между классификацией АС и их характеристикой.

1	1 Б	А	Два пользователь, не все пользователи имеют право доступа ко всей информации, совершенно секретная информация.
2	1 А	Б	Два пользователь, не все пользователи имеют право доступа ко всей информации, информация особой важности.
3	1 В	В	Два пользователь, не все пользователи имеют право доступа ко всей информации, секретная информация.

15. Установить соответствие между классификацией АС и их характеристикой.

1	3 Б	А	Два пользователь, не все пользователи имеют право доступа ко всей информации, совершенно секретная информация.
2	2 А	Б	Два пользователь, не все пользователи имеют право доступа ко всей информации, секретная информация.
3	1 В	В	Два пользователь, доступ ко всей информации, секретная

			информация.
1	1 Б	А	Один пользователь, носители одного уровня, конфиденциальная информация.

### **Задания на установление правильной последовательности**

1. Расположите в хронологической последовательности (от раннего к позднему) следующие события (2 балла):

1. разработка ТЗ на проектирование;
2. формулировка цели проектирования;
3. разработка модели данных;
4. разработка бизнес-модели системы.

2. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Техническое проектирование
2. Разработки рабочей документации
3. Анализ предметной области ИС
4. Внедрение и опытная эксплуатация
5. Отладки и тестирование

3. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Поставка
2. Разработка
3. Верификация
4. Управление конфигурацией
5. Приобретение
6. Документирование

4. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Формулирование цели создания (развития) системы
2. Характеристика объектов автоматизации
3. Обучение персонала системы
4. Внедрения ИС
5. Разработка технического задания

5. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Обследование деятельности каждого автоматизируемого подразделения
2. Детальный анализ бизнес-процессов подразделения
3. Систематизация и анализ потоков данных и документов



- 4.Согласования задач ИС с руководством предприятия
5. Разработка модели данных
6. Разработка бизнес-модели подразделения предприятия

6.Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Техническое проектирование
2. Разработки рабочей документации
3. Анализ предметной области ИС
4. Внедрение и опытная эксплуатация
5. Отладки и тестирование

7. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Требования к функциональным возможностям ИС
2. Сопровождение
3. Проектирование,
4. Детальное программирование,
5. Кодирование,
6. Сертификация,

8.Расположите в хронологической последовательности (от раннего к позднему) следующие события (2 балла):

1. разработка ТЗ на проектирование;
2. формулировка цели проектирования;
3. разработка модели данных;

9.Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Характеристика объектов автоматизации
2. Обучение персонала системы
3. Разработка технического задания
4. Определение модели данных,
5. Разработка технического задания,
6. Формирование календарного плана работ
7. Разработка предварительных проектных решений

10. Расположите в хронологической последовательности (от раннего к позднему) следующие действия при проектировании ИС (2 балла):

1. Обследование деятельности каждого автоматизируемого подразделения
2. Детальный анализ бизнес-процессов подразделения
3. Систематизация и анализ потоков данных и документов
- 4.Согласования задач ИС с руководством предприятия
5. Разработка модели данных

## 6. Разработка бизнес-модели подразделения предприятия

### 11. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам
2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet
3. Защита внешних каналов передачи информации
4. Разработка политики информационной безопасности
5. Анализ угрозы безопасности

### 12. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций
2. Передача управления программе-носителю вируса
3. Поиск жертвы
4. Заражение найденной жертвы
5. Загрузка вируса в память

### 13. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности
2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности
3. Разработка политики антивирусной безопасности
4. Разработка плана обеспечения антивирусной безопасности

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

1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

### 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

**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

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

### Компетентностно-ориентированная задача № 2

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

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

А-111

Б-110

В-101

Г-100

Определите, каким кодовым словом может быть закодирована буква Д.

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

### **Компетентностно-ориентированная задача № 3**

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

### **Компетентностно-ориентированная задача № 4**

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

### **Компетентностно-ориентированная задача № 5**

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

### **Компетентностно-ориентированная задача №6**

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 №7**

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 №8**

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. Прodelайте это двумя способами: через окно свойств группы и окно свойств пользователя.

### **Компетентностно-ориентированная задача №9**

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 №10**

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 №11**

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 №12**

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 №13**

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 №14**

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.