МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

_____ М.О. Таныгин
(подпись)

«31» 08 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине

Защита информации
(наименование дисциплины)

38.03.01 Экономика, профиль «Бухгалтерский учет, анализ и аудит»
(код и наименование ОПОП ВО)

Курск – 2021

Задание для проведение текущего контроля успеваемости

Юго-Западный государственный университет

Кафедра информационной безопасности

Вопросы для собеседования

по дисциплине «Защита информации»

(наименование дисциплины)

Тема №1 «Базовые понятия»

1. Какой смысл несёт в себе словосочетание «информационная безопасность»?
2. Что такое информационная безопасность?
3. Что такое защита информации?
4. Какой смысл отражает в себе понятие – угрозы информационной безопасности?
5. От чего зависит информационная безопасность?
6. Что такое ущерб и в каком значении это слово употребляется в определении информационной безопасности?
7. Компьютерная безопасность, это информационная безопасность? Ответ объясните
8. Что такое доступность?
9. Что такое целостность?
10. Что такое конфиденциальность?
11. На какие два направления можно разделить понятие целостности?
12. О чем говориться в Доктрине информационной безопасности Российской федерации?
13. Что из себя представляет жизненный цикл ИС?

Тема №2 «Конфиденциальность. Классификация угроз»

1. Что такое угроза?

2. Как называют людей, предпринимающих попытки реализации угрозы?
3. Какой промежуток времени называют окном опасности?
4. По каким критериям производится классификация угроз?
5. Можно ли использовать несколько критериев для классификации одной угрозы? Ответ объясните
6. Перечислите основные источники внутренних отказов.
7. Приведите пример угрозы доступности.
8. Является ли удаленное потребление ресурсов угрозой?
9. Что понимается под конфиденциальной информацией?
10. Что такое вирус?
11. Что такое червь?
12. Перечислите основные угрозы целостности
13. Перечислите основные угрозы конфиденциальности
14. Какое назначение имеет перечень конфиденциальных сведений предприятия?
15. Какие угрозы наносят наибольший ущерб субъектам информационных отношений?

Тема №3 «Угрозы ИБ. Классы нарушителей. Оценка риска»

1. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
2. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
3. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
4. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
5. Каким образом классифицируются каналы утечки информации?

6. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
7. Что такое скрытые каналы утечки информации и как их обнаружить?

Тема №4 «Персональные данные. Защита авторских прав»

1. Что такое персональные данные?
2. Что из себя представляют авторские права?
3. Что такое обработка персональных данных?
4. Что включает в себя обработка персональных данных?
5. Перечислите основные принципы обработки персональных данных
6. Какая глава Гражданского кодекса описывает основные составляющие такого понятия как авторское право

Тема №5 «Выявление контрафактной продукции»

1. Что такое контрафактная продукция?
2. Перечислите оптимальные методы контроля и защиты информационных систем?
3. На основе каких критериев оценки следует выбирать средства защиты?
4. Что такое лицензирование программных продуктов и для чего оно производится?
5. Перечислите основные этапы лицензирования

Тема №6 «Криптографические методы защиты»

1. Приведите пример сервисов безопасности
2. Что такое криптография?
3. Что включает в себя понятие криптографическая защита информации?

4. Какие виды преобразования информации вы знаете?
5. Перечислите основные способы преобразования информации
6. Шифры каких видов вам знакомы?
7. Что из себя представляют потоковые шифры?
8. Что такое скремблирование?
9. Чем отличаются симметричные и ассиметричные шифры?
10. Что такое клеточный автомат и какое отношение это понятие имеет к шифрованию?

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не может ответить на поставленные вопросы.

- 2 балла выставляется обучающемуся, если доля правильных ответов от 50% до 90%.

-4 балла выставляется обучающемуся, если доля правильных ответов более 90%.

Составитель А.Л. Марухленко

«___» _____ 2021г.

Юго-Западный государственный университет

Кафедра информационной безопасности

Контрольные вопросы для защиты

практических работ

по дисциплине «Защита информации»

(наименование дисциплины)

Контрольные вопросы для защиты практической работы №1.

1. Перечислите основные обязанности администратора безопасности
2. Какие программные и аппаратные средства позволяют идентифицировать и оценивать возможные риски в сети?
3. Проанализируйте как GFI LANguard защищает против червей.
4. При каких обстоятельствах GFI LANguard вывод диалог во время патча.
5. Вы можете изменить сообщение, выведенное на экран, когда GFI LANguard выполняет административные задачи? Если да, то как?

Контрольные вопросы для защиты практической работы №2.

1. Что из себя представляет полиалфавитное шифрование?
2. Чьи труды были взяты за основу Шифра Виженера?
3. Опишите процесс шифрования
4. Опишите процесс дешифрования
5. В данный момент, шифр уязвим к криптоанализу?
6. Какой вклад внёс Гилберт Вернам по отношению к шифру?

Контрольные вопросы для защиты практической работы №3.

1. Что такое скремблирование?
2. Каким требованиям должен удовлетворять двоичный сигнал для синхронной передачи?
3. Назовите один из способов обработки двоичных посылок

4. В каких видах систем применяется скремблирование?
5. Перечислите основные типы скремблеров и дескремблеров

Контрольные вопросы для защиты практической работы №4.

1. Что представляет собой алгоритм RSA?
2. Почему шифр RSA называется ассиметричным?
3. По какой формуле производится шифрование
4. По какой формуле производится дешифрование
5. В чем заключается криптостойкость алгоритма?
6. Что из себя представляют открытый и закрытый ключ?

Контрольные вопросы для защиты практической работы №5.

1. Что такое клеточный автомат?
2. В каких сферах деятельности принимаются клеточные автоматы?
3. Какое отношение имеют клеточные автоматы к информационной безопасности?
4. Кем была разработана игра «Жизнь»?
5. Какие алгоритмы применяются в функциях?

Контрольные вопросы для защиты практической работы №6.

1. Что в себя включает понятие защита программного обеспечения?
2. Какими инструментами пользуются злоумышленники для исследования программ?
3. Что такое отладчик?
4. Что такое дизассемблер?
5. Для чего используют шифрование исполняемого файла?
6. Какие методы используются для обнаружения модифицированного кода?

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не выполнил работу.

- 3 балла выставляется обучающемуся, если студент выполнил работу и доля правильных ответов от 50% до 90%.

- 6 балла выставляется обучающемуся, если студент выполнил работу и доля правильных ответов более 90%.

Составитель А.Л. Марухленко

«___» _____ 2021г.

7Юго-Западный государственный университет

Кафедра информационной безопасности

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

по дисциплине «Защита информации»

(наименование дисциплины)

Задания в закрытой форме

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   a. Разработка аппаратных средств обеспечения правовых данных
   b. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   c. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2. 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
3. Виды информационной безопасности:
   a. Персональная, корпоративная, государственная
   b. Клиентская, серверная, сетевая
   c. Локальная, глобальная, смешанная
4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   a. несанкционированного доступа, воздействия в сети
   b. инсайдерства в организации

c. чрезвычайных ситуаций

5. Основные объекты информационной безопасности:
   a. Компьютерные сети, базы данных
   b. Информационные системы, психологическое состояние пользователей
   c. Бизнес-ориентированные, коммерческие системы
6. Основными рисками информационной безопасности являются:
   a. Искажение, уменьшение объема, перекодировка информации
   b. Техническое вмешательство, выведение из строя оборудования сети
   c. Потеря, искажение, утечка информации
7. К основным принципам обеспечения информационной безопасности относится:
   a. Экономической эффективности системы безопасности
   b. Многоплатформенной реализации системы
   c. Усиления защищенности всех звеньев системы
8. Основными субъектами информационной безопасности являются:
   a. руководители, менеджеры, администраторы компаний
   b. органы права, государства, бизнеса
   c. сетевые базы данных, фаерволлы
9. К основным функциям системы безопасности можно отнести все перечисленное:
   a. Установление регламента, аудит системы, выявление рисков
   b. Установка новых офисных приложений, смена хостинг-компании
   c. Внедрение аутентификации, проверки контактных данных пользователей
10. Принципом информационной безопасности является принцип недопущения:
   a. Неоправданных ограничений при работе в сети (системе)

b. Рисков безопасности сети, системы
c. Презумпции секретности

11. Принципом политики информационной безопасности является принцип:

a. Невозможности миновать защитные средства сети (системы)
b. Усиления основного звена сети, системы
c. Полного блокирования доступа при риск-ситуациях

12. Принципом политики информационной безопасности является принцип:

a. Усиления защищенности самого незащищенного звена сети (системы)
b. Перехода в безопасное состояние работы сети, системы
c. Полного доступа пользователей ко всем ресурсам сети, системы

13. Принципом политики информационной безопасности является принцип:

a. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b. Одноуровневой защиты сети, системы
c. Совместимых, однотипных программно-технических средств сети, системы

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

a. Компьютерный сбой
b. Логические закладки («мины»)
c. Аварийное отключение питания

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

a. Прочитать приложение, если оно не содержит ничего ценного – удалить
b. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

c. Удалить письмо с приложением, не раскрывая (не читая) его

16. Принцип Кирхгофа:
    a. Секретность ключа определена секретностью открытого сообщения
    b. Секретность информации определена скоростью передачи данных
    c. Секретность закрытого сообщения определяется секретностью ключа
17. ЭЦП – это:
    a. Электронно-цифровой преобразователь
    b. Электронно-цифровая подпись
    c. Электронно-цифровой процессор
18. Наиболее распространены угрозы информационной безопасности корпоративной системы:
    a. Покупка нелицензионного ПО
    b. Ошибки эксплуатации и неумышленного изменения режима работы системы
    c. Сознательного внедрения сетевых вирусов
19. Наиболее распространены угрозы информационной безопасности сети:
    a. Распределенный доступ клиент, отказ оборудования
    b. Моральный износ сети, инсайдерство
    c. Сбой (отказ) оборудования, нелегальное копирование данных
20. Наиболее распространены средства воздействия на сеть офиса:
    a. Слабый трафик, информационный обман, вирусы в интернет
    b. Вирусы в сети, логические мины (закладки), информационный перехват
    c. Компьютерные сбои, изменение администрирования, топологии
21. Утечкой информации в системе называется ситуация, характеризуемая:

a. Потерей данных в системе
b. Изменением формы информации
c. Изменением содержания информации

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

a. Целостность
b. Доступность
c. Актуальность

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

a. Вероятное событие
b. Детерминированное (всегда определенное) событие
c. Событие, происходящее периодически

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

a. Регламентированной
b. Правовой
c. Защищаемой

25. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

a. Программные, технические, организационные, технологические
b. Серверные, клиентские, спутниковые, наземные
c. Личные, корпоративные, социальные, национальные

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

a. Владелец сети
b. Администратор сети
c. Пользователь сети

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

a. Руководств, требований обеспечения необходимого уровня безопасности

b. Инструкций, алгоритмов поведения пользователя в сети
c. Нормы информационного права, соблюдаемые в сети

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

a. Аудит, анализ затрат на проведение защитных мер
b. Аудит, анализ безопасности
c. Аудит, анализ уязвимостей, риск-ситуаций

29. Под информационной безопасностью понимается…

a. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
b. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
c. нет правильного ответа

30. Защита информации – это..

a. комплекс мероприятий, направленных на обеспечение информационной безопасности.
b. процесс разработки структуры базы данных в соответствии с требованиями пользователей
c. небольшая программа для выполнения определенной задачи

31. От чего зависит информационная безопасность?

a. от компьютеров
b. от поддерживающей инфраструктуры
c. от информации

32. Основные составляющие информационной безопасности:

a. Целостность
b. Достоверность

c. конфиденциальность

33. Доступность – это…

a. возможность за приемлемое время получить требуемую информационную услугу.
b. логическая независимость
c. нет правильного ответа

34. Целостность – это..

a. целостность информации
b. непротиворечивость информации
c. защищенность от разрушения

35. 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

36. Для чего создаются информационные системы?

a. получения определенных информационных услуг
b. обработки информации
c. все ответы правильные

37. Целостность можно подразделить:

a. Статическую
b. Динамичную
c. структурную

38. Где применяются средства контроля динамической целостности?

a. анализе потока финансовых сообщений
b. обработке данных
c. при выявлении кражи, дублирования отдельных сообщений

39. 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

40. 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

41. Атака – это…
a. попытка реализации угрозы
b. потенциальная возможность определенным образом нарушить информационную безопасность
c. программы, предназначенные для поиска необходимых программ.

42. Источник угрозы – это..
a. потенциальный злоумышленник
b. злоумышленник
c. нет правильного ответа

43. 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

44. 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.

45. Угрозы можно классифицировать по нескольким критериям:

a. по спектру И.Б.
b. по способу осуществления
c. по компонентам И.С.

46. По каким компонентам классифицируется угрозы доступности:

a. отказ пользователей
b. отказ поддерживающей инфраструктуры
c. ошибка в программе

47. Основными источниками внутренних отказов являются:

a. отступление от установленных правил эксплуатации
b. разрушение данных
c. все ответы правильные

48. Основными источниками внутренних отказов являются:

a. ошибки при конфигурировании системы
b. отказы программного или аппаратного обеспечения
c. выход системы из штатного режима эксплуатации

49. 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

50. Какие существуют грани вредоносного П.О.?

a. вредоносная функция

b. внешнее представление
c. способ распространения

51. По механизму распространения П.О. различают:
a. Вирусы
b. Черви
c. все ответы правильные

52. Вирус – это…
a. код обладающий способностью к распространению путем внедрения в другие программы
b. способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
c. небольшая программа для выполнения определенной задачи

53. Черви – это…
a. код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
b. код обладающий способностью к распространению путем внедрения в другие программы
c. программа действий над объектом или его свойствами

54. Конфиденциальную информацию можно разделить:
a. Предметную
b. Служебную
c. глобальную

55. Природа происхождения угроз:
a. Случайные
b. Преднамеренные
c. природные

56. Предпосылки появления угроз:
a. Объективные

b. Субъективные
c. преднамеренные

57. К какому виду угроз относится присвоение чужого права?
a. нарушение права собственности
b. нарушение содержания
c. внешняя среда

58. Отказ, ошибки, сбой – это:
a. случайные угрозы
b. преднамеренные угрозы
c. природные угрозы

59. Отказ - это…
a. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
b. некоторая последовательность действий, необходимых для выполнения конкретного задания
c. структура, определяющая последовательность выполнения и взаимосвязи процессов

60. Ошибка – это…
a. неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
b. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
c. негативное воздействие на программу

61. Сбой – это…
a. такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
b. неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
c. объект-метод

62. Побочное влияние – это…
    a. негативное воздействие на систему в целом или отдельные элементы
    b. нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
    c. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
63. СЗИ (система защиты информации) делится:
    a. ресурсы автоматизированных систем
    b. организационно-правовое обеспечение
    c. человеческий компонент
64. Что относится к человеческому компоненту СЗИ?
    a. системные порты
    b. администрация
    c. программное обеспечение
65. Что относится к ресурсам А.С. СЗИ?
    a. лингвистическое обеспечение
    b. техническое обеспечение
    c. все ответы правильные
66. По уровню обеспеченной защиты все системы делят:
    a. сильной защиты
    b. особой защиты
    c. слабой защиты
67. По активности реагирования СЗИ системы делят:
    a. Пассивные
    b. Активные
    c. полупассивные
68. Правовое обеспечение безопасности информации – это…

a. совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
b. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
c. нет правильного ответа

69. Правовое обеспечение безопасности информации делится:
a. международно-правовые нормы
b. национально-правовые нормы
c. все ответы правильные

70. Информацию с ограниченным доступом делят:
a. государственную тайну
b. конфиденциальную информацию
c. достоверную информацию

71. Что относится к государственной тайне?
a. сведения, защищаемые государством в области военной, экономической … деятельности
b. документированная информация
c. нет правильного ответа

72. Вредоносная программа - это…
a. программа, специально разработанная для нарушения нормального функционирования систем
b. упорядочение абстракций, расположение их по уровням
c. процесс разделения элементов абстракции, которые образуют ее структуру и поведение

73. Основополагающие документы для обеспечения безопасности внутри организации:
a. трудовой договор сотрудников
b. должностные обязанности руководителей

c. коллективный договор

74. К организационно - административному обеспечению информации относится:

a. взаимоотношения исполнителей
b. подбор персонала
c. регламентация производственной деятельности

75. Что относится к организационным мероприятиям:

a. хранение документов
b. проведение тестирования средств защиты информации
c. пропускной режим

76. Какие средства используется на инженерных и технических мероприятиях в защите информации:

a. Аппаратные
b. Криптографические
c. физические

77. Программные средства – это…

a. специальные программы и системы защиты информации в информационных системах различного назначения
b. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
c. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

78. Криптографические средства – это…

a. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

b. специальные программы и системы защиты информации в информационных системах различного назначения
c. механизм, позволяющий получить новый класс на основе существующего

79. По отношению к защищаемой информации существуют следующие угрозы:

a. несанкционированный доступ
b. утечка
c. сокрытие
d. разглашение

80. Клавиатурные шпионы применяются злоумышленником для ...

a. Отслеживания журнала посещения
b. Определения прав доступа пользователей ОС
c. Перехвата паролей пользователей операционной системы
d. Определения количества пользователей

81. Защита информации - это ...

a. совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой
b. состояние информации, при котором изменять её могут только уполномоченные лица
c. комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации
d. данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность

82. Для любой информационной системы характерны следующие понятия:

a. непредвиденное обстоятельство
b. происшествие

c. злоумышленник

d. уязвимость

e. угроза

83. В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:

a. внешние

b. параметрические

c. электрические

d. дистанционные

e. электромагнитные

84. Что означает слово "конфиденциальный" в переводе с латинского?

a. безопасность

b. доверие

c. хранение

d. защита

e. По источникам появления угрозы подразделяют на:

f. внешние и внутренние

g. естественные и искусственные

h. пользовательские и сетевые

85. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

a. Авторизация

b. Аутентификация

c. Обезличивание

d. Деперсонализация

e. Идентификация

86. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

a. Авторизация
b. Обезличивание
c. Деперсонализация
d. Аутентифика́ция
e. Идентификация

87. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом

a. Авториза́ция
b. Идентификация
c. Аутентификация
d. Обезличивание
e. Деперсонализация

88. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

a. Токен
b. Password
c. Пароль
d. Login
e. Смарт-карта

89. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

a. Идентификация
b. Аутентификация
c. Авторизация

d. Экспертиза
e. Шифрование

90. Для безопасной передачи данных по каналам интернет используется технология:

a. Www
b. Dicom
c. Vpn
d. Ftp
e. Xml

91. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

a. Антивирус
b. Замок
c. Брандма́уэр
d. Криптография
e. Экспертная система

92. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:

a. Дисциплинарные взыскания
b. Административный штраф
c. Уголовная ответственность
d. Лишение свободы
e. Смертная казнь

93. Несанкционированный доступ к информации это:

a. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально

b. Работа на чужом компьютере без разрешения его владельца
c. Вход на компьютер с использованием данных другого пользователя
d. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
e. Доступ к субд под запрещенным именем пользователя

94. «Персональные данные» это:

a. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
b. Фамилия, имя, отчество физического лица
c. Год, месяц, дата и место рождения, адрес физического лица
d. Адрес проживания физического лица
e. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

95. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:

a. Выход в интернет без разрешения администратора
b. При установке компьютерных игр
c. В случаях установки нелицензионного по
d. В случае не выхода из информационной системы
e. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

96. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:

a. Нет, только к административной ответственности
b. Нет, если это государственное предприятие
c. Да

d. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
e. Да, но только в случае осознанных неправомочных действий сотрудника

97. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

a. Идентификация
b. Аутентификация
c. Стратификация
d. Регистрация
e. Авторизация

98. Наиболее опасным источником угроз информационной безопасности предприятия являются:

a. Другие предприятия (конкуренты)
b. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
c. Рядовые сотрудники предприятия
d. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
e. Хакеры

99. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:

a. Нет, не при каких обстоятельствах
b. Нет, но для отправки срочных и особо важных писем можно
c. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
d. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем

e. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

100. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:

a. Информация составляющая государственную тайну
b. Информация составляющая коммерческую тайну
c. Персональная
d. Конфиденциальная информация
e. Документированная информация

Задания в открытой форме

1. Информация как предмет защиты.
2. Субъекты информационных отношений.
3. Организация системы защиты информации.
4. Комплексная защита информационных систем
5. Работа с конфиденциальными данными.
6. Угрозы информационной безопасности.
7. Модель поведения нарушителя.
8. Классификация угроз
9. Угрозы утечки по техническим каналам, уязвимости каналов взаимодействия.
10. Анализ сетевого трафика.
11. Сканирование сети.
12. Угрозы выявления пароля.
13. Подмена доверенного объекта.
14. Внедрение ложного объекта.
15. Отказ в обслуживании.
16. Обработка персональных данных.

17. Выявление контрафактной продукции.

18. Выбор оптимальных методов контроля и защиты информационной систем.

19. Лицензирование программных продуктов.

20. Интеграция механизмов защиты в программное обеспечение для борьбы с НСД.

21. Основы криптографии, методы защиты.

22. Классификация криптографических методов.

23. Потоковые шифры.

24. Скремблирование.

25. Ассиметричные шифры.

26. Клеточные автоматы

Задание на установление правильной последовательности

1. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:

   a. Опытная и промышленная эксплуатация
   b. Проектный этап
   c. Аттестация или декларирование
   d. Предпроектный этап

2. Выберите правильную последовательность этапов в жизненном цикле атаки:

   a. Выбор способа атаки
   b. Закрепление
   c. Эксплуатация
   d. Достижение цели
   e. Исполнение команд
   f. Разведка и сбор данных
   g. Доставка

Задание на установление соответствия

1. Установить соответствие

1) RSA	a) семейство криптографических алгоритмов — однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224
2) DES	b) криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел
3) SHA-2	c) алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3)

2. Установить соответствие

1) Mail-Worm	a) У данного типа червей, как и у почтовых червей, существуют два способа распространения червя по IRC-каналам, повторяющие способы, описанные выше.
2) IM-Worm	b) черви, распространяющиеся в формате сообщений электронной почты.
3) P2P-Worm	c) прочие сетевые черви, среди которых имеет смысл дополнительно выделить интернет-черви и LAN-черви
4) IRC-Worm	d) черви, распространяющееся при помощи пиринговых (peer-to-peer) файлообменных сетей.
5) Net-Worm	e) черви, использующие интернет-пейджеры.

Компетентностно-ориентированные задачи

1. Зашифровать исходный текст используя шифрование с помощью таблицы Виженера
2. Зашифровать исходный текст используя шифр RSA
3. Зашифровать исходный текст используя алгоритм шифрования Эль-Гамаля
4. Зашифровать исходный текст используя алгоритм шифрования Деффи-Хеллмана
5. Подпишите документ используя ЭЦП
6. Включите шифрование твердотельного накопителя используя операционную систему Windows 10
7. Воспользовавшись операционной системой Linux произведите сканирование локальной сети на поиск подозрительных устройств
8. Опишите модель поведения нарушителя для административного корпуса завода ООО «СтройМаш»
9. Не имея непосредственного доступа к персональному компьютеру, совершите удаленный запуск приложений на нём
10. Произведите установку антивирусного программного обеспечения на персональный компьютер