**Примерные оценочные материалы, применяемые при проведении**

**текущей аттестации по дисциплине**

**«Защита программ и данных»**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на тестовые вопросы из нижеприведенного списка.

1.В качестве аутентификатора в сетевой среде могут использоваться:А) координаты субъекта
Б) фамилия субъекта
В) несекретный ключ
Г) секретный криптографический ключ

2. Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в ИС 2 и 3 классов защищенности ФСТЭК:

А) не реже 1 раза в 2 года;

Б) не реже 1 раза в год;

В) не реже 1 раза в 6 месяцев;

Г) не регламентируется;

3.Кто является основным ответственным за определение уровня классификации информации?А) руководитель среднего звена
Б) высшее руководство
В) пользователь

Г) владелец

4. Основная цель мер безопасности, предпринимаемых на административном уровне:А) отчитаться перед вышестоящими инстанциями
Б) выполнить положения действующего законодательства
В) сформировать программу безопасности и обеспечить ее исполнение
Г) классификация ресурсов

5. Что такое защита информации?А) недопущение несанкционированного доступа к информации
Б) комплекс мероприятий, направленных на обеспечение информационной безопасности
В) использование антивирусных программ
Г) использование средств аутентификации

6. Сколько классов защищенности ИС устанавливает ФСТЭК России для информации, не составляющей государственную тайну:

А) 3;

Б) 4;

В) 5;

Г) 7;

7. Кто, в конечном счете, несет ответственность за гарантии того, что данные классифицированы и защищены?А) руководство
Б) владельцы данных
В) пользователи

Г) администраторы

8. Перехват данных является угрозой:А) конфиденциальности
Б) уязвимости
В) целостности
Г) доступности

9. Вирусы, заражающие файлы-документы и электронные таблицы популярных офисных приложений, называют:
А) резидентными вирусами
Б) макровирусами
В) стелс-вирусами
Г) загрузочными вирусами

10. Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности, это:
А) аутентификация
Б) идентификация
В) авторизация
Г) самоидентификация

11. Уникальная последовательность символов, предназначенная для создания электронной подписи, называется:
А) Ключ электронной подписи
Б) Квалифицированный сертификат проверки ключа электронной подписи
В) Ключ проверки электронной подписи

Б) Сертификат открытого ключа

12. В международных стандартах выделяют:

А) 3 класса безопасности информационных систем;

Б) 4 класса безопасности информационных систем;

В) 5 классов безопасности информационных систем;

Г) 7 классов безопасности информационных систем;

13. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?А) выполнение анализа рисков

Б) поддержка
В) определение цели и границ

Г) делегирование полномочий

14. Журнал регистрации доступа не предусмотрен в ИС с классом безопасности:

А) B1;

Б) С1;

В) С2;

Г) B2;

15. Согласно ФЗ «Об информации, информационных технологиях и о защите информации», информация – это:
А) сведения (сообщения, данные), информирующие о событиях, действиях, фактах
Б) сведения (сообщения, данные) независимо от формы их представления
В) сведения (сообщения, данные) независимо от формы их передачи

Г) сведения (сообщения, данные) независимо от формы их получения

16. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц – это:
А) распространение информации
Б) предоставление информации
В) документирование информации

Г) первичная обработка информации

17. Защита информации это:

А) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее

Б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа
В) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

Г) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

18. В международных стандартах выделяют:

А) 3 уровня безопасности информационных систем;

Б) 4 уровня безопасности информационных систем;

В) 5 уровней безопасности информационных систем;

Г) 7 уровней безопасности информационных систем;

19. Совокупность свойств информации, характеризующих степень ее соответствия потребностям пользователя, это:
А) универсальность информации
Б) массовость информации
В) качество информации

Г) корреляция информации

20. Увеличение размера скрываемого сообщения в контейнере фиксированной емкости:

А) не влияет на надежность сокрытия;

Б) может влиять, все зависит от содержания скрываемого сообщения;

В) понижает надежность сокрытия;

Г) повышает надежность сокрытия.

21. Объектами государственной информационной политики не являются:

А) печатные средства массовой информации
Б) программное обеспечение
В) информационная безопасность

Г) средства связи

22. Естественные угрозы безопасности информации вызваны:

А) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

Б) деятельностью человека
В) ошибками при проектировании ИС, ее элементов или разработке ПО;

Г) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

23. Сколько категорий значимости объектов критической информационной инфраструктуры устанавливается в РФ:

А) две
Б) три
В) четыре

Г) пять

24. Какая информация может быть отнесена к коммерческой тайне:

А) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица
Б) информация о ведущих специалистах предприятия и местах их работ
В) о составе имущества государственного или муниципального унитарного предприятия

Г) о задолженности работодателей по выплате заработной платы

25. Какая информация не может быть отнесена к коммерческой тайне:

А) о перечне основных заказчиков работ коммерческого предприятия
Б) о задолженности работодателей по выплате заработной платы
В) о тематике работ, выполняемых предприятием

Г) ценовая и сбытовая политика предприятия

26. К средствам защиты информации не относятся:

А) аппаратные;

Б) организационные;

В) химическиие;

Г) психологические.

27. Искусственные угрозы безопасности информации вызваны:

А) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

Б) деятельностью человека
В) ошибками при проектировании ИС, ее элементов или разработке ПО;

Г) корыстными устремлениями злоумышленников

28. Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах; это:

А) файл
Б) электронный документ
В) электронное сообщение

Г) электронная база данных

29. Распространение персональных данных:

А) действия, направленные на раскрытие персональных данных определенному кругу лиц
Б) действия, направленные на раскрытие персональных данных неопределенному кругу лицВ) действия, направленные на передачу персональных данных на территорию иностранного государства

Г) действия, направленные на передачу персональных данных на территории РФ и на территории иностранных государств

30. К посторонним лицам, нарушителям информационной безопасности относятся:

А) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации

Б) представители конкурирующих организаций
В) персонал, обслуживающий технические средства;

Г) пользователи

31. В стеганографиилюбая информация, предназначенная для сокрытия тайных сообщений **-** это:

А) стегоключ;

Б) стеганосистема;

В) контейнер;

Г) сообщение, встраиваемое в контейнер.

32. К методам обеспечения информационной безопасности НЕ относятся:

А) организационно-технические,

Б) экономические

В) правовые

Г) информационные

33. Организационно-технические методы обеспечения информационной безопасности НЕ включают

А) внутренние правила работы с данными, регламент передачи сведений, доступ к ним ,

Б) разработку новых средств защиты информации

В) перманентный контроль над действенностью принимаемых мер в области обеспечения информационной безопасности

Г) метрологический контроль ПО, используемого на предприятии.

34. Правовые методы обеспечения информационной безопасности НЕ включают

А) лицензирование деятельности в части обеспечения информационной безопасности;

Б) сертификацию технических средств информационной защиты;

В) аттестацию объектов информатизации согласно соответствию нормам информационной безопасности РФ;

Г) стандартизацию выходной документации предприятия.

35. К стандартам информационной безопасности не относятся:

А) Рекомендации по стандартизации;

Б) ГОСТы;

В) Руководящие документы ФСТЭК;

Г) Международные стандарты.

36. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п.:

А) пустые письма,

Б) нигерийские письма

В) фишинг

Г) черный пиар

37. К способам нейтрализации угроз информационной безопасности не относятся:

А) Правовые;

Б) Информационные;

В) Программно-технические;

Г) Организационные.

38. Каких видов электронной подписи не существует:

А) простая неквалифицированная

Б) усиленная неквалифицированная

В) усиленная квалифицированная

Г) простая.

39. Какой закон определяет виды электронных подписей:

А) Об электронной цифровой подписи,

Б) [Об электронной подписи](https://www.diadoc.ru/docs/laws/N63-fs)

В) Об информации, информационных технологиях и защите информации

Г) О персональных данных.

40. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы.:

А) сторож,

Б) сканер

В) доктор

Г) детектор

41.Наука о тайной передаче информации путем сокрытия самого факта передачи **-** это:

А) защита информации;

Б) стеганография;

В) криптография;

Г) имитозащита.

42. Аллюзия - это:

А) использование фраз, которые предполагаются известными тому, к кому обращена речь, и неизвестными посторонним лицам;

Б) тайное сообщение, в котором шифрообозначениями являются любые символы, кроме букв и цифр;

В) тайное сообщение, состоящее из первых букв строк стихотворений;

Г) тайное сообщение, в котором слова или буквы сообщения записываются в определенных позициях.

43**.** Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние**:**

А) сторож,

Б) сканер

В) доктор

Г) детектор

44. Пустышечный шифр - это:

А) использование фраз, которые предполагаются известными тому, к кому обращена речь, и неизвестными посторонним лицам;

Б) тайное сообщение, в котором шифрообозначениями являются любые символы, кроме букв и цифр;

В) тайное сообщение, состоящее из первых букв строк стихотворений;

Г) тайное сообщение, в котором слова или буквы сообщения записываются в определенных позициях.

45. Акростих - это:

А) использование фраз, которые предполагаются известными тому, к кому обращена речь, и неизвестными посторонним лицам;

Б) тайное сообщение, в котором шифрообозначениями являются любые символы, кроме букв и цифр;

В) тайное сообщение, состоящее из первых букв строк стихотворений;

Г) тайное сообщение, в котором слова или буквы сообщения записываются в определенных позициях.

46. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

А) сторож,

Б) сканер

В) ревизор

Г) детектор

47. Наука о методах обеспечения конфиденциальности и аутентичности информации - это:

А) защита информации;

Б) стеганография;

В) криптография;

Г) имитозащита.

48. Видоизменение текста документа таким образом, что только тот или те, для кого текст документа предназначен, были в состоянии восстановить исходный текст:

А) шифрование документа;

Б) рецензирование документа;

Б) редактирование документа;

Г) защита информации.

49. Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ- это:

А) асимметричное шифрование;

Б) криптографическая система с открытым ключом;

В) блочное шифрование;

Г) симметричное шифрование.

50.Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов**:**

А) сторож,

Б) сканер

В) ревизор

Г) детектор

51. К способам защиты информации не относится:

А) управление;

Б) регламентация;

В) редактирование;

Г) принуждение.