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
Защита информации в компьютерных системах и сетях
(наименование дисциплины)

02.03.03 Математическое обеспечение и администрирование информационных систем, профиль «Математическое и информационное обеспечение экономической деятельности»
(код и наименование ОПОП ВО)

Курск – 2022

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Вопросы для устного опроса по теме 1

1. Классификация угроз информационной безопасности автоматизированных систем.

2. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.

3. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).

4. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: перехват сеанса (Session hijacking), отказ в обслуживании (Denial of Service, DoS), парольная атака полного перебора (brute force attack).

5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.

6. Основные характеристики спама и методы борьбы с ним.

7. Виды интернет - мошенничества: фишинг и фарминг и методы борьбы с ними.

8. Угрозы и уязвимости проводных корпоративных сетей.

9. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.

10. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: отказ в обслуживании, атаки типа “ человек в середине”, атака подмены ARP-записей, анонимный доступ в Интернет.

11. Способы обеспечения информационной безопасности компьютерных сетей. Фрагментарный и комплексный подходы.

12. Пути решения проблем защиты информации в сети Интернет. Информационная безопасность электронного бизнеса.

Вопросы для устного опроса по теме 2

13. Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности.

14. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности.

15. Основные этапы разработки политики безопасности.

Вопросы для устного опроса по теме 3

16. Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе паролей.

17. Аутентификация на основе PIN-кода.

18. Строгая аутентификация. Примеры протоколов аутентификации.

19. Биометрическая аутентификация пользователя.

20. Электронные системы идентификации и аутентификации.

21. Комбинированные системы идентификации и аутентификации.

Вопросы для устного опроса по теме 4

22. Основные функции и дополнительные возможности межсетевых экранов. Политика работы МЭ.

23. Особенности функционирования межсетевых экранов на уровнях модели OSI. Варианты исполнения МЭ.

24. Основные схемы подключения межсетевых экранов.

Вопросы для устного опроса по теме 5

25. Понятие компьютерного вируса. Классификация вирусов.

26. Специализированные утилиты для борьбы с вредоносным ПО: антишпионы, антируткиты и антикейлоггеры.

27. Троянские программы. Виды троянских программ.

28. Компьютерные черви. Виды компьютерных червей.

29. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”.

30. Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных

мониторов.

31. Антивирусные программы: утилита Dr. Web Curelt, программа Dr. Web., антивирус Avira AntiVir Personal, антивирус Avast! Home Edition.

32. Популярные пакеты антивирусной защиты: пакеты компании ESET (ESET NOD32 Antivirus, ESET NOD32 Smart Security), пакеты “Лаборатории Касперского” (Антивирус Касперского, Kaspersky Internet Security, Kaspersky Mobile Security).

Вопросы для устного опроса по теме 6

33. Концепция адаптивного управления безопасностью.

34. Средства анализа защищенности и общие требования к ним.

35. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак.

36. Обзор современных средств обнаружения атак. Продукты компании Internet Security Systems. Продукты компании Cisco Systems.

Вопросы для устного опроса по теме 7

37. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Показатели защищенности межсетевых экранов.

38. Классы защищенности автоматизированных систем.

39. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Защита конфиденциальной информации в АС и на рабочих местах пользователей ПК.

40. Требования к защите информации в локальных вычислительных сетях и при межсетевом взаимодействии. Требования к защите информации при работе с системами управления базами данных.

41. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Вопросы для устного опроса по теме 8

42. Понятие аудита безопасности информационных систем и цели его проведения. Стандарты, используемые при проведении аудита.

43. Основные этапы проведения аудита безопасности информационных

систем.

44. Анализ рисков и управление рисками. Методы оценки рисков и уровня защиты информационных систем.

45. Обзор программных продуктов для анализа и управления рисками: GRAMM, RiskWath, COBRA, ПО компании MethodWare, ПО “Аван Гард”.

Вопросы для устного опроса по теме 9

46. Защита информации сайта от несанкционированного доступа с помощью аутентификации.

47. Защита контента сайта от несанкционированного копирования.

48. Методы защиты сайта от DDos – атак.

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не может ответить на поставленные вопросы или допустил принципиальные ошибки в выполнении предусмотренных программой знаний;
- 1 балл выставляется обучающемуся, если доля правильных ответов от 50% до 90%;
- 2 балла выставляется обучающемуся, если доля правильных ответов более 90%.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1. Шифрование с помощью таблицы Виженера

1. Что такое шифр Цезаря?
2. В чем заключается метод Виженера?
3. Что такое частотный анализ?
4. Что такое мощность алфавита?
5. Как повысить криптостойкость метода Виженера?

Практическая работа №2. Фаервол COMODO FIREWALL.

1) Дайте определение межсетевого экрана.
2) Перечислите основные функции межсетевых экранов.
3) Перечислите основные схемы подключения межсетевых экранов.
4) Перечислите типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI.
5) Дайте классификацию межсетевых экранов.

Практическая работа №3. Антивирусная программа: Kaspersky Internet Secuirity

1. Дайте классификацию компьютерных вирусов.
2. В чем основное отличие вирусов-сценариев от файловых вирусов?
3. Существование каких вирусов зависит от конкретной программы?
4. В чем основное отличие троянской программы от вируса. Приведите пример троянской программы.
5. Дайте классификацию компьютерных червей. Приведите примеры компьютерных червей.

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не выполнил практическую работу.
- 2 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов от 50% до 90%.
- 4 балла выставляется обучающемуся, если студент выполнил практическую работу, доля правильных ответов более 90%.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1. Разработка обзорного документа по сертифицированным продуктам в заданной области информационной безопасности

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

Лабораторная работа №2. Разработка сайтов на языке JavaScript и обеспечение их информационной безопасности

1. Какие методы ввода и вывода информации существуют в языке JavaScript? Поясните на примерах. 4
2. Нужно ли при объявлении переменной в языке JavaScript указывать ее тип?
3. Каким образом можно вывести значение всех элементов массива в языке JavaScript?
4. Какие операторы языка JavaScript служат для реализации механизмов ветвления. Запишите общий вид этих операторов.
5. Какие операторы языка JavaScript служат для реализации механизмов цикла. Запишите общий вид этих операторов.

Лабораторная работа №3. Разработка и защита web-приложений с серверными сценариями на языке PHP

1. В чем отличие php-страницы от html-страницы?
2. Какие типы переменных поддерживает язык PHP?
3. Как передать переменную в php-страницу?
4. Какие параметры существуют у функции date()?
5. Для чего используется функция isset()?

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не выполнил лабораторную работу.
- 2 балла выставляется обучающемуся, если студент выполнил лабораторную работу, доля правильных ответов от 50% до 90%.
- 4 балла выставляется обучающемуся, если студент выполнил лабораторную работу, доля правильных ответов более 90%.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

Задание №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.

Задание №2

Какая сетевая атака является характерной именно для беспроводных сетей?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №3

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №4

Под политикой безопасности организации понимают:

1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №5

Политика удаленного доступа – это:

1. Специализированная политика безопасности.
2. Базовая политика безопасности.
3. Процедура безопасности.

4. Руководство по архитектуре безопасности.

Задание №6

Политики безопасности разделяют на уровни:
1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.
4. Нет разделения на уровни.

Задание №7

Под аутентификацией понимают:
1. Процедуру проверки подлинности заявленного пользователя, процесса, устройства.
2. Процедуру распознавания пользователя по его идентификатору.
3. Процедуру предоставления субъекту определенных полномочий и ресурсов в сети.
4. Регистрацию действий пользователя в сети.

Задание №8

Вероятность угадывания PIN –кода из 4 десятичных цифр за 3 попытки равна:
1. 0,0003.
2. 0,003
3. 0,00003.
4. 0,0004.

Задание №9

Различают следующие виды систем идентификации и аутентификации:
1. Электронные, биометрические и комбинированные.
2. Электронные и биометрические.
3. Электронные, биометрические и механические.
4. Электронные, биометрические и криптографические.

Задание №10

Какую функцию не может выполнять межсетевой экран?
1. Лечение файлов, зараженных вирусами.
2. Фильтрация трафика.
3. Трансляция сетевых адресов.
4. Регистрация событий.

Задание №11

Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности?

1. Комплексный межсетевой экран.
2. Экранирующий маршрутизатор.
3. Шлюз сеансового уровня.
4. Прикладной шлюз.

Задание №12

Различают следующие варианты исполнения межсетевых экранов:
1. Программный и программно-аппаратный.
2. Программный и аппаратный.
3. Аппаратный и программно – аппаратный.
4. Существуют только программные межсетевые экраны.

Задание №13

Какая вредоносная программа не размножается, но способна удаленно управлять компьютером и воровать пароли?
1. Троянская программа.
2. Червь.
3. Файловый вирус.
4. Макровирус.

Задание №14

Какая антивирусная программа не конфликтует с другими антивирусами, но не имеет функции автоматического обновления антивирусной базы?
1. Dr. Web Curelt.
2. Kaspersky Internet Security.
3. Eset NOD 32 Antivirus.
4. Avira AntiVir Personal.

Задание №15

Какой метод выявления вируса позволяет обнаруживать только известные вирусы?
1. Обнаружение, основанное на сигнатурах.
2. Обнаружение программ подозрительного поведения.
3. Обнаружение вирусов при помощи эмуляции работы программы.
4. Эвристический анализ.

Тема 6. Технологии анализа защищенности и обнаружения сетевых атак

Задание №16

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.

Задание №17

Какая сетевая атака является характерной именно для беспроводных сетей?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №18

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №19

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа?

1. 7.
2. 5.
3. 9.
4. 6.

Задание №20

Какой класс защищенности автоматизированных систем предъявляет наиболее высокие требования к информационной безопасности?

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №21

Вторая группа классов защищенности автоматизированных систем включает автоматизированные системы:

1. В которых работают несколько пользователей и все они имеют одинаковые права доступа к информации.
2. В которых работают несколько пользователей, и они имеют различные права доступа к информации.

3. В которых работает только один пользователь.
4. В которых работает один пользователь или несколько пользователей, имеющих одинаковые права доступа к информации.

Задание №22

Какой стандарт, используемый при проведении аудита, состоит из двух частей: “Практические рекомендации” и “Спецификации системы”?
1. Стандарт BS7799
2. Стандарт ISO17799
3. Стандарт ISO/IEC15408
4. Стандарт SysTrust

Задание №23

Какой этап проведения аудита является первым?
1. Инициирование и планирование процедуры аудита.
2. Сбор информации аудита.
3. Анализ данных аудита.
4. Оценка соответствия требованиям стандарта.

Задание №24

В каком методе анализа рисков рассчитываются минимальный и максимальный ущерб?
1. Оценка по верхним и нижним значениям.
2. Оценка рисков на этапе рассмотрения этапов вторжения.
3. Логарифмическая шкала.
4. Оценка на основе выявления слабого звена.

Задание №25

Каким атакам не подвергаются Web-сайты?
1. XSS атакам.
2. SQL инъекции.
3. DoS атакам.
4. Sniffing атакам.

Задание №26

По виду предоставляемой информации веб-приложения классифицируются на:
1. Статические и динамические.
2. Непрерывные.
3. Дискретные.

Задание №27

По степени связанности компонентов системы приложения делятся на:
1. Слабо сопряжённые.
2. Мало сопряжённые.
3. Средне сопряжённые.

Задание №28

Какие угрозы безопасности информации являются преднамеренными:
1. Открытие электронного письма, содержащего вирус.
2. Ошибка персонала.
3. Не авторизированный доступ.
4. Открытие сайта.

Задание №29
Заключительный этап построения системы защиты:
1. Планирование.
2. Сопровождение.
3. Анализ уязвимых мест.
4. Отчётность.

Задание №30
Под какие системы вирусы распространяются наиболее динамично:
1. Windows.
2. Mac OS.
3. Android.
4. Linux.

Задание №31
Какой вид идентификации и аутентификации является наиболее распространённым:
1. Одноразовые пароли.
2. Постоянные пароли.
3. системыPKI.

Задание №32
Основная масса угроз приходится на:
1. Шпионские программы.
2. Троянские программы.
3. Черви.

33. Основные составляющие информационной безопасности:

a. Целостность

b. Достоверность

c. Конфиденциальность

34. Доступность – это…

a. возможность за приемлемое время получить требуемую информационную услугу.

b. логическая независимость

c. нет правильного ответа

35. Целостность – это..

a. целостность информации

b. непротиворечивость информации

c. защищенность от разрушения

36. Конфиденциальность – это..

a. защита от несанкционированного доступа к информации

b. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

c. описание процедур

37. Для чего создаются информационные системы?

a. получения определенных информационных услуг

b. обработки информации

c. все ответы правильные

38. Целостность можно подразделить:

a. Статическую

b. Динамичную

c. структурную

39. Где применяются средства контроля динамической целостности?

a. анализе потока финансовых сообщений

b. обработке данных

c. при выявлении кражи, дублирования отдельных сообщений

40. Какие трудности возникают в информационных системах при конфиденциальности?

a. сведения о технических каналах утечки информации являются закрытыми

b. на пути пользовательской криптографии стоят многочисленные технические проблемы

c. все ответы правильные

41. Угроза – это…

a. потенциальная возможность определенным образом нарушить информационную безопасность

b. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

c. процесс определения отвечает на текущее состояние разработки требованиям данного этапа

42. Атака – это…

a. попытка реализации угрозы

b. потенциальная возможность определенным образом нарушить информационную безопасность

c. программы, предназначенные для поиска необходимых программ.

43. Источник угрозы – это..

a. потенциальный злоумышленник

b. злоумышленник

c. нет правильного ответа

44. Окно опасности – это…

a. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

b. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

c. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

45. Какие события должны произойти за время существования окна опасности?

a. должно стать известно о средствах использования пробелов в защите.

b. должны быть выпущены соответствующие заплаты.

c. заплаты должны быть установлены в защищаемой И.С.

46. Угрозы можно классифицировать по нескольким критериям:

a. по спектру И.Б.

b. по способу осуществления

c. по компонентам И.С.

47. По каким компонентам классифицируется угрозы доступности:

a. отказ пользователей

b. отказ поддерживающей инфраструктуры

c. ошибка в программе

48. Основными источниками внутренних отказов являются:

a. отступление от установленных правил эксплуатации

b. разрушение данных

c. все ответы правильные

49. Основными источниками внутренних отказов являются:

a. ошибки при конфигурировании системы

b. отказы программного или аппаратного обеспечения

c. выход системы из штатного режима эксплуатации

50. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

a. невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

b. обрабатывать большой объем программной информации

c. нет правильного ответа

51. Какие существуют грани вредоносного П.О.?

a. вредоносная функция

b. внешнее представление

c. способ распространения

Задания в открытой форме

1. … – это сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Назовите субъекты информационных отношений.
2. … информации заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.
3. ... свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.
4. … свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
5. Основные 7 принципов обеспечения информационной безопасности: …
6. Защита … – не разовое мероприятие, а непрерывный целенаправленный процесс, предполагаемый принятие соответствующих мер на всех этапах жизненного цикла защиты системы.
7. Важно правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми – это принцип …
8. на этапе разработки системы защиты в нее должна закладываться некая избыточность, которая позволила бы увеличить срок ее жизнеспособности – описывается принцип …
9. Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Это … меры защиты информации.

10. Нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий. Это … меры защиты информации.
11. Представляют собой мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Это … меры защиты информации.
12. Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты. Это … меры защиты информации.
13. Представляют из себя программное обеспечение, предназначенное для выполнения функций защиты информации. Это … меры защиты информации.
14. … - это отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации.
15. … - это отношения, возникающие при создании и использовании информационных технологий и средств их обеспечения
16. … - это отношения, возникающие при защите информации и прав субъектов, участвующих в информационных процессах и информатизации
17. … - это отношения, возникающие
18. Документированная информация представляет собой обыкновенные данные, а подход, отождествляющий информацию и данные, носит название «...».
19. К сведениям … следует относить такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.
20. К … сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства

или отраслям экономики РФ в одной или нескольких областях деятельности.

21. Понятие … тесно связано с понятием защиты информации и является реализацией системы защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы.

Задания на установление соответствия

1. Установить соответствие

1) Целостность	a) заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.
2) Доступность	b) свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
3) Конфиденциальность	c) свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

2. 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

3. Установить соответствие

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.
2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми.

4. Установить соответствие

1) Первый фактор	a) прочность существующего механизма защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода или преодоления.
2) Второй фактор	b) величина ущерба, наносимого владельцу АСОД в случае успешного осуществления угроз безопасности
3) Третий фактор	c) каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты

5. Установить соответствие мер защиты информации:

1) Правовые	a) Реализуются в виде механических, электрических и электронных устройств, предназначенных для

	препятствования проникновению и доступу потенциального нарушителя к компонентам защиты.
2) Морально-этические	b) Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3) Административные	c) К ним относятся нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий.
4) Технические	d) Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

6. Установить соответствие мер защиты информации:

1) К сведениям особой важности следует относить	a) Все иные из числа сведений, составляющих государственную тайну.
2) К совершенно секретным сведениям следует относить	b) Такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.
3) К секретным сведениям следует относить	c) Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

7. Установить соответствие

1) Коммерческая тайна	a) Служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством.
2) Служебная тайна	b) Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
3) Профессиональная тайна	c) Информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

8. Установить соответствие

1) Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	a) Мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).

3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
4) Постоянно проводимые мероприятия включают:	d) Мероприятия проводимые и повторяемые только при полном пересмотре принятых решений.

9. Установить соответствие

1) Общедоступные персональные данные	a) Это персональные данные, касающиеся расовой или национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья.
2) Специальные категории персональных данных	b) Это персональные данные, доступ к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
3) Биометрические персональные данные	c) Это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

10. Установить соответствие

1) Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	a) Мероприятия по непрерывной поддержке функционирования и управления используемыми средствами защиты.
2) Разовые мероприятия включают:	b) Анализ системных журналов и принятие мер по обнаруженным нарушениям правил работы.
3) Периодически проводимые мероприятия включают:	c) Мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АСОД.
4) Постоянно проводимые мероприятия включают:	d) Мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АСОД или внешней среде (мероприятия, проводимые по необходимости).

11. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные спетоскопы, установленные в смежном помещении
2) Акусто-вибрационный (через ограждающие кострукции)	b) Направленные микрофоны, установленные за границей КЗ
3) Акусто-электрический (через соединительные	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС,

линии ВТСС)	обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Защищенность рассматривается как увязка вопросов защиты информации

12. Установить соответствие технических каналов утечки информации:

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

13. Установить соответствие технических каналов утечки информации:

1) Прямой акустический (окна, двери, щели, проемы)	a) Электронные устройства перехвата речевой информации с датчиками микрофонного типа при условии неконтролируемого доступа к ним посторонних лиц
2) Акусто-оптический (через оконные стекла)	b) Лазерные акустические локационные системы, находящиеся за пределами КЗ
3) Акусто-электрический (через соединительные линии ВТСС)	c) Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4) Акусто-электромагнитный (параметрический)	d) Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

14. Установить соответствие дальности подавления диктофонов:

1) Аналоговые диктофоны	a) 5–6 м.
2) Цифровые диктофоны	b) Не более 1,5 м
3) Аналоговые диктофоны в металлическом корпусе	c) 4–5 м
4) Современные цифровые диктофоны в металлическом корпусе	d) Практически не подавляются

15. Установить соответствие

1) I группа	a) Блокираторы представляют собой генераторы помех с ручным управлением, обеспечивающие подстановку заградительной помехи в диапазоне частот работы базовых станций соответствующего стандарта (т.е. в диапазоне рабочих частот приемников телефонов сотовой связи). Помеха приводит к срыву управления сотовым телефоном базовой станции (потеря сети) и

	следовательно невозможности установления связи и передачи информации.
2) II группа	b) В своем составе кроме передатчика помех имеют еще специальный приемник, обеспечивающий прием сигналов в диапазонах частот работы передатчиков телефонных аппаратов соответствующего стандарта. Учитывая, что вся система сотовой связи работает в дуплексном режиме, специальный приемник используется как средство автоматического управления передатчиком помех. При обнаружении сигнала в одном из диапазонов частот приемник выдает сигнал управления на включения передатчика заградительных помех соответствующего диапазона частот. При пропадании сигнала приемник выдает сигнал управления на выключение сигнала помех соответствующего диапазона.
3) III группа	c) Так называемые «интеллектуальные блокираторы связи». На примере GSM: приемник блокиратора в течение короткого времени (примерно 300 мкс) обнаруживает в КЗ излучение входящего в связь мобильного телефона, вычисляет номер частотного канала и временной слот, выделяемый данному телефону.

16. Установить соответствие:

1) Косвенные каналы	a) связанные с доступом к элементам АСОД, но не требующие изменения компонентов системы.
2) Прямые каналы	b) не связанные с физическим доступом к элементам АСОД.
3) Прямые каналы	c) связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.

17. Установить соответствие:

1) Нарушитель	a) намеренно идущий на нарушение из корыстных побуждений.
2) Злоумышленник	b) 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	c) Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам.

18. Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	4) Знает структуру, функции и механизмы действия

	средств защиты, их слабые и сильные стороны.
5) 4 уровень	6) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

19. Установить соответствие нарушителей по времени действия:

1) 3 уровень	a) В период неактивности компонентов системы (нерабочее время, перерывы, ремонт и т.п.).
2) 2 уровень	b) Во время функционирования АСОД (во время работы компонентов системы).
3) 1 уровень	c) Как в процессе функционирования АСОД, так и в период неактивности системы.

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

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

Задания на установление правильной последовательности

1. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
    1. Опытная и промышленная эксплуатация
    2. Проектный этап
    3. Аттестация или декларирование
    4. Предпроектный этап

2. Выберите правильную последовательность этапов в жизненном цикле атаки:
    1. Выбор способа атаки
    2. Закрепление
    3. Эксплуатация
    4. Достижение цели
    5. Исполнение команд
    6. Разведка и сбор данных
    7. Доставка

3. Выберите правильную последовательность этапов разработки профиля защиты.
    1. Анализ среды применения ИТ-продукта с точки зрения
    2. безопасности.
    3. Выбор профиля-прототипа.
    4. Синтез требований.

4. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
    1. Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
    2. Реализация защитных мер по противодействию скрытых каналов
    3. Организация контроля за противодействием скрытых каналов.
    4. Выявление скрытых каналов и оценка их опасности для активов организации

5. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:
    1. Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;
    2. Определение и выработка политики информационной безопасности;
    3. Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;
    4. Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;

5. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

6. Установите последовательность этапов работы по обеспечению информационной безопасности:

1. Определение требований к системе защиты информации;
2. Выбор контрмер, обеспечивающих режим иб, и средств защиты;
3. Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;
4. Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

7. Выберите правильную последовательность этапов процесса управления рисками:

1. идентификация активов и ценности ресурсов, нуждающихся в защите;
2. анализ угроз и их последствий, определение слабостей в защите;
3. классификация рисков, выбор методологии оценки рисков и проведение оценки;
4. выбор, реализация и проверка защитных мер;
5. оценка остаточного риска;
6. выбор анализируемых объектов и степени детальности их рассмотрения;

8. Выберите правильную последовательность этапов обеспечения информационной:

1. оценка стоимости;
2. реализация политики;
3. квалифицированная подготовка специалистов;
4. аудит;
5. разработка политики безопасности;

9. Выберите правильную последовательность этапов развития информационной безопасности до первой половину 20-го века:

1. Характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
2. Связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).
3. Связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в

этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

4. Связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

10. Выберите правильную последовательность этапов развития информационной безопасности после первой половины 20-го века:

1. Обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.
2. Связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.
3. Связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

11. Выберите последовательность уровней защищенности персональных данных

1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

12. Выберите последовательность уровней безопасности информации:

1. Административный уровень
2. Процедурный уровень
3. Программно-технический уровень

4. Законодательный уровень

13. Выберите последовательность проведения моделирования угроз:

1. Определение негативных последствий от угроз безопасности информации.
2. Определение объектов воздействия угроз безопасности информации.
3. Оценка возможности реализации угроз и их актуальности.

14. Выберите правильную последовательность этапов оценки угроз безопасности информации:

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

15. Выберите правильную последовательность этапов построения политики безопасности:

1. Выбор и установка средств защиты;
2. Организация обслуживания по вопросам информационной безопасности;
3. Создание системы периодического контроля информационной безопасности
4. Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
5. Подготовка персонала работе со средствами защиты;

16. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:

1. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
2. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
3. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
4. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

17. Установите этапы существования оборудования ИБ:

1. Установка.
2. Эксплуатация.
3. Выведение из эксплуатации.
4. Инициация.
5. Закупка.

18. Выберите правильную последовательность этапов построения системы защиты:

1. Анализ
2. Реализация системы защиты
3. Сопровождение системы защиты.
4. Разработка системы защиты

19. Выберите последовательность приоритетных этапов защиты информации:

1. Защита информации от несанкционированного доступа;
2. Защита информации в системах связи;
3. Защита юридической значимости электронных документов;
4. Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
5. Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
6. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

20. Устранение уязвимости состоит из следующих этапов:

1. Инсталляция программного модуля для устранения угрозы информационной безопасности.
2. Разработка «патча» (заплатки), призванного устранить существующий пробел.
3. Появление сигнала от пользователей или от администратора сети о наличии слабого места в информационной системе.

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

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).

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

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

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

6. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в США в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Yahoo! и Яндекс.

7. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в Японии в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Google и Яндекс.

8. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в США в 2019 г. материалов по антивирусным программам в информационно-поисковых системах Rambler и Google.

9. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в ФРГ в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Google.

10. Рассчитать коэффициент Танимото и коэффициент корреляции и определить эффективность поиска страниц, связанных с разработками и публикациями в России в 2019 г. материалов по документальным БД в Internet в информационно-поисковых системах Яндекс и Rambler.

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.