**V5: Защита информации.**

I: 1.

Q: [*выбрать 3 ответа*]

S: Информационная безопасность, это состояние определенного объекта, в качестве которого может выступать

-: деятельность по предотвращению утечки информации

-: информация, данные

-: ресурсы автоматизированной системы

-: информационная система

I: 2.

Q:

S: Безопасность информации – состояние защищенности информации, при котором обеспечены её

-: доступность

-: целостность

-: засекреченность

-: конфиденциальность

I: 3.

Q: [*выбрать один правильный ответ*]

S: Свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц, называется…

-: защищенность

-: секретность

-: конфиденциальность

-: скрытность

I: 4.

Q:

S: Неизменность информации в процессе ее передачи или хранения

-: монолитность

-: целостность

-: постоянство

I: 5.

Q: [*выбрать один правильный ответ*]

S: Свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц

-: публичность

-: доступность

-: оперативность

-: открытость

I: 6.

Q: [*выберите 5 из 6 параметров*]

S: Безопасность автоматизированной информационной системы – состояние защищенности автоматизированной системы, при котором обеспечиваются …, …, …, …, … её ресурсов.

-: конфиденциальность

-: доступность

-: целостность

-: неизменность

-: подотчетность

-: подлинность

I: 7.

Q:

S: Обеспечение идентификации субъекта доступа и регистрации его действий называется

-: подотчётность

-: п\*дотчетность

I: 8.

Q:

S: Свойство соответствия предусмотренному поведению или результату называется

-:

I: 9.

Q:

S: Свойство, гарантирующее, что субъект или ресурс идентичны заявленным

-: аутентичность

-: подлинность

I: 10.

Q:

S: Способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты

-: неотказуемость

-: апеллируемость

I: 1.

Q:

S: В Российской Федерации к нормативно-правовым актам министерств и ведомств области информационной безопасности относятся

-: постановления

-: приказы

-: указы

-: инструкции

-: инструктивные письма

-: решения

I: 2.

Q:

S: К нормативно-методическим документам в сфере информационной безопасности относятся

-: Доктрина информационной безопасности РФ

-: Указы президента РФ

-: Руководящие документы ФСТЭК (Гостехкомиссии)

-: Приказы ФСБ

-: Постановления правительства РФ

-: Методические указания

I: 3.

Q:

S: Следующие госорганы РФ не контролируют деятельность в области защиты информации

-: ФСТЭК

-: Рособрнадзор

-: Роскомнадзор

-: Ростехнадзор

I: 4.

Q:

S: Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности

I: 5.

Q:

S: Этапы развития средств информационных коммуникаций

1: появление технических средств электро- и радиосвязи

2: появление радиолокационных и гидроакустических средств

3: создание электронных вычислительных машин

4: появление локальных информационно-коммуникационных сетей

5: использование сверхмобильных коммуникационных устройств с широким спектром задач

6: создание глобальных информационно-коммуникационных сетей

I: 6.

S: Категории обрабатываемых в информационной системе персональных данных (ПДн)

L1: ПДн, касающиеся расовой, национальной принадлежности, политических и религиозных взглядов, состояния здоровья и интимной жизни

R1: категория 1

L2: ПДн, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию

R2: категория 2

L3: ПДн, позволяющие идентифицировать субъекта

R3: категория 3

L4: обезличенные и общедоступные ПДн

R4: категория 4

R5: категория 0

R6: категория 5

I: 7.

S: Обязательность сертификации и оценки соответствия информационной системы ПДн требованиям безопасности информации

L1: обязательная сертификация

R1: ИС ПДн 1 и 2 класса

L2: декларирование соответствия требованиям безопасности информации

R2: ИС ПДн 3 класса

L3: оценка соответствия только по решению оператора ПДн

R3: ИС ПДн 4 класса

R4: ИС ПДн 1 класса

R5: ИС ПДн 2 класса

I: 8.

Q:

S: Федеральная служба по техническому и экспортному контролю создана на безе

-: ФАПСИ

-: ФСТЭК

-: Гостехкомисси\*

-: Росинформтехнологи\*

I: 9.

Q:

S: Международные соглашения, не относящиеся к области защиты интеллектуальной собственности

-: Парижская конвенция

-: Болонская конвенция

-: Бернская конвенция

-: Женевская конвенция

-: Венская конвенция

-: Гаагская конвенция

I: 10.

Q:

S: Статьи УК РФ, относящиеся к области защиты информации

-: ст. 102

-: ст. 138

-: ст. 165

-: ст. 183

-: ст. 218

I: 11.

Q:

S: Статьи УК РФ, относящиеся к области борьбы с киберпреступностью

-: ст. 271

-: ст. 272

-: ст. 273

-: ст. 274

-: ст. 275

-: ст. 276

I: 1.

Q:

S: Средства защиты от несанкционированного доступа

-: средства авторизации

-: мандатное управление доступом

-: избирательное управление доступом

-: управление доступом на основе ролей

-: шифрование

-: аудит

I: 2.

Q:

S: Типичными CASE инструментами являются инструменты ### конфигурацией

I: 3.

Q:

S: Типичными CASE инструментами являются инструменты ### данных

I: 4.

Q:

S: Типичными CASE инструментами являются инструменты ### и ###

-: анализа

-: проектирования

I: 5.

Q:

S: Типичными CASE инструментами являются инструменты ### моделей

I: 6.

Q:

S: Типичными CASE инструментами являются инструменты ### и ### кода

-: рефакторинга

-: генераторы

I: 7.

Q:

S: Типичными CASE инструментами являются инструменты для построения ### диаграмм

I: 8.

Q:

S: К программно-техническим средствам защиты информации относятся

-: системы мониторинга сетей

-: программы политики защиты информации

-: антивирусные средства

- криптографические средства

-: анализаторы протоколов

I: 9.

Q:

S: К техническим средствам защиты информации относятся

-: системы резервного копирования

-: системы бесперебойного питания

-: системы аутентификации

-: эвристический анализатор

-: средства предотвращения взлома корпусов и краж оборудования

-: инструментальные средства анализа систем защиты

I: 10.

Q:

S: ПЭМИ - ### электромагнитное излучение, возникающее при работе технических средств обработки информации

I: 11

Q:

S: Для предотвращение утечки ПЭМИ используют ### подавление опасных сигналов: отключение источников сигналов, применение буферных устройств, фильтрация сигналов, ограничение сигналов.

I: 12

Q:

S: Для предотвращение утечки ПЭМИ используют ### подавление опасных сигналов: пространственное зашумление, линейное зашумление

I: 13.

Q:

S: ### и ### обеспечения безопасности информации 

-методы

-: средства

I: 1.

Q:

S: Виды воздействия на информацию

-: блокирование

-: нарушение целостности

-: нарушение конфиденциальности

-: копирование

-: уничтожение

-: модификация

-: искажение

I: 2.

Q:

S: Потенциально возможное событие, действие, процесс или явление, которое может привести к причинению ущерба чьим-либо интересам

I: 3.

Q:

S: ### угрозы, вызванные воздействием на АС объективных физических процессов, стихийных природных явлений, не зависящих от человека

I: 4.

Q:

S: Угрозы информационной безопасности, относящиеся к естественным, делятся на

-: природные

-: технические

-: антропогенные

-: военные

I: 5.

Q:

S: Каналы проникновения в информационную систему по типу основного средства для реализации угрозы

-: человек

-: люди

-: аппаратура

-: программ\*

I: 6.

Q:

S: Каналы проникновения в информационную систему по способу получения информации

-: физический

-: информационный

-: итерационный

-: трансграничный

-: электромагнитный

I: 7.

Q:

S: Технические меры противодействия угрозам информационной безопасности

-: средства аутентификации

-: аппаратное шифрование

I: 8.

Q:

S: На рисунке показана



I: 9.

Q:

S: Модель ### защиты информации 

I: 10.

Q:

S: Модель ### защиты информации 

I: 11.

Q:

S: Модель ### защиты информации

I: 12.

Q:

S: Принцип(ы) защиты информации, не относящийся(еся) к обеспечению рационального уровня защиты

-: соответствие уровня защиты ценности информации

-: гибкость защиты

-: многозональность защиты

-: максимальная стойкость защиты

-: многорубежность защиты

I: 13.

Q:

S: Классификация ### признаков объекта 

I: 14.

Q:

S: С точки зрения защиты, основными ### и ### информации являются следующие: люди, документы, продукция, измерительные датчики, интеллектуальные средства обработки информации, черновики и отходы производства, материалы и технологическое оборудование.

-: источник\*

-: носител\*

I: 1.

S: Сопоставьте названия антивирусных программ и изображений

L1: 

R1L2: 

L3: 

L4: 

L5: 

I: 2.

Q:

S: RAID-массив это

-: набор жестких дисков, подключенных особым образом

-: антивирусная программа

-: вид хакерской утилиты

-: база защищенных данных

-: брандмауэр

I: 3.

Q: [*выберите несколько правильных ответов*]

S: Отметьте составные части современной антивирусной программы

-: модем

-: принтер

-: сканер

-: межсетевой экран

-: стриммер

I: 4.

Q: [*выберите несколько правильных ответов*]

S: Вредоносные программы - это

-: шпионские программы

-: программы, наносящие вред данным и программам, находящимся на компьютере

-: антивирусные программы

-: программы, наносящие вред пользователю, работающему на зараженном компьютере

- троянские утилиты и сетевые черви

I: 5.

Q: [*выберите несколько правильных ответов*]

S: К вредоносным программам относятся

-: потенциально опасные программы

-: вирусы, черви, трояны

-: шпионские и рекламные программы

-: вирусы, программы-шутки, антивирусное программное обеспечение

-: межсетевой экран, брандмауэр

I: 6.

Q: [*выберите один из 5 вариантов ответа*]

S: Сетевые черви это

-: вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

-: вирусы, которые проникнув на компьютер, блокируют работу сети

-: вирусы, которые внедряются в документы под видом макросов

-: хакерские утилиты управляющие удаленным доступом компьютера

-: вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

I: 7.

Q: [*выберите один из 5 вариантов ответа*]

S: Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы

-: загрузочный вирус

-: макровирус

-: троян

-: сетевой червь

-: файловый вирус

I: 8.

Q:

S: Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию

-: троян

-: троян\*

-: троянская программа

I: 9.

Q: [*Выберите один из 5 вариантов ответа*]

S: Руткит - это

-: вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю

-: разновидность межсетевого экрана

-: программа использующая для распространения Рунет

-: вредоносная программа, маскирующаяся под макрокоманду

-: программа для скрытого взятия под контроль взломанной системы

I: 10.

Q: [*выберите несколько правильных ответов*]

S: Компьютерные вирусы это

-: вредоносные программы, наносящие вред данным.

-: программы, уничтожающие данные на жестком диске

-: программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

-: программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

-: это скрипты, помещенные на зараженных интернет-страничках

I: 11.

Q: [*Выберите один из 5 вариантов ответа*]

S: Вирус внедряется в исполняемые файлы и при их запуске активируется

-: загрузочный вирус

-: макровирус

-: файловый вирус

-: сетевой червь

-: троян

I: 12.

Q: [*Выберите один из 5 вариантов ответа*]

S: Вирус поражающий документы называется

-: троян

-: файловый вирус

-: макровирус

-: загрузочный вирус

-: сетевой червь

I: 1.

Q:

S: Основными путями проникновения вирусов в компьютер являются

-: больной пользователь

-: заархивированные файлы

-: компьютерные сети

-: файлы, созданные в Word и Excel

-: флеш-диски

I: 2.

Q:

S: Места и каналы возможного ### доступа к информации в компьютерной сети 

I: 3.

Q:

S: Нарушение конфиденциальности данных, циркулирующих в сети, просмотр и/или запись данных, передаваемых по линиям связи является ### угрозой сетевой безопасности

I: 4.

Q:

S: Нарушение целостности или доступности ресурсов (компонентов) сети, несанкционированное использование устройств, имеющих доступ к сети для изменения отдельных сообщений или потока сообщений является ### угрозой сетевой безопасности

I: 5.

Q: Установить соответствие значков фаерволов (межсетевых экранов)

L1: 

L2: 

L3: 

L4: 

I: 6.

Q:

S: Функции брандмауэра (межсетевого экрана)

-: фильтрация доступа к заведомо незащищенным службам

-: препятствование получению закрытой информации из защищенной подсети

-: контроль доступа к узлам сети

-: защищает узлы сети от проникновения через "люки" (back doors) или уязвимости ПО

-: обеспечивает защиту от многих внутренних угроз, в первую очередь - утечки данных

-: защищает от загрузки пользователями вредоносных программ, в том числе вирусов

I: 7.

S: Расположить алгоритмы шифрования Wi-Fi в порядке возрастания крипто стойкости

1 WPA-PSK

2: : WPA-802.1x

3 WEP

4: WPA2:

I: 8.

Q:

S: Сниффер это

-: анализатор сетевого адреса

-: генератор кода

-: счетчик трафика

-: анализатор трафика

-: блокиратор попыток несанкционированного доступа

-: анализатор MAC-адреса

I: 9.

Q:

S: Расположите в порядке возрастания уровни модели OSI

1: физический

2: канальный

3: сетевой

4: транспортный

5: сеансовый

6: представления

7: прикладной

I: 10.

Q:

S: Расположите в порядке возрастания уровни стека TCP/IP

1: доступа к среде

2: сетевой

3: транспортный

4: прикладной