**Примерные оценочные материалы, применяемые при проведении**

**промежуточной аттестации по дисциплине**

**«Антивирусная защита»**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на 50 тестовых вопросов из нижеприведенного списка.

1. **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

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

А) нормированной  
Б) регламентированной  
В) правовой  
Г) защищаемой

**3. Что из перечисленного не относится к числу основных угроз информационной безопасности?**А) целостность  
Б) защита от копирования  
В) доступность  
Г) конфиденциальность

**4. Что необходимо сделать при выведении из эксплуатации устройства хранения информации?**А) осуществить гарантированное стирание остаточной информацииБ) сохранить устройство в безопасном месте  
В) физически уничтожить устройство  
Г) осуществить гарантированное стирание остаточной информации и физически уничтожить устройство

**5. Политика безопасности строится на основе:**  
А) сбора сведений о сотрудниках  
Б) анализа рисков  
В) изучения политик схожих организаций  
Г) тестирования знаний сотрудников

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

А) прочитать приложение, если оно не содержит ничего ценного – удалить  
Б) сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама  
В) выяснить формат приложенного файла и его размер  
Г) удалить письмо с приложением, не раскрывая (не читая) его

**7. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?**

А) аутентичность  
Б) доступность  
В) целостность  
Г) конфиденциальность

**8. К какой категории персональных данных можно отнести адресную книгу?:**

А) биометрические

Б) специальные

В) дополнительные

Г) общедоступные

**9. Выберите тип вредоносных программ:**  
А) шпионское, рекламное программное обеспечение  
Б) Microsoft Office  
В) операционная система Linux

Г) Windows Defender

**10. 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

**11. Основные угрозы доступности информации:**

А) злонамеренное изменение данных  
Б) хакерская атака  
В) перехват данных  
Г) непреднамеренные ошибки пользователей

**12. Наиболее эффективное средство для защиты от сетевых атак:**

А) использование антивирусных программ  
Б) посещение только «надёжных» Интернет-узлов  
В) использование только сертифицированных программ-браузеров при доступе к сети Интернет  
Г) использование сетевых экранов или «firewall»

**13. Следствием наличия уязвимостей в информационной системе является:**

А) атака  
Б) угроза  
В) нападение  
Г) необходимость замены компонентов системы

**14. Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации?**

А) законодательный  
Б) административный  
В) процедурный  
Г) программно-технический

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

А) две  
Б) три  
В) четыре

Г) пять

**16. На каком уровне защиты информации находятся непосредственно средства защиты?**

А) законодательный  
Б) административный  
В) процедурный  
Г) программно-технический

**17. Анализ защищенности информационных систем проводится с помощью:**

А) сканеров безопасности  
Б) браузеров  
В) межсетевых экранов  
Г) команды ping

**18. 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

**19. 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

**20. 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

**21. 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

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

А) владелец сети  
Б) администратор сети  
В) пользователь сети  
Г) провайдер

**23. 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

**24. Согласно ФЗ «О персональных данных», персональные данные это:**  
А) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу  
Б) сведения (сообщения, данные), независимо от формы их представления  
В) данные, находящиеся в персональной собственности физического лица  
Г) информация о заработках физического лица

**25. Ограничение доступа к информации может устанавливаться:**

А) Указом Президента РФ

Б) Федеральным законом

В) Постановлением Правительства РФ

Г) Конституциями (Уставами) субъектов РФ

**26. 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

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

А) три

Б) четыре

В) пять

Г) семь

**28. Перехват данных является угрозой:**А) конфиденциальности  
Б) уязвимости  
В) целостности  
Г) доступности  
**29. Вирусы, заражающие файлы-документы и электронные таблицы популярных офисных приложений, называют:**  
А) резидентными вирусами  
Б) макровирусами  
В) стелс-вирусами  
Г) загрузочными вирусами

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

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

**32. Информация, составляющая государственную тайну, не может иметь гриф**

А) «для служебного пользования»

Б) «секретно»

В) «совершенно секретно»

Г) «особой важности»

**33. Утечка информации – это**

А) несанкционированный процесс переноса информации от источника к злоумышленнику

Б) процесс раскрытия секретной информации

В) процесс уничтожения информации

Г) непреднамеренная утрата носителя информации

**34. 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

**35. 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

**36. Межсетевой экран это:**

А) устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем

Б) сетевое устройство, используемое для установления и управления потоками данных между различными сетями путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации

В) вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

Г) устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика

**37. Ограничение прав пользователей по вводу информации в информационную систему обязательно выполняется для систем**

А) 1 класса защищенности

Б) 1 и 2 класса защищенности

В) 1, 2, 3 классов защищенности

Г) 2 и 3 классов защищенности

**38. Способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ- это:**

А) асимметричное шифрование

Б) криптографическая система с открытым ключом

В) блочное шифрование

Г) симметричное шифрование

**39. Политика сетевой безопасности это:**

А) формальный процесс обнаружения вторжений, обычно характеризующийся сбором сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, включая то, когда и как это произошло

Б) совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как должна обеспечиваться защита ее сетевой инфраструктуры и сервисов

В) документ, отражающий позицию руководства по обеспечению информационной безопасности в соответствии с требованиями основной деятельности организации и правовыми и регулирующими нормами

Г) процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и предупреждения об опасности, и связанный с этим анализ

**40. Следствием наличия уязвимостей в информационной системе является:**

А) атака  
Б) угроза  
В) нападение  
Г) необходимость замены компонентов системы

**41. Коммутатор это:**

А) Устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика

Б) Устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем

В) Сетевое устройство, используемое для установления и управления потоками данных между различными сетями путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации

Г) Вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности

**42. Что такое «инструментальные средства аудита»**

А) автоматизированные инструментальные средства, помогающие анализировать содержание журналов событий

Б) автоматические инструментальные средства, помогающие анализировать содержание журналов событий В) любые технические средства, используемые в ходе аудита

Г) программно-технические средства, реализующие анализ документов, представленных для проведения аудита

**43. Маршрутизатор это:**

А) Вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности

Б) Сетевое устройство, используемое для установления и управления потоками данных между различными сетями путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации

В) Устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем

Г) Устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика

**44. Утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами:**  
А) Руткит   
Б) Бэкап  
В) Камбэк

Г) Xdelta

**45. Отличительными способностями компьютерного вируса являются:**  
А) способность к самостоятельному запуску и многократному копированию кода   
Б) значительный объем программного кода  
В) легкость распознавания

Г) способность к восстановлению зараженных файлов

**46. Компьютерные вирусы:**  
А) являются следствием ошибок в операционной системе  
Б) пишутся людьми специально для нанесения ущерба пользователем ПК   
В) возникают в связи со сбоями в аппаратных средствах компьютера

Г) являются следствием ошибок в программах-интерпретаторах

**47. Сетевые черви бывают:**  
А) Web-черви  
Б) черви операционной системы  
В) черви MS Office

Г) черви Photoshop

**48. Какие вирусы активизируются в самом начале работы с операционной системой:**  
А) загрузочные вирусы

Б) троянцы  
В) черви

Г) стелс-вирусы

**49. Для периодической проверки компьютера на наличие вирусов используется:**  
А) компиляция  
Б) антивирусное сканирование  
В) дефрагментация диска

Г) программа-интерпретатор

**50. Как называется вирус, попадающий на компьютер при работе с электронной почтой:**  
А) текстовый  
Б) сетевой +  
В) файловый

Г) почтовый