_____ — цель прогресса внедрения и тестирования средств защиты.
Гарантировать правильностьреализации средств защиты
Определить уровень расходов на систему защиты
Выбор мер и средств защиты
Выявить нарушителя
1
_____ — это недостаток систем шифрования с открытым ключом.
Относительно низкая производительность
На одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста
При использовании простой замены легко произвести подмену одного шифрованного текста другим
Необходимость распространения секретных ключей
1
_____ — это политика информационной безопасности.
Стандарт безопасности
Профиль защиты
Итоговый документ анализа рисков
Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации
4
_____ — это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы.
Авторизация
Идентификация
Аудит
Аутентификация
1
. — это присвоение субъектам и объектам доступа уникального номера,шифра, кода и т.п. с целью получения доступа к информации.
Идентификация
Авторизация
Аутентификация
Аудит
1
— это проверка подлинности пользователя по предъявленному им идентификатору.
Аутентификация
Идентификация
Авторизация
Аудит
1
— это проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.
Аутентификация
Идентификация
Авторизация
Аудит
1
. _____ — это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.
Безопасность информации
Надежность информации
Уязвимость информации

Защищенность информации
1
. _____ занимается обеспечением скрытности информации в информационных массивах.
Стеганография
Криптография
Криптология
Аутентификация
1
. _____ называется запись определенных событий в журнал безопасности сервера.
Аудитом
Учетом
Мониторингом
Трафиком
1
_____ называется конечное множество используемых для кодирования информации знаков.
алфавитом
знаком
алгоритмом
символом
1
. _____ называется конфигурация из нескольких компьютеров, выполняющих общее приложение.
Кластером
Суперсервером
Сетью
Сервером
1
. _____ называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий.
Профилем защиты
Стандартом безопасности
Профилем безопасности
Системой защиты
1
_____ называется оконечное устройство канала связи, через которое процесс может передавать или получать данные.
Сокетом
Портом
Хостом
Терминалом
1
. _____ называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля.
Мониторингом
Администрированием
Управлением ресурсами
Аудитом
1
. называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
Электронной подписью
Идентификатором
Ключом

Шифром
1
. _____ называется процесс имитации хакером дружественного адреса.
"Спуфингом"
Проникновением
Взломом
"Крэком"
1
. называется процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска.
Управлением риском
Минимизацией риска
Мониторингом средств защиты
Оптимизацией средств защиты
1
. _____ называется система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.
Брандмауэром
Фильтром
Браузером
Маршрутизатором
1
. _____ называется совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением.
Качеством информации
Актуальностью информации
Целостностью
Доступностью
1
. _____ называется список объектов, к которым может быть получен доступ, вместе с доменом защиты объекта.
Перечнем возможностей
Доменом
Списком управления доступом
Списком владельцев
1
. _____ называется удачная криптоатака.
Взломом
Раскрытием шифра
Проникновением
Вскрытием
1
. _____ называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС.
Программными закладками
Компьютерными червями
Внутрипрограммными вирусами
Вирусами
. _____ обеспечивается защита исполняемых файлов.
Обязательным контролем попытки запуска

Специальным режимом запуска
Дополнительным хостом
Криптографией
1
_____ обеспечивается защита от форматирования жесткого диска со стороны пользователей.
Специальным программным обеспечением
Системным программным обеспечением
Аппаратным модулем, устанавливаемым на контроллер
Аппаратным модулем, устанавливаемым на системную шину ПК
4
. _____ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.
Криптоанализ
Стеганография
Криптография
Криптология
1
. _____ определяется как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных.
Контроль доступа
Аутентификация
Целостность
Причастность
4
. ._____создается для реализации технологии RAID.
Псевдодрайвер
Компилятор
Интерпретатор
Специальный процесс
1
_____ составляет основу политики безопасности
Способ управления доступом
Программное обеспечение
Управление риском
Выбор каналов связи
1
. _____ уровень ОС связан с доступом к информационным ресурсам внутри организации.
Сетевой
Внешний
Приложений
Системный
1
_____ характеризует соответствие средств безопасности решаемым задачам.
Эффективность
Корректность
Унификация
Адекватность
1
_____ является администратором базы данных.

Любой пользователь, создавший БД
Администратор сервера баз данных
Старший пользователь группы
Системный администратор
1
. _____ является достоинством дискретных моделей политики безопасности.
Простой механизм реализации
Числовая вероятностная оценка надежности
Динамичность
Высокая степень надежности
1
_____ является достоинством матричных моделей безопасности.
Легкость представления широкого спектра правил обеспечения безопасности
Контроль за потоками информации
Гибкость управления
Расширенный аудит
1
_____ является достоинством модели конечных состояний политики безопасности.
Высокая степень надежности
Дешевизна
Простота реализации
Удобство эксплуатации
1
. _____ является достоинством модели политики безопасности на основе анализа угроз системе.
Числовая вероятностная оценка надежности
Динамичность
Простой механизм реализации
Высокая степень надежности
1
. _____ является задачей анализа модели политики безопасности на основе анализа угроз системе.
Максимизация ресурса для взлома
Максимизация затрат для взлома
Максимизация времени взлома
Минимизация вероятности преодоления системы защиты
4
. _____ является наиболее надежным механизмом для защиты содержания сообщений.
Криптография
Дополнительный хост
Специальный режим передачи сообщения
Специальный аппаратный модуль
1
. _____ является наукой, изучающей математические методы защиты информации путем ее преобразования.
Криптология
Криптоанализ
Стеганография
Криптография

1
. является недостатком многоуровневых моделей безопасности.
Невозможность учета индивидуальных особенностей субъекта
Сложность представления широкого спектра правил обеспечения безопасности
Отсутствие полного аудита
Отсутствие контроля за потоками информации
1
. является недостатком модели конечных состояний политики безопасности.
Сложность реализации
Изменение линий связи
Низкая степень надежности
Статичность
1
. _____ является первым этапом разработки системы защиты ИС.
Анализ потенциально возможных угроз информации
Изучение информационных потоков
Стандартизация программного обеспечения
Оценка возможных потерь
1
. _____ является сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях.
Kerberos
Network DDE
SendMail
Net Logon
1
. _____ является содержанием параметра угрозы безопасности информации "конфиденциальность".
Несанкционированное получение
Несанкционированная модификация
Уничтожение
Искажение
1
. _____ являются достоинствами аппаратной реализации криптографического закрытия данных.
Высокая производительность и простота
Целостность и безопасность
Практичность и гибкость
Доступность и конфиденциальность
1
. _____ являются достоинствами программной реализации криптографического закрытия данных.
Практичность и гибкость
Безопасность и эффективность
Корректность и функциональность
Высокая производительность и простота
1
. "Троянский конь" является разновидностью модели воздействия программных закладок
искажение
перехват
наблюдение и компрометация

уборка мусора
1
. "Уполномоченные серверы" были созданы для решения проблемы
имитации IP-адресов
подделки электронной подписи
перехвата трафика
НСД
1
"Уполномоченные серверы" фильтруют пакеты на уровне
приложений
физическом
канальном
транспортном
1
Администратор _____ занимается регистрацией пользователей СУБД.
сервера баз данных
системный
сетевой
базы данных
1
Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем.
физическом
канальном
сетевом
транспортном
1
Брандмауэры второго поколения представляли собой ...
"уполномоченные серверы"
маршрутизаторы с фильтрацией пакетов
"неприступные серверы"
хосты с фильтрацией пакетов
1
Брандмауэры первого поколения представляли собой ...
маршрутизаторы с фильтрацией пакетов
"неприступные серверы"
"уполномоченные серверы"
хосты с фильтрацией пакетов
1
В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:
быть равен
быть меньше
доминировать
специально оговариваться
1
В многоуровневой модели, если уровни безопасности субъекта и объекта доступа не сравнимы, то...
выполняются запросы минимального уровня безопасности
все запросы выполняются

доступ специально оговаривается
никакие запросы на выполняются
4
В СУБД Oracle под ролью понимается:
набор привилегий
группа субъектов
группа объектов
совокупность процессов
1
Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
доступность
целостность
конфеденциалность
детерминированность
1
Восстановление данных является дополнительной функцией услуги защиты
целостность
доступность
конфеденциалность
детерминированность
1
Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство
доступность
детерминированность
целостность
восстанавливаемость
1
Два ключа используются в криптосистемах
с открытым ключом
с закрытым ключом
симметричных
двойного шифрования
1
Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели
искажение
Несанкционированное получение
Несанкционированная модификация
Уничтожение
1
Длина исходного ключа в ГОСТ 28147-89 (бит):
256
64
128
56
1
Длина исходного ключа у алгоритма шифрования DES (бит):
56

256
64
128
1
Для создания базы данных пользователь должен получить привилегию от:
администратора сервера баз данных
сетевого администратора
системного администратора
старшего пользователя своей группы
1
Единственный ключ используется в криптосистемах
симметричных
асимметричных
с закрытым ключом
с открытым ключом
1
Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:
базовой
средней
низкой
стандартной
1
Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты
встроенных в ОС
уровня приложений
сетевого уровня
системного уровня
1
Из перечисленного аутентификация используется на уровнях:1. Прикладном 2. сетевом 3. Транспортном 4.канальном 5. Физическом
1,2,3
2,3,4
3,4,5
1,3,5
1
Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:1. Аутентификация 2. контроль доступа 3. причастность 4. целостность 5. контроль трафика
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4
1
Из перечисленного в автоматизированных системах используется аутентификация по:1. паролю 2. предмету 3. физиологическим признакам 4.периферийным устройствам 5. терминалу
1,2,3
1,3,4
2,3,5
3,4,5

1
Из перечисленного в обязанности сотрудников группы информационной безопасности входят: 1.расследование причин нарушения защиты 2. управление доступом пользователей к данны 3. устранение дефектов аппаратной части 4. исправление ошибок в программном обеспечении
1,2
2,3
3,4
1,4
1
Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля:1. дата и время события 2. идентификатор пользователя 3. результат действия 4. тип события
1,2,3
2,3,4
1,3,4
1,2,3,4
4
Из перечисленного в ОС UNIX существуют администраторы: 1. аудита 2. печати 3. системных утилит 4. службы аутентификации
1,2,3
2,3,4
1,3,4
1,2,3,4
4
Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на:1. базы данных 2. процедуры 3. сервер баз данных 4. события
1,2,3
2,3,4
1,3,4
1,2,3,4
4
Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для: 1. владельца 2. всех основных пользователей 3. членов группы владельца 4. конкретных заданных пользователей 5. конкретных заданных групп пользователей
1,2,3
2,3,4
3,4,5
1,3,4
1
Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:1. визуальное сканирование 2. исследование динамических 3. характеристик движения руки 4. непосредственное сравнение изображений 5. сравнение характерных деталей в цифровом виде
1,2,3
2,3,4
3,4,5
1,3,4
1
Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:1. непосредственное сравнение изображений 2. сравнение характерных деталей в цифровом виде 3. визуальное сканирование 4. исследование динамических
1,2
2,3

3,4
1,4
1
Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются:1. голос 2. личная подпись 3. отпечатки пальцев 4. форма кисти
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4
1
Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:1.выполнение 2. запись 3. чтение
1,2,3
1,2
2,3
1,3
1
Из перечисленного для СУБД важны такие аспекты информационной безопасности, как: 1. Доступность 2. Конфиденциальность 3. Целостность 4.многоплатформенность 5.своевременность
1,2,3
2,3,4
3,4,5
1,3,4
1
Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:1. Изменение 2. чтение 3.выполнение
1
2
3
1,2
4
Из перечисленного контроль доступа используется на уровнях:1. Прикладном 2. сетевом 3 транспортном
1,2,3
1,2
2,3
1,3
1
Из перечисленного метка безопасности состоит из таких компонентов, как: 1. категория 2. области 3 уровень секретности
1,2,3
1,2
2,3
1,3
1
Из перечисленного методами защиты потока сообщений являются:1 использование случайных чисел 2. нумерация сообщений 3 отметка времени
1,2,3
1,2
2,3

1,3
1
Из перечисленного на сетевом уровне рекомендуется применение услуг:1. аутентификации 2 контроля доступа 3 конфиденциальности 4 целостности 5 уровень секретности
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4
1
Из перечисленного на транспортном уровне рекомендуется применение услуг: 1. аутентификации 2. контроля доступа 3. конфиденциальности 4 целостности 5 уровень секретности
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4
1
Из перечисленного объектами для монитора обращений являются:1. задания 2. программы 3.устройства 4. Файлы
1,2,3,4
2,3,4
1,3,4
1,2,4
1
Из перечисленного подсистема управления криптографическими ключами структурно состоит из:1. программно-аппаратных средств 2. центра распределения ключей 3.подсистемы защиты ключей 4подсистемы генерации ключей
1,2,3
1,2
2,3
1,4
2
Из перечисленного пользователи СУБД разбиваются на категории:1. администратор базы данных 2. администратор сервера баз данных 3 конечные пользователи 4.групповые пользователи 5.системный администратор
1,2,3
2,3,4
3,4,5
1,3,5
1
Из перечисленного привилегии в СУБД могут передаваться:1. группам 2. ролям 3. субъектам 4.процессам 5.объектам
1,2,3
2,3,4
3,4,5
1,3,5
1
Из перечисленного привилегии СУБД подразделяются на категории: 1. безопасности 2 доступа 3.чтения 4.тиражирования
1,2,3
1,2

2,3
1,4
2
Из перечисленного привилегиями безопасности являются: 1. created 2. operator 3. security; 4.operator 5. trace
1,2,3,4,5
2,3,4
1,3,4,5
1,4,5
1
Из перечисленного система брандмауэра может быть: 1. ПК 2. маршрутизатором 3. хостом
1
2
1,2
1,2,3
4
Из перечисленного система защиты электронной почты должна: 1. быть кросс-платформенной 2. обеспечивать все услуги безопасности 3. поддерживать работу с почтовыми клиентами 4.поддерживать работу только с лицензионным ПО 7.обеспечивать аудит
1,2,3,4
1,2,3
1,2
2,3
2
Из перечисленного составляющими информационной базы для монитора обращений являются: 1. вид 2.доступа 3. форма допуска 4.файлы 5.порты
1
2
1,2
1,2,3
4
Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни:1. внешний 2. приложений 3. сетевой 4. системный 5.серверный
1,3
2,3
1,2,4
1,2,3,4
4
Из перечисленного субъектами для монитора обращений являются:1. порты 2. программы 3 терминалы
1,2,3
2,3
1,2
2
1
Из перечисленного типами услуг аутентификации являются: 1. достоверность объектов коммуникации 2. достоверность происхождения данных 3. асинхронном 4. синхронном
1,3
3,4
1,2
2,4
3

Из перечисленного тиражирование данных происходит в режимах: 1. асинхронном 2. синхронном 3.Канальном 4.физическом
1,3
3,4
1,2
2,4
3
Из перечисленного управление маршрутизацией используется на уровнях: 1. прикладном 2. сетевом 3. Транспортном 4. Канальном 5. Физическом
5,3
3,5
1,2
3,4
3
Из перечисленного услуга защиты целостности доступна на уровнях: 1. прикладном 2. сетевом 3 транспортном 4.сеансовом 5.физическом
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного услуга обеспечения доступности реализируется на уровнях: 1. прикладном 2. сетевом 3. Физическом 4.канальном
5,3
1,3,5
1,2
2,3,4
3
Из перечисленного формами причастности являются: 1. к посылке сообщения 2. подтверждение получения сообщения 3.санкционированный канал связи 4.лицензионное программное обеспечение
1,3
3,4
1,2
2,4
3
Из перечисленного функция подтверждения подлинности сообщения использует следующие факты:1. доставка по адресу 2. неизменность сообщения при передаче 3. санкционированный отправитель 4. санкционированный канал связи 5.лицензионное программное обеспечение
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного цифровая подпись используется для обеспечения услуг: 1. аутентификации 2. целостности 3.расширенного содержания письма 4.электронного ключа
5,3
1,3,5
1,2
2,3,4
3
Из перечисленного электронная почта состоит из:1. краткого содержания письма

2.прикрепленных файлов 3. тела письма 4. расширенного содержания письма 5. электронного ключа
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного ядро безопасности ОС выделяет типы полномочий:1. подсистем 2. ядра 3. периферийных устройств 4.пользователей
1,3
3,4
1,2
2,4
3
Из перечисленного, аспектами адекватности средств защиты являются: .1. корректность 2. эффективность 3.унификация 4.конфиденциальность
1,3
3,4
1,2
2,4
3
Из перечисленного, группами требований к документированию системы защиты информации являются: 1. обработка угроз 2. протоколирование 3. тестирование программ 4. Аутентификация 5.резервное копирование
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного, группами требований к системам защиты информации являются: 1. конкретные 2. общие 3. организационные 4.программные 5.технические
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного, параметрами классификации угроз безопасности информации являются:1. источники угроз 2. предпосылки появления 3. природа происхождения 4.степень прогнозируемости 5.размер ущерба
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного, подсистема регистрации и учета системы защиты информации должна обеспечивать: 1. оповещение о попытках нарушения защиты 2. учет носителей информации 3.управление потоками информации 4.аутентификация 5.идентификация
5,3
1,3
1,2
3,4
3

Из перечисленного, подсистема управления доступом системы защиты информации должна обеспечивать:1. аутентификация 2. идентификация 3. управление потоками информации 4.оповещение о попытках нарушения защиты 5.учет носителей информации
5,3
1,3,5
1,2,3
2,3,4
3
Из перечисленного, процесс анализа рисков при разработке системы защиты ИС включает:1. анализ потенциальных угроз 2. оценка возможных потерь 3.оценка возможных затрат 4.анализ потенциального злоумышленника
1,3
3,4
1,2
2,4
3
Из перечисленного, с точки зрения пользователя СУБД, основными средствами поддержания целостности данных являются: 1. ограничения 2. правила 3.Стандарты 4.нормативы
1,3
3,4
1,2
2,4
3
Из перечисленного, согласно "Оранжевой книге" требованиями в области аудита являются:1. идентификация и аутентификация 2. регистрация и учет 3.политика безопасности 4. непрерывность защиты
1,3
3,4
1,2
2,4
3
Из перечисленного, угрозы безопасности по предпосылкам появления классифицируются как:1. объективная 2. субъективная 3.стихийная 4.преднамеренная 5.случайная
5,3
3,5
1,2
2,3
3
Из перечисленного, угрозы безопасности по природе происхождения классифицируются как:1. Преднамеренная 2. случайная 3.субъективная 4.стихийная 5.объективная
5,3
3,5
1,2
2,3
3
Из перечисленных программных закладок, по методу внедрения в компьютерную систему различают: 1. драйверные 2. загрузочные 3. прикладные 4. программно-аппаратные 5.троянские
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4,5

1
Из перечисленных разделов, криптография включает: 1. криптосистемы с открытым ключом 2. симметричные криптосистемы 3. системы электронной подписи 4. управление ключами 5.асимметричные криптосистемы
1,2,3,4
2,3,4,5
1,3,4,5
1,2,4,5
1
Из перечисленных свойств, безопасная система обладает:1. доступность 2. конфиденциальность 3. целостность 4.точность
1,2,4
2,3,4
1,3,4
1,2,3
4
Как предотвращение неавторизованного использования ресурсов определена услуга защиты
контроль доступа
причастность
целостность
аутентификация
1
Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки
адресов отправителя и получателя
содержания сообщений
электронной подписи
структуры данных
1
Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты
за определенное время
фиксированным ресурсом
фиксированными затратами
ограниченной компетенцией злоумышленника
1
На ресурсов ОС. уровне ОС происходит определение допустимых для пользователя
системном
приложений
внешнем
сетевом
1
Наименее затратный криптоанализ для криптоалгоритма DES
перебор по всему ключевому пространству
разложение числа на простые множители
теорией помехоустойчивого кодирования
безошибочности шифрования
1
Наименее затратный криптоанализ для криптоалгоритма RSA
перебор по всему ключевому пространству
разложение числа на простые множители

теорией помехоустойчивого кодирования
безошибочности шифрования
2
Обеспечение взаимодействия удаленных процессов реализуется на _____у
транспортном
сеансовом
канальном
сетевом
1
Обеспечение целостности информации в условиях случайного воздействия изучается:
перебор по всему ключевому пространству
разложение числа на простые множители
теорией помехоустойчивого кодирования
безошибочности шифрования
3
Обычно в СУБД применяется управление доступом
произвольное
иерархическое
административное
декларируемое
1
Организационные требования к системе защиты
административные и процедурные
управленческие и идентификационные
аппаратурные и физические
административные и аппаратурные
1
Основной целью системы брандмауэра является управление доступом
к защищаемой сети
внутри защищаемой сети
к секретной информации
к архивам
1
Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему
хотя бы одного средства безопасности
Пароля
аудита
всех средств безопасности
1
По умолчанию пользователь не имеет никаких прав доступа к:
таблицам и представлениям
формам
таблицам и формам
представлениям и формам
1
198. По умолчанию право на подключение к общей базе данных предоставляется:
всем пользователям
создателям

определенным пользователям
доступным пользователям
1
Поддержка диалога между удаленными процессами реализуется на _____
уровне модели взаимодействия открытых систем.
сеансовом
сетевом
канальном
транспортном
1
Показатель _____ является главным параметром криптосистемы.
криптостойкости
безошибочности шифрования
скорости шифрования
надежности функционирования
1
Полномочия подсистем ядра безопасности ОС ассоциируются с:
пользователями
Процессами
Приложениями
периферийными устройствами
1
При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается:
тип разрешенного доступа
объект системы
субъект системы
факт доступа
1
При избирательной политике безопасности в матрице доступа объекту системы соответствует:
строка
столбец
ячейка
прямоугольная область
При избирательной политике безопасности в матрице доступа субъекту системы соответствует:
строка
столбец
ячейка
прямоугольная область
2
При качественном подходе риск измеряется в терминах
заданных с помощью шкалы или ранжирования
денежных потерь
заданных с помощью ранжирования
объема информации
1
При количественном подходе риск измеряется в терминах
денежных потерь
заданных с помощью ранжирования

объема информации
заданных с помощью шкалы
1
Применение услуги причастности рекомендуется на _____ уровне модели OSI.
прикладном
сеансовом
физическом
транспортном
1
Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа
имитатор
фильтр
заместитель
перехватчик
1
С использованием прикладных ресурсов ИС связан уровень ОС:
приложений
сетевой
внешний
системный
1
С помощью закрытого ключа информация:
расшифровывается
зашифровывается
транслируется
копируется
1
С помощью открытого ключа информация:
зашифровывается
транслируется
копируется
расшифровывается
1
С точки зрения ГТК основной задачей средств безопасности является обеспечение:
защиты от НСД
надежности функционирования
сохранности информации
простоты реализации
1
Система защиты должна гарантировать, что любое движение данных
идентифицируется, авторизуется, обнаруживается, документируется
контролируется, кодируется, фиксируется, шифруется
анализируется, идентифицируется, шифруется, учитывается
копируется, шифруется, проектируется, авторизуется
1
Стандарт DES основан на базовом классе
блочные шифры
замещения
перестановки

гаммирование
1
Требования к техническому обеспечению системы защиты
аппаратурные и физические
программные и физические
аппаратурные и программные
аппаратурные
1
У всех программных закладок имеется общая черта
обязательно выполняют операцию записи в память
перехватывают прерывания
постоянно находятся в оперативной памяти
обязательно выполняют операцию чтения из памяти
1
Услугами _____ ограничивается применение средств защиты физического уровня.
конфиденциальности
целостности
аутентификации
контроля доступа
1
Формирование пакетов данных реализуется на уровне модели взаимодействия открытых систем.
канальном
транспортном
сетевом
физическом
1
Являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры, клавиатурные шпионы типа
фильтры
имитаторы
заместители
перехватчики
1