1. Службы безопасности предназначенные для защиты от атак доступа
* конфиденциальность, идентифицируемость
* целостность, идентифицируемость
* доступность , целостность
* идентифицируемость, доступность
1. Какое свойство службы безопасности предназначаются для защиты от атак отказа в обслуживании?
* конфиденциальность
* целостность
* доступность
* идентифицируемость
1. Для защиты от атак какого типа предназначена служба конфиденциальности?
* атаки доступа
* атаки модификации
* атаки отказа в обслуживании
* атаки отказа от обязательств
1. Для защиты от атак какого типа предназначена служба доступности?
* атаки доступа
* атаки модификации
* атаки отказа в обслуживании
* атаки отказа от обязательств
1. К механизмам конфиденциальности относятся:
* идентификация и аутентификация
* шифрование файлов
* правильное управление ключами при использовании шифрования
1. Обеспечивает секретность информации, открывает доступ к информации только аутентифицированным пользователям
* служба конфиденциальности
* служба целостности
* служба доступности
* служба идентифицируемости
1. Атака доступа направлена на:
* нарушение конфиденциальности информации
* уничтожение компьютера
* уничтожение информации
1. Поддерживает готовность информации к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям
* служба конфиденциальности
* служба целостности
* служба доступности
* служба идентифицируемости
* служба идентифицируемости
1. Для обеспечения конфиденциальности потока данных применяются методы:
* физической защиты
* скрытия информации
* аудита
1. Переключение по отказу:
* предотвращает полную потерю информации при случайном или преднамеренном уничтожении файлов
* обеспечивает восстановление информации и сохранение производительности
* защищает системы, информацию и производственные мощности от стихийных бедствий
1. Выделите верное утверждение в отношении информационной безопасности.
* наступление нового этапа развития ИТ приводит к быстрому повышению уровняинформационной безопасности
* наступление нового этапа развития ИТ приводит к быстрому падению уровня информационной безопасности
* уровень информационной безопасности не зависит от этапов развития ИТ
1. Какие меры должен в себя включать комплексный подход к обеспечению информационной безопасности?
* Законодательные, административные, процедурные, научно-технические
* Социальные, Законодательные, административные, процедурные, моральные
* Административные, процедурные, научно-технические, моральные
* Процедурные, Социальные, Законодательные, административные
* научно-технические, Социальные, Законодательные, административные, процедурные
1. К какому уровню обеспечения ИБ относятся действия общего и специального характера, предпринимаемые руководством организации?
* законодательный
* административный
* процедурный
* научно-технический
1. К какому уровню обеспечения ИБ относятся конкретные методики, программно-аппаратные, технологические и технические меры?
* законодательный
* административный
* процедурный
* научно-технический
1. В организации проводятся проверки «чистый стол», целью которых является выявление нарушений требований по хранению ключевых носителей и конфиденциальных документов. К какому уровню обеспечения ИБ они относятся?
* аконодательный
* административный
* процедурный
* научно-технический
1. Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?
* стратегическая безопасность
* информационная безопасность
* экономическая безопасность
* корпоративная безопасность
1. Какой аспект информационной безопасности отражает то, что защищенная информация должна быть доступна только тому, кому она предназначена?
* целостность
* конфиденциальность
* доступность
1. Какой аспект информационной безопасности отражает актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения?
* целостность
* конфиденциальность
* доступность
1. Если злоумышленник подменил исходное сообщение, передаваемое по сети Интернет, какое свойство информации он нарушил?
* целостность
* конфиденциальность
* доступность
1. Какой аспект ИБ наиболее актуален для провайдера Интернет-услуг?
* целостность
* конфиденциальность
* доступность
1. Какой аспект ИБ наиболее актуален для фармацевтической компании, занимающейся разработкой новых лекарств?
* целостность
* конфиденциальность
* доступность
1. Какая из нижеперечисленных угроз представляет наибольшую опасность?
* вредоносные программы
* хакерские атаки
* действия инсайдеров
* финансовое мошенничество
1. Как называется практически бесполезная информация, рассылаемая абонентам электронной почты?
* DoS
* Virus
* Spam
* Worm
1. Что принято считать ресурсом или активом информационной системы?
* модель информационной системы
* все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет
* именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите
1. Какие из перечисленных вариантов решений в отношении рисков являются неуместными:
* принят, устранен
* принят, дезавуирован
* дезавуирован, отклонен
1. Какой из перечисленных классов функциональных требований включает требования кодирования информации?
* класс приватности (конфиденциальности)"
* класс защиты функций безопасности объекта
* класс криптографической поддержки (криптографической защиты)
1. Что представляет собой событие - триггер?
* событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска
* событие, увеличивающее время отклика web - сервера
* это одна из разновидностей атак на сервер
1. Что формируют потенциальные злоумышленные действия по отношению к объектам?
* вероятностный набор действий по подавлению угроз
* шаблоны мер потенциального противодействия
* набор угроз ИБ
1. Что из перечисленного предписывается выполнить при проектировании системы с полным перекрытием?
* выверить остаточную стоимость активов
* детально прописать пути потенциального проникновения
* согласовать порядок применения альтернативных инструментов защиты
1. Может ли анализ угроз каким-то образом помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня?
* нет
* да
* спорно
1. Чем определяется высокая стойкость системы?
* уровнем стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения
* уровнем стойкости, при котором обеспечивается защита от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
* уровнем стойкости функции безопасности объекта оценки, на котором обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения
1. Что обеспечивает базовая стойкость?
* защиту от тщательно спланированного и организованного нарушения безопасности объекта оценки нарушителем с высоким потенциалом нападения
* защиту от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
* адекватную защиту от случайного нарушения безопасности объекта оценки нарушителем с низким потенциалом нападения
1. Что из перечисленного предписывается выполнить при проектировании системы с полным перекрытием?
* выверить остаточную стоимость активов
* детально прописать пути потенциального проникновения
* согласовать порядок применения альтернативных инструментов защиты
1. Что определяет ресурсы или активы ИС?
* модель ИС
* все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет
* именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите
1. Каковы цели анализа и тестирования прикладных систем в аспектах информационной безопасности?
* оперативное внесение изменений в операционные системы
* обеспечение целостности программного обеспечения
* обеспечение более эффективного использования готовых пакетов программ
1. Окно опасности перестает существовать, когда:
* администратор безопасности узнает об угрозе
* производитель ПО выпускает заплату
* заплата устанавливается в защищаемой ИС
1. Окно опасности появляется, когда:
* становится известно о средствах использования уязвимости
* появляется возможность использовать уязвимость
* устанавливается новое ПО
1. Окно опасности - это:
* промежуток времени
* часть пространства
* плохо закрепленная деталь строительной конструкции
1. Самыми опасными источниками внутренних угроз являются:
* некомпетентные руководители
* обиженные сотрудники
* любопытные администраторы
1. Самыми опасными источниками угроз являются:
* внутренние
* внешние
* пограничные
1. Самыми опасными угрозами являются:
* непреднамеренные ошибки штатных сотрудников
* вирусные инфекции
* атаки хакеров
1. Агрессивное потребление ресурсов является угрозой:
* доступности
* конфиденциальности
* целостности
1. Перехват данных является угрозой:
* доступности
* конфиденциальности
* целостности
1. Дублирование сообщений является угрозой:
* доступности
* конфиденциальности
* целостности
1. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
* отсутствие целостной концепции безопасности при проектировании базового программного обеспечения
* просчеты при реализации базового программного обеспечения
* недостаточное тестирование базового программного обеспечения
1. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
* использование недостаточно апробированных технологий
* архитектурные просчеты при построении информационных систем
* использование приложений, полученных из ненадежных источников
1. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
* просчеты при администрировании информационных систем
* необходимость постоянной модификации информационных систем
* сложность современных информационных систем
1. Выберите вредоносную программу, которая открыла новый этап в развитии данной области:
* Melissa
* Bubble Boy
* ILOVEYOU
1. Для внедрения бомб чаще всего используются ошибки типа:
* отсутствие проверок кодов возврата
* переполнение буфера
* нарушение целостности транзакций
1. Меры информационной безопасности направлены на защиту от:
* нанесения неприемлемого ущерба
* нанесения любого ущерба
* подглядывания в замочную скважину