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

Информационная безопасность телекоммуникационных систем
(наименование учебной дисциплины)

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

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ.

Тема 1. Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»

1. Основное понятие информации.
2. Какие виды информации существуют?
3. Назовите основные требования к информационной безопасности
4. Дайте определение «телекоммуникационные системы»
5. Назовите основные отличия дисциплин «Информационная безопасность» и «Информационная безопасность телекоммуникационных систем».

Тема 2. Доктрина информационной безопасности РФ

1. Назовите основную концепцию ИБ РФ
2. Какие существуют типы угроз ИБ РФ?
3. Назовите методы обеспечения ИБ РФ.

Тема 3. Угрозы информационной безопасности ТКС

1. Дайте определение «Угроза ИБ ТКС»
2. Классификация угроз по аспекту информационной безопасности. Назовите основные угрозы доступности
3. Назовите основные угрозы целостности
4. Какие основные угрозы конфиденциальности существуют?

Тема 4. Классификация угроз по компонентам ТКС

1. Назовите все классы угроз передачи информации в ТКС.
2. Раскройте понятие «Информационные угрозы».
3. Раскройте понятие «Атака».

Тема 5. Методы оценки уязвимостей ТКС.

1.Как проводиться тестирование на проникновение?
2. Какие методы используются для иденфикации потенциальных сбоев?
3. Назовите причины опасности макровирусов.
4. Какие можно применять методы защиты от компьютерных вирусов?
5. Назовите способы распространения вредоносных программ?

Тема 6. Системы электросвязи, угрозы безопасности и методы их защиты

1. Что такое сетевая атака?
2. В чем состоит технология анализа защищенности?
3. Назовите угрозы безопасности электросвязи?
4. Какие существуют методы защиты электросвязи?

5. Какие могут возникнуть организационные проблемы?

Тема 7. Общие методы организации защищенной речевой связи в телефонной сети

1. Дайте определение системе защиты информации.

2. Перечислите классы защищенности автоматизированных систем.

3. Какие существуют особенности защиты информации при работе с системами управления базами данных?

4. Как обеспечить безопасность информации на рабочем месте пользователя ПК?

5. Назовите основные требования к информационной безопасности.

Тема 8 Методы защиты информации в телефонном канале связи.

1 Что предполагает ограничение физического доступа?

2 В чём заключаются методы защиты информации, основанные на преобразовании сигналов в линии связи?

3 Что следует учитывать при использовании защитного шума?

4 При каком значении отношения шум/сигнал возникает невозможность фиксации факта разговора?

Тема 9 Рекомендации по ограничению физического доступа к оборудованию связи.

1 На что направлен метод ограничения физического доступа к оборудованию связи?

2 Как решается проблема легко заменяемых элементов?

3 Какой орган осуществляет сертификацию аппаратуры, применяемой в сетях связи?

4 Каких правил следует придерживаться при организации рабочего места абонента защищенной связи?

5 Как должны быть направлены в пространстве антенны генераторов электромагнитного шума?

Тема 10 Защита речевой информации в канале связи путем преобразования

сигнала.

1 Опишите механизм преобразования с инверсией спектра и статическими перестановками спектральных компонент речевого сигнала

2 Опишите механизм преобразования с временными перестановками и временной инверсией элементов речевого сигнала со статическим законом перестановки

3 Опишите механизм преобразования с временными или частотными перестановками с переменными перестановками под управлением криптоблока

4 Назовите плюсы использования скремблеров

5 Чем ограничивается применение аппаратуры защиты с кодированием голоса на скорости 1200-4800 бит/сек с последующим шифрованием цифрового потока?
6 Преимущества и недостатки использования симметричных и несимметричных систем при решении задач защиты информации в канале связи

Тема 11 Информационная безопасность телефонной связи.
1 По каким критериям можно разделить системы телефонной связи?
2 Перечислите пути и места утечки информации в телефонных системах
3 В каком диапазоне частот передается сигнал аналоговой телефонной связи?
4 Что относится к организационным и организационно-техническим методам защиты информации?
5 Что такое скремблирование, его виды
6 Какие существуют варианты подключения шифрующих устройств в зависимости от требований к секретности систем связи?

Тема 12 Современные криптографические алгоритмы.
1 Как в классической криптографии называется секретная единица, позволяющая отправителю зашифровать сообщение, а получателю – расш2 Опишите стандарт DES
3 Опишите российский стандарт шифрования данных ГОСТ 28147-89
4 В чём заключается суть асимметричных криптосистем?
5 Опишите механизм шифрования, при использовании генератора псевдослучайных чисел
6 Назовите размеры ключа для алгоритма DES и алгоритма ГОСТ 28147-89

Тема 13 Защита информации в системах волоконно-оптической связи.
1 Опишите физические особенности оптических волокон
2 Опишите технические особенности оптических волокон
3 Опишите механизм скрытой передачи информации по оптическим линиям связи
4 Назовите недостатки волоконной технологии
5 Что включают в себя локальные участки волоконно-оптической линии?
6 Что включают в себя распределенные участки волоконно-оптической линии?

Тема 14 Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС.
1 Что такое поляризационная модовая дисперсия (ПМД)?
2 Что вызывает ПМД?

3 Какие внешние факторы влияют на величину ПМД?
4 В каких единицах измеряется ПМД?
5 Какие процедуры позволяют контролировать уровень ПМД при изготовлении и прокладке кабеля?
6 Что вызывает дифференциальную групповую задержку DGD?

Тема 15 Пути утечки информации из ВОЛС.ифровать?
1 Какие особенности передачи сигнала по ВОЛС обуславливают возможность снятия информации с помощью рассеянного излучения за пределами ОВ?
2 Что включает в себя ВОЛС?
3 Перечислите физические принципы формирования каналов утечки в ВОЛС
4 В каких случаях возможно нарушение полного внутреннего отражения при механическом воздействии на волокно?
5 На какие группы делятся способы несанкционированного доступа к ВОЛС?
6 Кратко опишите метод оптического туннелирования

Тема 16 Методы защиты информации, передаваемой по ВОЛС.
1 Назовите два основных направления защиты информации в ВОЛС
2 Опишите механизм технических средств, используемых для защиты от несанкционированного доступа к сигналам, передаваемым по ОВ
3 Назовите виды систем диагностики состояния (СДС)
4 Для какого метода криптографической защиты информации используются коды, размножающие ошибки?
5 Какие параметры сигнала изменяются при использовании режима динамического хаоса?
6 Какие преимущества предоставляют криптографии?

Тема 17 Защита ВОЛС.
1 Назовите достоинства использования защищенных ВОЛС по сравнению с применением аппаратуры засекречивания
2 Назовите три основных направления разработки защищенных ВОЛС
3 Опишите метод кодового зашумления
4 Опишите метод создания и контроля картины интерференции
5 Опишите метод анализа модового состава
6 Опишите метод режима динамического хаоса

Тема 18 Виртуальные частные сети.
1 Что представляют собой виртуальные частные сети?
2 Какие составляющие необходимы для реализации VPN?
3 Виды VPN
4 Какими протоколами регламентируется безопасность VPN?
5 Перечислите способы атак на VPN

6 Назовите преимущества VPN

Критерии оценки:

1 балл 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.

0,5 балла 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 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. На сколько категорий и каких подразделяются все виды
6. информации (кратко охарактеризовать каждую)?
7. Что такое инфокоммуникационная безопасность?
8. Что такое защита информации?

Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»

1 Классификация систем телефонной связи.

2 Сколько групп методов защиты телефонных сообщений известно. Кратко изложить эти методы.

3 Перечислить особенности метода зашумления.

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

1 Что такое сигнализация, система сигнализации и протокол сигнализации?

2 Привести виды сигнализации в телефонных сетях по их функциональному назначению?

3 Какие виды кодирования используются в существующих системах сигнализации?

4 Чем характеризуются импульсный и тональный наборы номера?

5 Как можно определить тональный номер абонента, подключившись к телефонной линии?

Практическая работа №4 «Обработка тональных сигналов набора номера»

1 Привести схему нерайонированной и районированной ГТС.

2 Что такое сигнализация, система сигнализации и протокол сигнализации.

3 Привести виды сигнализации в телефонных сетях по их функциональному назначению.

4 Привести классы систем межстанционной сигнализации.

5 Какие используются виды кодирования набора номера.

6 Чем характеризуются импульсный и тональный наборы номера.

Практическая работа №5 «Модификация тонального сигнала набора номера»

1 Что такое источники угрозы и уязвимость ТКС?

2 По каким четырем критериям классифицируют угрозы ТКС?

3 Что такое доступность информации и какие 4 типа угроз доступности выделяют?

4 Сколько различают видов угроз типа «отказ пользователей» и какие?

5Сколько различают видов угроз типа «внутренний отказ инфокоммуникационной системы» и какие?

6Сколько различают видов угроз типа «отказ поддерживающей инфраструктуры» и какие?

7 Что такое достоверность информации?

Практическая работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов»

1 Что такое конфиденциальность данных?

2 На сколько видов и каких можно разделить конфиденциальную информацию?

3 На сколько типов и каких можно разделить основные угрозы конфиденциальности информации?

4 На сколько видов и каких можно разделить технические угрозы?

5 Что такое перехват сообщений?

6 Сколько выделяют нетехнических угроз и каких?

7 Сколько вариантов и каких возможно для сокрытия (маскировки) аналоговых телефонных сигналов?

8 Сколько вариантов и каких возможно для сокрытия (маскировки) цифровых телефонных сигналов?

Критерии оценки:

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

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий;

недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

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

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

2ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Что такое защищенная телекоммуникационная система (ЗТС)?
a. Система защиты от вирусов
b. Система защиты от кражи учетных данных
c. Система, обеспечивающая безопасность передачи и хранения информации
d. Система, обеспечивающая ускорение работы телекоммуникационных сетей

2. Какие технологии обеспечивают защиту информации в ЗТС?
a. Технологии видеонаблюдения
b. Технологии пожарной сигнализации
c. Криптографические технологии
d. Технологии резервного копирования данных

3. Какие меры защиты должны быть реализованы в ЗТС для защиты от утечки данных?
a. Установка антивирусных программ
b. Шифрование передаваемых данных
c. Использование сильных паролей
d. Регулярное обновление операционной системы

4. Каковы требования к безопасности ЗТС при обработке и хранении конфиденциальной информации?
a. Использование публичных сетей для передачи данных
b. Использование закрытых каналов связи
c. Хранение паролей в открытом доступе
d. Установка стандартных настроек безопасности

5. Какие меры защиты должны быть приняты для защиты системы от атак на уязвимые места?
a. Использование устаревших операционных систем
b. Регулярное обновление системы и исправление уязвимостей
c. Разрешение доступа к системе нескольким пользователям
d. Использование открытых портов для доступа к системе

6. Что такое криптографические методы защиты и какие они бывают?
a. Методы защиты от взлома паролей
b. Методы защиты от физического доступа к серверам
c. Методы защиты от вирусов

d. Методы защиты информации при помощи шифрования и бывают симметричными и асимметричными

7. Каковы основные принципы обеспечения безопасности в ЗТС?
a. Конфиденциальность, доступность, прозрачность
b. Надежность, гибкость, экономичность
c. Конфиденциальность, целостность, доступность
d. Совместимость, универсальность, расширяемость

8. Какие меры безопасности должны быть реализованы при работе с удаленными рабочими местами?
a. Использование общих паролей для доступа к системе
b. Работа в открытой сети без использования VPN-каналов
c. Использование многофакторной аутентификации
d. Использование нелицензионных программных продуктов

9. Каковы требования к защите от несанкционированного доступа в ЗТС?
a. Использование открытых сетей для передачи данных
b. Регулярное обновление программного и аппаратного обеспечения
c. Установка слабых паролей для доступа к системе
d. Отсутствие физической защиты серверов и коммутационного оборудования

10. Какие методы шифрования информации применяются в ЗТС?
a. Методы шифрования на основе искусственного интеллекта
b. Симметричное и асимметричное шифрование
c. Методы шифрования на основе сжатия данных
d. Методы шифрования на основе кодирования сообщений

11. Какие меры безопасности должны быть реализованы для защиты от вирусов и других вредоносных программ в ЗТС?
a. Использование устаревших антивирусных программ
b. Отключение всех сетевых портов на серверах
c. Регулярное обновление антивирусного ПО и контроль за содержанием входящей почты
d. Использование паролей, содержащих только буквы латинского алфавита

12. Каковы основные принципы защиты информации в ЗТС?
a. Обеспечение доступности и скорости передачи данных
b. Уменьшение затрат на обслуживание системы
c. Обеспечение конфиденциальности, целостности и доступности данных

13. Какие меры безопасности должны быть реализованы для защиты от атак типа "отказ в обслуживании" (DoS)?
a. Использование устаревших версий программного обеспечения
b. Открытие всех портов на серверах

c. Ограничение скорости входящего трафика и установка программных и аппаратных брандмауэров
d. Использование паролей, которые легко подбираются

14. Какие меры безопасности должны быть реализованы при работе с мобильными устройствами в ЗТС?
a. Использование нелицензионного программного обеспечения
b. Запрет на скачивание и установку приложений из неофициальных источников
c. Использование коротких паролей для доступа к устройству
d. Работа в открытых сетях без использования VPN-каналов

15. Что такое "многофакторная аутентификация"?
a. Аутентификация на основе анализа поведения пользователя
b. Аутентификация на основе биометрических данных пользователя
c. Аутентификация с использованием двух или более факторов (например, пароль и смарт-карта.
d. Аутентификация с использованием только логина и пароля

16. Что такое "защита периметра" в ЗТС?
a. Защита от вирусов и других вредоносных программ
b. Защита от атак типа "отказ в обслуживании" (DoS)
c. Защита внешних границ системы с помощью брандмауэров, IPS/IDS и других средств
d. Защита данных от несанкционированного доступа

17. Что такое "защита в глубину" в ЗТС?
a. Защита от вирусов и других вредоносных программ
b. Многоуровневая защита системы, включающая как технические, так и организационные меры безопасности
c. Защита от атак типа "отказ в обслуживании" (DoS)
d. Защита периметра системы

18. Какие меры безопасности должны быть реализованы при работе с электронной почтой в ЗТС?
a. Использование криптографических протоколов для защиты от перехвата сообщений
b. Отправка паролей и другой конфиденциальной информации по электронной почте без дополнительной защиты
c. Работа с почтовыми клиентами, которые не поддерживают SSL/TLS
d. Использование одинаковых паролей для доступа к разным почтовым ящикам

19. Что такое "безопасность приложений" в ЗТС?
a. Защита от вирусов и других вредоносных программ

b. Защита от атак типа "отказ в обслуживании" (DoS)
c. Защита периметра системы
d. Защита от уязвимостей, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к системе

20. Что такое "отказоустойчивость" в ЗТС?
a. Способность системы к работе при неблагоприятных условиях (например, при сбоях в питании)
b. Способность системы к работе при атаках и других сбоях в работе
c. Способность системы к работе при высокой нагрузке
d. Способность системы к работе с большим количеством пользователей

21. Что такое "шифрование" в ЗТС?
a. Защита от вирусов и других вредоносных программ
b. Процесс преобразования данных в нечитаемый вид для защиты от несанкционированного доступа
c. Защита от атак типа "отказ в обслуживании" (DoS)
d. Защита периметра системы

22. Что такое "VPN" в ЗТС?
a. Способ защиты от вирусов и других вредоносных программ
b. Способ защиты от атак типа "отказ в обслуживании" (DoS)
c. Способ создания защищенного канала связи через открытые сети
d. Способ защиты периметра системы

23. Что такое "DMZ" в ЗТС?
a. Система обнаружения вторжений
b. Зона размещения общедоступных серверов внутри защищенной сети
c. Метод аутентификации пользователей
d. Метод шифрования данных

24. Какое устройство используется для обеспечения безопасности сети на уровне 2 OSI?
a. Коммутатор
b. Маршрутизатор
c. Фаервол
d. Сетевой мост

25. Какая атака заключается в использовании множества компьютеров для атаки на одну цель?
a. DDoS-атака
b. Сканирование портов
c. Фишинг-атака
d. Атака "человек посередине" (Man-in-the-middle)

26. Какой протокол используется для удаленного управления компьютерами в ЗТС?
a. FTP
b. HTTP
c. SSH
d. RDP

27. Какие меры безопасности должны быть реализованы при работе с удаленными рабочими станциями в ЗТС?
a. Использование общего пароля для доступа к удаленным компьютерам
b. Использование общего пользователя для доступа к удаленным компьютерам
c. Использование индивидуальных учетных записей для доступа к удаленным компьютерам
d. Открытый доступ к удаленным компьютерам без авторизации

28. Прокси-шлюзы прикладного уровня (выберите самое точное определение, один ответ)

a. Имеют базу данных пользователей, которым разрешен доступ к защищаемому ресурсу.
b. Имеют прокси-агента, являющегося посредником между клиентом и сервером.
c. Имеют базу данных IP-адресов, с которых разрешен доступ к защищаемому ресурсу.
d. Не разрывают TCP-соединение.

29. Персональные межсетевые экраны для настольных компьютеров и ноутбуков устанавливаются

a. На маршрутизаторах, которые указаны на хосте в качестве шлюза по умолчанию.
b. На конечных точках VPN.
c. На отдельных компьютерах.
d. На хостах, которые они защищают.

30. Выделенные прокси-серверы предназначены для того, чтобы обрабатывать трафик

a. Конкретного пользователя.
b. Конкретного уровня модели OSI.
c. Конкретного адреса отправителя.
d. Конкретного прикладного протокола.

31. Примеры IP-адресов, которые не должны появляться в пакетах

a. 192.168.254.0
b. 0.0.0.0
c. с 127.0.0.0 по 127.255.255.255
d. 192.168.0.254

32. NAT используется

a. В IPv32.
b. В IPv64.
c. В IPv6.
d. В IPv4.

33. Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

34. Как называется стандарт для виртуальных локальных сетей?

a. ieee 802.11
b. ieee 802.11i
c. ieee 802.1q
d. 802.1ad

35. Как называется стандарт, который позволяет пробрасывать vlan внутри другого vlan’a?

a. ieee 802.11
b. ieee 802.11i
c. ieee 802.1q
d. 802.1ad

36. Выберите верные утверждения в отношении vlan и netdefendos.

a. vlan id может назначаться только одному порту
b. vlan id может назначаться разным портам
c. если на одном коммутаторе разным портам присвоены разные значения vlan id, трафик подключенных vlan не будет изолирован

d. если на одном коммутаторе разным портам присвоены разные значения vlan id, трафик подключенных vlan будет изолирован

37. Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

a. виртуальная частная сеть
b. виртуальная локальная сеть
c. защищенная магистральная сеть
d. виртуальная канальная сеть

38. Как называется канал типа «точка-точка» в vpn-соединении?

a. шлюз
b. транк
c. туннель
d. мост

39. Что такое "фильтрация трафика" в ЗТС?
a. Метод защиты от атак типа "отказ в обслуживании" (DoS)
b. Метод аутентификации пользователей
c. Метод шифрования данных
d. Метод контроля трафика, направленный на блокировку нежелательного трафика

40. Что такое "DMVPN" в ЗТС?
a. Система обнаружения вторжений
b. Метод аутентификации пользователей
c. Метод шифрования данных
d. Технология, позволяющая создавать защищенные виртуальные частные сети на основе интернет-соединений

41. Какая атака заключается в перехвате информации, передаваемой по сети?
a. Сканирование портов
b. Атака "человек посередине" (Man-in-the-middle)

42. Одна из причин, по которой коммутаторы не должны использоваться для предоставления каких-либо возможностей межсетевого экрана
a. Коммутаторы не могут видеть передаваемый трафик.
b. Коммутаторы не могут предотвращать возможные DoS-атаки.
c. Коммутаторы не могут видеть порт, на который ушел пакет.
d. Коммутаторы не могут видеть порт, на который пришел пакет.

43. Основное свойство коммутаторов (выберите самое точное определение, один ответ)
a. Коммутаторы передают пакеты только нужному адресату.
b. Коммутаторы могут фильтровать трафик в зависимости от интерфейса, с которого ушел пакет.
c. Коммутаторы могут фильтровать трафик в зависимости от интерфейса, на который пришел пакет.
d. Коммутаторы могут фильтровать трафик в зависимости от типа трафика.

44. Политика безопасности – это (выберите самое точное определение, один ответ)
a. Совокупность административных мер, которые определяют порядок прохода в компьютерные классы.
b. Межсетевые экраны, используемые в организации.
c. Множество критериев для предоставления сервисов безопасности.
d. Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности

45. Основные классы атак на передаваемые по сети данные
a. Удаленная и локальная.
b. Видимая и невидимая.
c. Активная и пассивная.
d. Внешняя и внутренняя.

46. Атака называется пассивной, если
a. Оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.
b. Оппонент не предполагает проникновение в систему.
c. Оппонент не использует никаких инструментальных средств для выполнения атаки.
d. Оппонент не анализирует перехваченные сообщения.

47. Риск — это
a. Вероятность того, что в системе остались неизвестные уязвимости.
b. Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.
c. Невозможность ликвидировать все уязвимости в информационной системе.
d. Невозможность исправить все ошибки в программном обеспечении.

48. Возможные стратегии управления рисками
a. Избежать риск.
b. Принять риск.
c. Уменьшить риск.

d. Передать риск.

49. Целостность – это

e. Невозможность несанкционированного доступа к информации.
f. Невозможность несанкционированного выполнения программ.
g. Невозможность несанкционированного изменения информации.
h. Невозможность несанкционированного просмотра информации.

50. Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется

a. Конфиденциальностью.
b. Целостностью.
c. Аутентификацией.
d. Доступностью.

51. Многофакторная аутентификация означает

a. Аутентификация не может выполняться с помощью пароля.
b. Аутентификация должна выполняться с использованием смарт-карты.
c. Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.
d. Аутентификация должна выполняться третьей доверенной стороной.

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

a. Хищение жестких дисков, подключение к сети, инсайдерство
b. Перехват данных, хищение данных, изменение архитектуры системы
c. Хищение данных, подкуп системных администраторов, нарушение регламента работы

53. Виды информационной безопасности:

a. Персональная, корпоративная, государственная
b. Клиентская, серверная, сетевая
c. Локальная, глобальная, смешанная

54. Цели информационной безопасности – своевременное обнаружение, предупреждение:

d. несанкционированного доступа, воздействия в сети
e. инсайдерства в организации
f. чрезвычайных ситуаций

55. Основные объекты информационной безопасности:

g. Компьютерные сети, базы данных
h. Информационные системы, психологическое состояние пользователей
i. Бизнес-ориентированные, коммерческие системы

56. Основными рисками информационной безопасности являются:

j. Искажение, уменьшение объема, перекодировка информации

k. Техническое вмешательство, выведение из строя оборудования сети
l. Потеря, искажение, утечка информации

57. К основным принципам обеспечения информационной безопасности относится:
m. Экономической эффективности системы безопасности
n. Многоплатформенной реализации системы
o. Усиления защищенности всех звеньев системы

58. Основными субъектами информационной безопасности являются:
p. руководители, менеджеры, администраторы компаний
q. органы права, государства, бизнеса
r. сетевые базы данных, фаерволлы

59. К основным функциям системы безопасности можно отнести все перечисленное:
s. Установление регламента, аудит системы, выявление рисков
t. Установка новых офисных приложений, смена хостинг-компании
u. Внедрение аутентификации, проверки контактных данных пользователей

60. Принципом информационной безопасности является принцип недопущения:
v. Неоправданных ограничений при работе в сети (системе)
w. Рисков безопасности сети, системы
x. Презумпции секретности

61. Принципом политики информационной безопасности является принцип:
y. Невозможности миновать защитные средства сети (системы)
z. Усиления основного звена сети, системы
aa. Полного блокирования доступа при риск-ситуациях

62. Принципом политики информационной безопасности является принцип:
bb. Усиления защищенности самого незащищенного звена сети (системы)
cc. Перехода в безопасное состояние работы сети, системы
dd. Полного доступа пользователей ко всем ресурсам сети, системы

63. Принципом политики информационной безопасности является принцип:
ee. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
ff. Одноуровневой защиты сети, системы

gg. Совместимых, однотипных программно-технических средств сети, системы

64. Наиболее распространены угрозы информационной безопасности корпоративной системы:
hh. Покупка нелицензионного ПО
ii. Ошибки эксплуатации и неумышленного изменения режима работы системы
jj. Сознательного внедрения сетевых вирусов

65. Наиболее распространены угрозы информационной безопасности сети:
kk. Распределенный доступ клиент, отказ оборудования
ll. Моральный износ сети, инсайдерство
mm. Сбой (отказ) оборудования, нелегальное копирование данных

66. Наиболее распространены средства воздействия на сеть офиса:
nn. Слабый трафик, информационный обман, вирусы в интернет
oo. Вирусы в сети, логические мины (закладки), информационный перехват

67. Какой протокол используется для шифрования трафика в ЗТС?
a. FTP
b. HTTP
c. SSL/TLS
d. POP3

68. Что такое "централизованное управление доступом" в ЗТС?
a. Метод защиты от атак типа "отказ в обслуживании" (DoS)
b. Метод контроля доступа, при котором управление осуществляется централизованно
c. Метод шифрования данных
d. Метод аутентификации пользователей

69. Что такое защищенная телекоммуникационная система?
a. Система, которая защищает от несанкционированного доступа только телекоммуникационные сети
b. Система, которая обеспечивает безопасность передачи информации в телекоммуникационных сетях
c. Система, которая предназначена для ускорения передачи информации в телекоммуникационных сетях

70. Какие методы шифрования используются в защищенных телекоммуникационных системах?
a. Асимметричное шифрование
b. Симметричное шифрование
c. Гибридное шифрование

d. Все вышеперечисленные

71. Какие протоколы обеспечивают защиту информации в телекоммуникационных сетях?
a. TCP/IP
b. SSL/TLS
c. HTTP
д) FTP

72. Что такое VPN?
a. Виртуальная частная сеть
b. Сетевой протокол, который обеспечивает безопасность передачи данных через общедоступную сеть
c. Протокол передачи голоса в реальном времени
e) Программное обеспечение для управления базами данных

73. Какие меры безопасности используются в защищенных телекоммуникационных системах?
a. Контроль доступа
b. Аутентификация
c. Шифрование
d. Мониторинг сетевой активности
e. Все вышеперечисленные

74. Какая технология позволяет создавать виртуальные частные сети через Интернет?
a. VLAN
b. PPTP
c. FTP
d. VPN

75. Какой тип аутентификации рекомендуется использовать для защищенных телекоммуникационных систем?
a. Простая аутентификация
b. Двухфакторная аутентификация
c. Многократная аутентификация
d. Без аутентификации

76. Какой протокол используется для удаленного управления сетевыми устройствами в ЗТС?
a. SSH
b. FTP
c. SNMP
d. RDP

77. Что такое "физическая безопасность" в ЗТС?
a. Метод контроля доступа, при котором управление осуществляется централизованно
b. Меры безопасности, направленные на защиту физических объектов информационной системы, таких как серверные комнаты, кабинеты сетевых администраторов и т.д.
c. Метод защиты от атак типа "отказ в обслуживании" (DoS)
d. Метод шифрования данных

78. Какие меры безопасности рекомендуется применять для защиты сети от внешних атак?
a. Использование сложных паролей
b. Регулярное обновление антивирусных баз и операционной системы
c. Установка фаервола и контроля трафика
d. Использование открытых Wi-Fi-сетей для доступа в Интернет

79. Что такое "защищенная телекоммуникационная система"?
a. Система, которая не подвержена взлому.
b. Система, которая использует протоколы шифрования и другие меры безопасности для защиты передачи данных.
c. Система, которая используется только для обмена защищенными данными.

80. Какие протоколы шифрования часто используются в защищенных телекоммуникационных системах?
a. SSL и SSH
b. HTTP и SMTP
c. AES и RSA

81. Какие меры безопасности могут быть приняты в защищенных телекоммуникационных системах для защиты от взлома?
a. Ограничение доступа по IP-адресам
b. Установка антивирусного программного обеспечения
c. Обучение пользователей правилам безопасности

82. Какие методы могут быть использованы для защиты от DDoS-атак в защищенных телекоммуникационных системах?
a. Использование CDN
b. Установка фильтров пакетов
c. Регулярное обновление ПО

83. Какие основные задачи решает администратор защищенной телекоммуникационной системы?
a. Мониторинг системы безопасности
b. Управление пользователями и доступом к системе
c. Установка и настройка программного обеспечения

84. Что такое "бэкап" в контексте защищенных телекоммуникационных систем?
a. Зашифрованный файл, содержащий копию важной информации, который используется для восстановления данных в случае их потери или повреждения.
b. Программное обеспечение для шифрования данных, которые передаются по сети.
c. Специальное устройство для хранения защищенных данных.

85. Какие меры могут быть приняты для обеспечения безопасности паролей в защищенных телекоммуникационных системах?
a. Установка сложных паролей, которые состоят из букв, цифр и специальных символов
b. Требование смены пароля через определенный период времени
c. Использование двухфакторной аутентификации

86. Что такое "фаервол" в контексте защищенных телекоммуникационных систем?
a. Специальное устройство для шифрования данных, которые передаются по сети.
b. Программное обеспечение для защиты от несанкционированного доступа к сети.
c. Система для мониторинга и анализа трафика в сети.

87. Какие основные задачи решает команда безопасности в защищенных телекоммуникационных системах?
a. Мониторинг системы безопасности
b. Разработка и реализация политики безопасности
c. Оценка уязвимостей системы

88. Какие методы могут быть использованы для защиты от социальной инженерии в защищенных телекоммуникационных системах?
a. Регулярное обучение пользователей правилам безопасности
b. Ограничение доступа к конфиденциальной информации
c. Использование антивирусного программного обеспечения

89. Криптографические средства
a. средства защиты с помощью преобразования информации (шифровани.
b. правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.
c. нормы, традиции в обществе.

90. Аппаратно-программные средства защиты -

a. средства, в которых программные (микропрограммны и аппаратные части полностью взаимосвязаны и неразделимы.
b. средства защиты с помощью преобразования информации (шифровани.
c. это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.
d. предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем

91. Программные средства защиты –
a. предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.
b. предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем
c. это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

92. Физические средства защиты -
a. предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.
b. предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.
c. средства, в которых программные (микропрограммны и аппаратные части полностью взаимосвязаны и неразделимы.

93. Маскировка –это…
a. метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.
b. метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при

которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

94. Коммерческая тайна это…
a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
b. ограничения доступа в отдельные отрасли экономики или на конкретные производства
c. защищаемые банками и иными кредитными организациями сведения о банковских операциях
d. защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

95. Какая из перечисленных атак на поток информации является пассивной:
a. перехват.
b. имитация.
c. модификация.
d. фальсификация.
e. Прерывание

96. Что такое защищенная телекоммуникационная система?
a. Система, которая защищает от несанкционированного доступа к информации
b. Система, которая быстро передает информацию
c. Система, которая создает пул совместно используемых ресурсов

97. Какие методы обеспечивают безопасность защищенной телекоммуникационной системы?
a. Аутентификация и авторизация
b. Сжатие данных и ускорение передачи информации
c. Использование большого количества серверов

98. Какие угрозы могут появиться при использовании защищенной телекоммуникационной системы?
a. Несанкционированный доступ к информации
b. Перегрузка системы большим количеством данных
c. Утечка информации

99. Какие организации могут использовать защищенные телекоммуникационные системы?
a. Государственные организации
b. Частные компании

c. Школы и университеты

100. Что такое шифрование данных в защищенной телекоммуникационной системе?
a. Процесс преобразования информации в нечитаемую форму
b. Процесс ускорения передачи информации
c. Процесс создания резервных копий данных

Задания в открытой форме

1. Для обеспечения безопасности передачи данных в защищенных телекоммуникационных системах используются _____.
2. Одним из наиболее эффективных способов защиты информации является применение криптографических _____.
3. Криптография является наукой об организации защиты информации при помощи _____.
4. Шифрование – это процесс преобразования информации в форму, которую можно передать по открытому каналу связи без угрозы ее _____.
5. Для шифрования информации в защищенных телекоммуникационных системах используются различные методы и алгоритмы, например, алгоритм _____.
6. Для защиты передачи данных по сетям Интернет используются протоколы безопасности, такие как SSL и _____.
7. Защита от несанкционированного доступа к информации в защищенных телекоммуникационных системах осуществляется при помощи системы авторизации и _____.
8. Одним из методов защиты информации в защищенных телекоммуникационных системах является управление правами доступа пользователей при помощи _____.
9. В процессе администрирования защищенных телекоммуникационных систем необходимо обеспечить контроль целостности и _____ передаваемых данных.
10. Одной из ключевых задач при администрировании защищенных телекоммуникационных систем является обеспечение _____ информации от несанкционированного доступа.
11. Защищенные телекоммуникационные системы могут использоваться для передачи конфиденциальных данных, таких как _____ информация, финансовые данные и персональные данные пользователей.
12. Администраторы защищенных телекоммуникационных систем должны следить за уровнем _____ системы и быстро реагировать на любые потенциальные угрозы.
13. Шифрование является одним из основных методов защиты информации в защищенных телекоммуникационных системах и позволяет обеспечить _____ передачи данных.

14. В защищенных телекоммуникационных системах используются различные методы аутентификации, такие как парольная аутентификация, аутентификация на основе сертификатов и _____ аутентификация.
15. Для защиты от атаки на службу аутентификации в защищенных телекоммуникационных системах используется метод двухфакторной аутентификации, который включает использование пароля и _____.
16. Администраторы защищенных телекоммуникационных систем должны регулярно проводить аудит системы безопасности, чтобы обнаружить и устранить _____ в работе системы.
17. Для обеспечения защиты от вредоносного программного обеспечения в защищенных телекоммуникационных системах используется антивирусное ПО и _____.
18. В защищенных телекоммуникационных системах широко используются сертификаты безопасности, которые служат для проверки _____ и подлинности пользователей.
19. Для защиты сетевых соединений и передачи данных в защищенных телекоммуникационных системах используются VPN и _____.
20. Комплексное администрирование защищенных телекоммуникационных систем включает в себя не только технические аспекты, но и организационные меры по обеспечению безопасности информации, такие как разработка политик безопасности и _____.

Задание на установление правильной последовательности

1. Установите правильную последовательность действий при администрировании защищенных телекоммуникационных систем:
a) Проведение аудита системы безопасности
b) Установка антивирусного ПО
c) Настройка методов аутентификации
d) Обеспечение защиты от несанкционированного доступа

2. Расположите шаги в правильной последовательности для установки защиты от вредоносного программного обеспечения:
a) Установка брандмауэра
b) Установка антивирусного ПО
c) Установка средств контроля целостности файлов

3. Расположите шаги в правильной последовательности для установки защиты от утечки информации:
a) Установка средств контроля информации
b) Настройка методов шифрования
c) Проведение аудита системы безопасности

4. Установите правильную последовательность действий при обнаружении угрозы в защищенной телекоммуникационной системе:
a) Изолирование уязвимости
b) Оценка уровня угрозы
c) Принятие мер для устранения угрозы

5. Расположите шаги в правильной последовательности для установки методов аутентификации в защищенной телекоммуникационной системе:
a) Настройка методов аутентификации на основе сертификатов
b) Настройка парольной аутентификации
c) Настройка двухфакторной аутентификации

6. Установите правильную последовательность действий при настройке методов шифрования в защищенной телекоммуникационной системе:
a) Настройка асимметричного шифрования
b) Настройка симметричного шифрования
c) Настройка гибридного шифрования

7. Установите последовательность действий при аудите защищенной телекоммуникационной системы.

a) проверка уровня защиты
b) оценка рисков
c) составление отчета
d) оценка соответствия требованиям законодательства
e) анализ технических решений

8. Разместите действия в правильном порядке при обеспечении безопасности информации в защищенной телекоммуникационной системе.

a) внедрение мер безопасности
b) тестирование системы
c) оценка рисков определение угроз
d) разработка мер по уменьшению рисков

9. Назовите правильную последовательность действий при разработке проекта защищенной телекоммуникационной системы.

a) выбор компонентов
b) разработка программного обеспечения
c) тестирование системы.
d) определение требований
e) разработка архитектуры

10. Установите правильный порядок действий при создании политики безопасности в защищенной телекоммуникационной системе.

a) анализ уязвимостей
b) выбор мер безопасности
c) разработка политики безопасности
d) определение угроз
e) внедрение политики.

11. Разместите действия в правильном порядке при управлении доступом в защищенной телекоммуникационной системе.

a) назначение прав доступа
b) мониторинг доступа
c) идентификация и аутентификация пользователей
d) определение доступных ресурсов

12. Установите правильную последовательность действий при обеспечении конфиденциальности данных в защищенной телекоммуникационной системе.

a) настройка шифрования
b) проверка работоспособности шифрования
c) определение уровня конфиденциальности
d) выбор методов шифрования

13. Назовите правильный порядок действий при обеспечении целостности данных в защищенной телекоммуникационной системе.

a) определение методов контроля целостности
b) внедрение методов контроля целостности
c) проверка работоспособности методов контроля целостности
d) выбор методов контроля целостности

14. Разместите действия в правильном порядке при обеспечении доступности данных в защищенной телекоммуникационной системе.

a) выбор методов обеспечения доступности
b) настройка методов обеспечения
c) определение требований к доступности

15. Разместите действия в правильном порядке при управлении резервными копиями в защищенной телекоммуникационной системе.

a) создание резервных копий
b) тестирование процесса восстановления данных
c) обновление резервных копий
d) определение требований к резервным копиям
e) выбор методов создания резервных копий

16. Установите правильную последовательность действий при контроле целостности конфигурации защищенной телекоммуникационной системы.

a) анализ отклонений от контрольных точек
b) принятие мер по восстановлению целостности
c) установка программного обеспечения для контроля целостности
d) создание контрольных точек
e) регулярная проверка целостности

17. Назовите правильный порядок действий при мониторинге защищенной телекоммуникационной системы.

a) выбор программного обеспечения для мониторинга
b) установка и настройка программного обеспечения
c) проведение мониторинга
d) определение параметров мониторинга
e) анализ результатов мониторинга и принятие мер

18. Разместите действия в правильном порядке при обеспечении физической безопасности защищенной телекоммуникационной системы.

a) выбор методов обеспечения физической безопасности
b) установка и настройка системы контроля доступа
c) определение угроз физической безопасности
d) обучение персонала правилам безопасности
e) проведение регулярных проверок системы безопасности

19. Установите правильную последовательность действий при обучении персонала работе с защищенной телекоммуникационной системой.

a) разработка учебной программы
b) проведение обучения
c) проведение тестирования знаний
d) определение требований к обучению
e) повышение квалификации персонала по мере необходимости

20. Установите правильную последовательность действий при обеспечении защиты от вредоносного программного обеспечения в защищенной телекоммуникационной системе.

a) установка и настройка антивирусного ПО и брандмауэра
b) мониторинг наличия вредоносного ПО
c) анализ уязвимостей
d) выбор мер по защите от вредоносного ПО

Задание на установление соответствия

1. Сопоставьте технологии шифрования с их характеристиками:

1) Симметричное шифрование	a) преобразование данных в уникальную строку фиксированной длины
2) Асимметричное шифрование	b) используется два ключа – открытый и закрытый – для зашифровки и расшифровки данных соответственно
3) Хэширование	c) используется одинаковый ключ для зашифровки и расшифровки данных

2. Сопоставьте типы защиты средств связи с их описанием:

1) Шифрование трафика	a) контроль трафика, проходящего через сетевые устройства, с целью обнаружения и блокировки вредоносных пакетов
2) Защита от перехвата сигнала	b) защита данных, передаваемых по сети, путем их шифрования
3) Фильтрация сетевого трафика	c) защита средств связи от несанкционированного доступа и перехвата информации

3. Сопоставьте типы угроз информационной безопасности с их описанием:

1) Фишинг	a) вредоносное программное обеспечение, которое может нанести ущерб информационной системе и пользователям.
2) Социальная инженерия	b) метод получения конфиденциальной информации, основанный на мошенническом обмане пользователя.

3) Мальварь	c) метод атаки на информационную систему, основанный на манипуляции людьми, которые имеют доступ к системе.

4. Сопоставьте методы аутентификации с их примерами:

1) Парольная аутентификация	a) использование специальной карты для проверки подлинности пользователя
2) Аутентификация по карте доступа	a) использование отпечатка пальца для проверки подлинности пользователя.
3) Аутентификация по отпечатку пальца	b) проверка подлинности пользователя по паролю, который он вводит при входе в систему.

5. Сопоставьте типы авторизации с их описанием:

1) RBAC (Role-Based Access Control)	a) система контроля доступа, основанная на атрибутах пользователей, таких как должность, отдел, местоположение и другие факторы
2) ABAC (Attribute-Based Access Control)	b) система контроля доступа, основанная на определенных правилах (политиках), которые определяют, какие пользователи имеют доступ к определенным ресурсам и какие действия они могут выполнять с этими ресурсами.
3) PBAC (Policy-Based Access Control)	c) система контроля доступа, основанная на определенных ролях пользователей, которые имеют определенный уровень доступа.

6. Сопоставьте типы атак с их описанием:

1) DoS-атака	a) метод атаки на веб-приложение, основанный на вводе вредоносного скрипта в поля на сайте, который выполняется на компьютере пользователя при просмотре страницы.
2) SQL-инъекция	b) метод атаки на веб-приложение, основанный на вводе вредоносного SQL-кода в формы на сайте.
3) XSS-атака	c) атака на информационную систему, целью которой является перегрузка ее ресурсов до такой степени, что она

	становится недоступной для пользователей.

7. Сопоставьте типы защиты данных с их описанием:

1) Шифрование данных	a) метод защиты данных, основанный на проверке того, что данные не были изменены или повреждены в процессе передачи или хранения.
2) Резервное копирование данных	b) метод защиты данных, основанный на преобразовании их в зашифрованный вид, который может быть расшифрован только с помощью ключа.
3) Контроль целостности данных	c) метод защиты данных, основанный на регулярном создании копий данных, чтобы в случае их потери или повреждения можно было бы их восстановить.

8. 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

9. Установить соответствие:

1) Планирование	a) Отладка программы в соответствии с индивидуальными запросами конкретного предприятия базируется на контроле конфиденциальных сведений в соответствии с признаками особенной документации, принятой в компании
2) Реализация	b) Заключается в точном определении программы защиты данных. Ответ на простой, казалось бы, вопрос: «Что будем защищать?»
3) Корректировка	c) Проанализировав информацию, собранную на этапе тестовой эксплуатации DLP-решения, приступают к перенастройке ресурса.

10. Установить соответствие уровней технологий блокчейн:

1) Уровень приложений	a) В этом разделе вы получите доступ ко всем основным инструментам, которые помогут вам создать и запустить уровень dApps.
2) Уровень услуг	b) Он поставляется с dApps, браузером dApp, пользовательским интерфейсом и хостингом приложений.
3) Семантический уровень	c) На этом уровне присутствуют консенсусные алгоритмы, виртуальные машины, любые требования к участию и так далее.

11. Установить соответствие:

1) Угроза целостности	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.

3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	d) Это угроза изменения информации.

12. Установить соответствие:

1) Системность целевая	a) Подразумевает единство организации всех работ по защите информации и их управления.
2) Системность пространственная	b) Защищенность информации рассматривается как составная часть общего понятия качества информации.
3) Системность временная	c) Защищенность основанная на принципе непрерывности функционирования системы защиты
4) Системность организационная	d) Защищенность рассматривается как увязка вопросов защиты информации

13. Установить соответствие средств информационной защиты:

1) SIEM-системы	a) Виртуально-частная сеть определяет использование собственной частной сети внутри общедоступной. Поэтому ваше приложение, работающее по VPN, будет надежно защищено.
2) CloudAV	b) Они собирают информацию о возможных угрозах из различных источников: файервол, антивирус, межсетевой экран и др., потом проводят анализ и могут среагировать на вероятность возникновения потенциальной угрозы, предупредив о ней заранее.
3) Брандмаузер и фаервол	c) Это специальная система шифрования вашей информации. Шифровка происходит таким образом, что для того, чтобы расшифровать нужную информацию, необходимо обладать специальным шифром.
4) Криптографическое преобразование	d) Это специализированные средства, которые контролируют выход во

	всемирную паутину, при необходимости фильтруют или блокируют сетевой трафик.

14. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.
3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

15. 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

16. Установить соответствие:

1) Программно-аппаратные	a) Для обеспечения безопасности используются приемы «перестраховки», с помощью которых исключается

(технические) методы	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

17. Установить соответствие:

1) Рабочая станция	a) Специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
2) Сервер	b) Согласованный набор стандартных это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
3) Сетевая технология	c) Это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
4) Информационно-коммуникационная технология	d) Это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею

18. Сопоставьте типы сетевых архитектур с их описанием:

1) Централизованная архитектура	a) тип архитектуры, в которой сетевые ресурсы распределены по всей сети и управляются несколькими администраторами.

2) Децентрализованная архитектура	b) тип архитектуры, в которой сетевые ресурсы предоставляются в виде услуги из удаленного облачного центра.
3) Облачная архитектура	c) тип архитектуры, в которой все сетевые ресурсы находятся в одном центральном месте и управляются единственным администратором.

19.Сопоставьте типы топологии сети с их описанием:

1) Звездообразная топология	a) тип топологии сети, в которой все устройства подключены к одной линии передачи данных, и данные передаются от одного устройства к другому с помощью широковещательных сообщений.
2) Кольцевая топология	b) тип топологии сети, в которой устройства подключены в кольцевую форму, и данные передаются от одного устройства к другому в определенном порядке.
3) Шина	c) тип архитектуры, в которой все сетевые ресурсы находятся в одном центральном месте и управляются единственным администратором.

20.Сопоставьте типы тестирования безопасности с их описанием:

1) Тестирование на проникновение	a) метод тестирования безопасности, который сканирует систему или приложение на наличие уязвимостей, которые могут быть использованы злоумышленниками.
2) Тестирование на отказ в обслуживании	b) метод тестирования безопасности, который проверяет, как система или приложение реагирует на DoS-атаку.
3) Тестирование на уязвимости	c) метод тестирования безопасности, который пытается взломать систему или приложение, чтобы обнаружить уязвимости.

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

1. Рассчитать необходимую длину ключа для защиты передаваемых данных с помощью алгоритма AES, если требуется надежность не менее 128 бит.
2. Подсчитать количество возможных сочетаний символов в пароле, содержащем 8 символов и состоящем из заглавных и строчных букв английского алфавита, цифр и специальных символов.
3. Рассчитать допустимую максимальную длину сегмента кабеля в сети Ethernet с пропускной способностью 10 Gbit/s, если задержка распространения в среде передачи составляет 5 нс/м.
4. Подсчитать количество IP-адресов в подсети, имеющей маску подсети 255.255.255.192.
5. Рассчитать требуемую пропускную способность канала связи для передачи видео с разрешением 1080p при частоте кадров 60 кадров/сек, если предполагается использование кодека H.264 и компрессия на уровне 50%.
6. Подсчитать количество возможных перестановок ключа в алгоритме шифрования DES.
7. Рассчитать требуемую пропускную способность сети для передачи потока VoIP (голос по протоколу IP) для 100 одновременных пользователей, если предполагается использование кодека G.711 и

использование дополнительной пропускной способности в 20% для сетевых протоколов и протоколов управления трафиком.

8. Подсчитать количество доступных адресов для IPv6-сети, использующей префикс /64.

9. Рассчитать объем памяти, необходимый для хранения ключевой информации в защищенной телекоммуникационной системе с использованием алгоритма RSA и длиной ключа 2048 бит.

10. Подсчитать максимально возможное количество одновременных сессий VPN (виртуальной частной сети) при использовании шифрования AES-256 и ключа длиной 128 бит в защищенной телекоммуникационной системе с общим ресурсом процессора в 80% и объемом оперативной памяти в 8 ГБ.

11. Рассчитать время, необходимое для обнаружения и прекращения DDoS-атаки на сеть с использованием средств мониторинга и защиты от DDoS.

12. Определить количество необходимых каналов связи для организации резервированной связи в защищенной телекоммуникационной системе с гарантированным временем восстановления связи не более 10 минут.

13. Рассчитать объем трафика, передаваемого по сети за сутки, при использовании VoIP-системы для 1000 пользователей с учетом сжатия данных на 50%.

14. Определить максимально возможное количество пользователей, которые могут одновременно использовать VPN-сервер, используя аутентификацию по сертификату с длиной ключа 2048 бит при условии максимального времени ожидания ответа сервера в 3 секунды.

15. Рассчитать максимальное количество кадров в секунду, которое может обрабатывать маршрутизатор при использовании протокола OSPF и объеме оперативной памяти в 2 ГБ.

16. Определить минимально необходимое количество физических серверов для обеспечения отказоустойчивости в защищенной телекоммуникационной системе с гарантированным временем восстановления не более 15 минут при отказе одного из серверов.

17. Рассчитать максимальное количество пользователей, которые могут одновременно использовать виртуальную рабочую станцию в защищенной телекоммуникационной системе при использовании протокола RDP и объеме оперативной памяти в 16 ГБ.

18. Определить объем доступного дискового пространства для хранения лог-файлов за неделю в защищенной телекоммуникационной системе при использовании 5 серверов и ежедневном объеме лог-файлов в 500 МБ.

19. Рассчитать время, необходимое для обновления ПО на 50 серверах в защищенной телекоммуникационной системе при использовании системы удаленного управления и обновления ПО.

20. Определить объем трафика, передаваемого по VPN-соединению в защищенной телекоммуникационной системе при использовании шифрования AES-256 и длины ключа 128 бит для передачи файла размером 1 ГБ.

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.