

ТЕРМИНОЛОГИЧЕСКИЙ ТЕСТ

Источники:

ГОСТ Р 50922-2006

ГОСТ Р 51275-2006

Часть 1. Основные термины, понятия, определения

Выбрать ОДИН правильный ответ из предложенных вариантов

1	Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил разграничения доступа называется
A	Защита информации от несанкционированного воздействия
B	Защита информации от несанкционированного доступа
C	Защита информации от утечки
D	Защита информации от разведки

2	Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
A	Программно-техническая защита информации
B	Программно-аппаратная защита информации
C	Техническая защита информации
D	Организационно-техническая защита информации

З	Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.
А	Комплексная защита информации
В	Система защиты информации
С	Комплекс средств защиты информации
Д	Служба защиты информации

4	Несанкционированное воздействие на ресурсы автоматизированной информационной системы , осуществляемое с использованием вредоносных программ
A	Вирусная атака
B	Программное воздействие
C	Вирусное воздействие
D	Компьютерная атака

5	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
A	Защита информации
B	Информационная безопасность
C	Защита информации от разведки
D	Обеспечение безопасности информации

6	Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.
A	Комплексная защита информации
B	Политика безопасности
C	Документационное обеспечение защиты информации
D	Система защиты информации

7

Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

A

Комплексная защищённость информации

B

Сохранность информации

C

Информационная безопасность

D

Безопасность информации

8

Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

A

Комплексная защита информации

B

Защита информации от преднамеренного доступа

C

Защита информации от несанкционированного доступа

D

Защита информации от преднамеренного воздействия

9	Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.
A	Защита информации от разглашения
B	Обеспечение конфиденциальности информации
C	Защита информации от несанкционированного доступа
D	Защита информации от утечки

10

Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

A

Комплексная защита информации

B

Защита информации от непреднамеренного воздействия

C

Защита информации от ошибок и сбоев

D

Защита информации от случайных факторов

11

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

A Конфиденциальная информация

B Коммерческая тайна

C Защищаемая информация

D Приватная информация

12

Объект защиты информации

- А** Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- В** Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.
- С** Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.
- Д** Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

13

Носитель защищаемой информации

- A** Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- B** Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.
- C** Информация или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.
- D** Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

14

Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

A

Атака

B

Угроза информации

C

Уязвимость

D

Фактор, воздействующий на защищаемую информацию

15

Угроза безопасности информации

- | | |
|----------|---|
| A | Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации |
| B | Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возможного нарушения конфиденциальности, целостности и доступности информации |
| C | Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней |
| D | Защита информации от утечки |

16

Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

A

Нарушение защищенности информации

B

Атака на информацию

C

Несанкционированный доступ к информации

D

Несанкционированное воздействие на информацию

17

Свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

- | | |
|----------|-------------------------------|
| A | Дестабилизирующий фактор |
| B | Угроза |
| C | Уязвимость |
| D | Недекларированная возможность |

18

Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

- A** Модель нарушителя безопасности информации
- B** Модель безопасности информации
- C** Модель угроз безопасности информации
- D** Модель защиты информации

19

Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

A

Комплексная защита информации

B

Физическая защита информации

C

Организационная защита информации

D

Техническая защита информации

20

Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

A

Документационная защита информации

B

Организационно-правовая защита информации

C

Правовая защита информации

D

Физическая защита информации

21

Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

A

Защита информации от утечки

B

Обеспечение конфиденциальности информации

C

Защита информации от разведки

D

Защита информации от несанкционированного доступа

22

Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

- A** Объект информационной безопасности
- B** Защищаемый объект информатизации
- C** Защищаемая информационная система
- D** Объект защиты информации

23

Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

A Источник уязвимости

B Источник угрозы

C Субъект атаки

D Субъект нападения

24

Несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

- A** Преднамеренное силовое электромагнитное воздействие на информацию
- B** Побочное электромагнитное излучение
- C** Паразитная наводка
- D** Атака «отказ в обслуживании»

25

Исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

A

Мониторинг безопасности информации

B

Спецпроверка

C

Аудит информационной безопасности

D

Специсследование

26

Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

A

Мониторинг

B

Спецпроверка

C

Аудит

D

Специсследование

27

Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

A

Мониторинг безопасности информации

B

Сертификация процесса защиты информации

C

Аудит безопасности информации

D

Экспертиза безопасности объекта

28

Периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности.

A

Мониторинг безопасности информации

B

Анализ рисков информационной безопасности

C

Аудит безопасности информации

D

Экспертиза документов по защите информации

29

Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

- A** Мониторинг безопасности информации
- B** Аудит информационной безопасности
- C** Анализ рисков информационной безопасности
- D** Экспертиза документов по защите информации

30

Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

A

Аттестация по требованиям безопасности

B

Сертификация системы защиты информации

C

Аудит документационного обеспечения защиты информации

D

Экспертиза документа по защите информации

31

Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

A

Экспертиза

B

Сертификация

C

Аттестация

D

Лицензирование

32

Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

A

Сертификация

B

Оценка соответствия

C

Аттестация

D

Лицензирование

33

Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

A

Оценка соответствия

B

Сертификация

C

Аттестация

D

Лицензирование

34

Программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы

A

Компьютерный вирус

B

Вредоносная программа

C

Троянская программа

D

Программная закладка

35

Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти системы установлены, или помещений и объектов, предназначенных для конфиденциальных переговоров

A

Защищаемое помещение

B

Объект информатизации

C

Информационная система

D

Система обработки информации

36

Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

A

Защищаемое помещение

B

Объект информатизации

C

Информационная система

D

Система обработки информации

37

Совокупность технических средств и программного обеспечения , а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации

A

Защищаемое помещение

B

Объект информатизации

C

Информационная система

D

Система обработки информации

38

Функциональные возможности программного обеспечения, не описанные в документации

A

программная закладка

B

недекларированные возможности

C

программное воздействие

D

уязвимость программного обеспечения

39

Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с использованием программных или программно- аппаратных средств

A

компьютерная атака

B

хакерское вторжение

C

Сетевая атака

D

нападение

40

Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с использованием программных или программно- аппаратных средств посредством протоколов межсетевого взаимодействия

A

компьютерная атака

B

хакерское вторжение

C

Сетевая атака

D

нападение