**Тестовое задание Защита информации»**

1. ***Информационная безопасность – это***
	1. защищенность информационной среды предприятия от внешних угроз ее формированию, использованию и развитию
	2. защищенность информационной среды предприятия от внутренних угроз ее формированию, использованию и развитию
	3. защищенность информационной среды предприятия от внешних и внутренних угроз ее формированию, использованию и развитию
2. ***Информационная безопасность – это процесс соблюдения аспектов (атрибутов безопасности):***
	1. эргономичности, конфиденциальности
	2. своевременности, доступности, целостности
	3. эргономичности, релевантности, целостности
	4. доступности, целостности, конфиденциальности
3. ***Доступность информации – это свойство информации***
	1. соответствовать нуждам, запросам пользователя
	2. возможность проведения всех операций по обработке информации (чтение, изменение, сохранение, пересылка и др.)
	3. такое понятие относится только к информации, размещенной в сети Интернет
4. ***Целостность информации – это…***
	1. правило, предполагающее сохранение информации на электронных и бумажных носителях
	2. понятие может относиться только к организации в целом, включая всю информацию данной организации
	3. соответствие логической структуры информации определенным правилам, причем, процессы обработки информации не должны нарушать общую структуру
5. ***Конфиденциальность информации – это возможность…***
	1. только чтения информации, без ее обработки
	2. доступа к информации определенного круга лиц в соответствии с установленными правилами
	3. доступа к информации за определенную плату
6. ***Угроза – это…***
	1. действия, которые привели к нарушению безопасности информации
	2. некоторое потенциально возможное нарушение безопасности информации
	3. такое понятие относится только к компьютерным вирусам
7. ***Атака – это…***
	1. действия, целью которых является нарушение безопасности информации
	2. только те действия, которые уже привели к нарушение безопасности информации
	3. такое понятие относится только к компьютерным вирусам
8. ***Превентивные меры по обеспечению безопасности информации предполагают…***
	1. любые действия по обеспечению безопасности информации
	2. действия, направленные на организацию защиты, упреждающе (т.е. до того момента, когда проблема возникла)
	3. действия на уровне антивирусных средств
	4. действия на уровне доступа пользователей к ресурсам организации
9. ***Закон «О персональных данных»***
	1. 152 – ФЗ
	2. 153 – ФЗ
	3. 157 – ФЗ
	4. 62 – ФЗ
10. ***Персональные данные – это (выберите наиболее полный ответ)…***
	1. фамилия, имя, отчество
	2. адрес местожительства
	3. данные паспорта
	4. любая информация, относящаяся к физическому лицу
11. ***Общедоступные персональные данные – это (выберите наиболее полный ответ)…***
	1. любые персональные данные
	2. персональные данные, доступ к которым неограниченного круга лиц предоставлен с согласия физического лица
	3. сведения о заработной плате физического лица
	4. сведения: паспортные данные, ИНН, адрес местожительства
12. ***Обезличивание персональных данных – это…***
	1. временное прекращение обработки персональных данных
	2. работа с персональными данными только определенного круга лиц
	3. действия, в результате которых невозможно определить принадлежность персональных данных конкретному физическому лицу
	4. действия, в результате которых невозможно восстановить содержимое персональных данных
13. ***Оператор персональных данных – это…***
	1. любое физическое лицо
	2. организация, осуществляющая обработку персональных данных, определяющая цели и содержание обработки
	3. организация, которая осуществляет передачу персональных данных через Государственную границу РФ
14. ***Установление подлинности объекта***
	1. аутентификация
	2. кодирование
	3. распознавание
	4. регистрация
15. ***Присвоение какому-либо субъекту или объекту уникального имени***
	1. идентификация
	2. аутентификация
	3. кодирование
	4. распознавание
16. ***Система защиты информации***
	1. совокупность организационных и технологических мер, технических средств, правовых норм, направленных на противодействие угрозам нарушителей
	2. осуществление мероприятий с целью системного обеспечения передаваемой, хранимой и обрабатываемой информации
	3. совокупность мер, направленных на обеспечение физической целостности информации
17. ***Средства защиты, предназначенные создать некоторую физически замкнутую среду вокруг объекта***
	1. технические
	2. методологические
	3. организационно-административные
	4. программные
18. ***Существуют средства защиты информации (отметить неверный ответ)***
	1. организационно-административные
	2. программные
	3. технические
	4. технологические
	5. модифицирующие
19. ***Несуществующие средства защиты***
	1. технологенные
	2. правовые
	3. технические
	4. технологические
20. ***Совокупность данных, которая может содержать подлежащие защите сведения***
	1. элементы защиты
	2. объект защиты
	3. субъект защиты
	4. терминал пользователя
21. ***Процессы, относящиеся к злоумышленным нарушениям надежности информации***
	1. несанкционированный просмотр данных
	2. помехи в каналах и линиях связи внешней среды
	3. технический сбой
22. ***Организационно-административные средства защиты***
	1. разграничение доступа к информации в соответствии с функциональными обязанностями должностных лиц
	2. использование автономных средств защиты аппаратуры
	3. регистрация пользователей компьютерных средств в журналах
	4. отключение пользователя от Интернета
23. ***Установление системы паролей относится к методу***
	1. аутентификации
	2. идентификации
	3. ратификации
24. ***Процессы по нарушению надежности информации классифицируют на***
	1. случайные и злоумышленные
	2. авторские и безымянные
	3. самостоятельные и несамостоятельные
	4. файловые и системные
25. ***Меры, ограничивающие несанкционированный доступ (отметить неверный ответ)***
	1. не хранить пароли в вычислительной системе в незашифрованном виде
	2. чаще менять пароль
	3. использовать максимально короткие пароли
26. ***Заражение компьютерными вирусами может произойти в процессе…***
	1. работы с файлами
	2. форматирования дискеты
	3. выключения компьютера
	4. печати на принтере
27. ***Программа, не являющаяся антивирусной***
	1. AVP
	2. Defrag
	3. Nod32
	4. Dr Web
28. ***Вирус может появиться в компьютере следующим образом…***
	1. переместиться с флешки
	2. при решении математической задачи
	3. при подключении к компьютеру модема
	4. самопроизвольно
29. ***Файловые вирусы поражают…***
	1. аппаратную часть компьютера
	2. системные области компьютера
	3. программы и документы на внешних носителях памяти
	4. оперативную память
30. ***Компьютерным вирусом является...***
	1. программа проверки и лечения дисков
	2. любая программа, созданная на языках низкого уровня
	3. программа, скопированная с плохо отформатированной дискеты
	4. специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью " размножаться "
31. ***Заражение «почтовым» вирусом происходит…***
	1. при открытии зараженного файла, присланного с письмом по E-mail
	2. при подключении к почтовому серверу
	3. при подключении к Web-серверу, зараженному «почтовым» вирусом
	4. при получении с письмом, присланном по E-mail, зараженного файла
32. ***Определяющим параметром эффективности работы антивирусной программы является …***
	1. стабильность и надежность работы
	2. принцип работы программы
	3. фирма-производитель
	4. емкость, занимаемая на диске антивирусной программой
33. ***Антивирусной называется специальная программа …***
	1. для создания и распространения компьютерных вирусов
	2. редактирующая код компьютерных вирусов
	3. для создания новых программ
	4. для обнаружения, уничтожения и защиты от компьютерных вирусов
34. ***Сетевые вирусы распространяются …***
	1. при загрузке драйвера устройства
	2. по различным компьютерным сетям
	3. в загрузочных секторах
	4. через оперативную память
35. ***Под многоплатформенностью антивирусной программы понимается …***
	1. умение работать с файлами различных типов
	2. наличие версий программы под различные конфигурации компьютера
	3. наличие версий программы под различные операционные системы
	4. использование большого объема вирусной базы
36. ***Под объемом вирусной базы понимается …***
	1. количество обнаруживаемых программой вирусов
	2. количество существующих вирусов
	3. число неучтенных программой вирусов
	4. число проверяемых файлов
37. ***Файл, содержащий внедренный в него вирус, называется …***
	1. вирусным
	2. зараженным
	3. испорченным
	4. неправильным
38. ***В зависимости от принципа работы выделяют группы антивирусных программ …***
	1. сканеры, макросы, фаги
	2. сканеры, базы данных, ревизоры
	3. доктора (фаги), ревизоры (инспекторы), базы данных
	4. детекторы, доктора (фаги), ревизоры (инспекторы), фильтры (сторожа), вакцинаторы (иммунизаторы)
39. ***Антивирусные программы доктора (фаги) выполняют …***
	1. поиск зараженных файлов и их лечение
	2. поиск известных вирусов
	3. предотвращение заражения файлов
	4. распространение известных вирусов
40. ***Антивирусные программы фильтры выполняют …***
	1. поиск зараженных файлов и их лечение
	2. поиск известных вирусов
	3. оповещение пользователя обо всех попытках какой-либо программы записаться на диск
	4. распространение известных вирусов
41. ***Антивирусные программы детекторы выполняют …***
	1. поиск зараженных файлов и их лечение
	2. поиск известных вирусов
	3. оповещение пользователя обо всех попытках какой-либо программы записаться на диск
	4. распространение известных вирусов
42. ***Антивирусные программы, оказывающие действие на определенный тип вирусов, и работающие таким образом, что вирус уже считает программу зараженной, называются…***
	1. вакцинаторы (иммунизаторы)
	2. фильтры (сторожа)
	3. ревизоры (инспекторы)
	4. доктора (фаги)