Тест №2 «Средства защиты информации от НСД»

1) Ключевыми характеристиками РКБ являются следующие:

а. устройство с очень высоким уровнем защищенности, примитивное, встроенное в контролируемую систему и стартующее до старта основной ОС, независимое от контролируемой системы.

б. устройство с очень высоким уровнем защищенности.

в. встроенное в контролируемую систему и стартующее до старта основной ОС устройство.

г. примитивное, независимое от контролируемой системы устройство.

2) Что означает термин «доверенная загрузка»?

а. загрузка различных ОС только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

б. загрузка различных ОС после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

в. загрузка различных ОС только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности).

г. загрузка различных ОС только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения идентификации/аутентификации пользователя.

3) Статический контроль целостности – это:

а. контроль целостности любых файлов, расположенных на жестком диске СВТ в момент начала сеанса пользователя.

б. контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

в. контроль целостности любых файлов, расположенных на жестком диске СВТ в момент начала сеанса пользователя и контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

г. все перечисленное неверно.

4) Динамический контроль целостности – это:

а. контроль целостности любых файлов, расположенных на жестком диске СВТ в момент начала сеанса пользователя.

б. контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

в. контроль целостности любых файлов, расположенных на жестком диске СВТ в момент начала сеанса пользователя и контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

г. все перечисленное неверно.

5) Какое из требований ниже соответствует дискреционной политике управления доступом?

а. задана решетка уровней конфиденциальности, субъект может получить доступ к сущности только в случае, когда уровень его доступа позволяет предоставить ему доступ к сущности с заданным уровнем конфиденциальности, и реализация доступа не приведет к возникновению информационных потоков «сверху вниз».

б. задана матрица доступов, субъект может получить определенный доступ к сущности, если в соответствующей ячейке этой матрицы есть соответствующее право доступа.

в. задано множество ролей, субъект обладает правом доступа к сущности, когда он обладает ролью, которой соответствует множество прав доступа, содержащее данное право доступа к данной сущности.

г. задан порядок безопасного взаимодействия субъектов системы, обеспечивающий невозможность воздействия на систему защиты и модификацию ее параметров или конфигурации.

6) Какое из требований ниже соответствует мандатной политике управления доступом?

а. задана решетка уровней конфиденциальности, субъект может получить доступ к сущности только в случае, когда уровень его доступа позволяет предоставить ему доступ к сущности с заданным уровнем конфиденциальности, и реализация доступа не приведет к возникновению информационных потоков «сверху вниз».

б. задана матрица доступов, субъект может получить определенный доступ к сущности, если в соответствующей ячейке этой матрицы есть соответствующее право доступа.

в. задано множество ролей, субъект обладает правом доступа к сущности, когда он обладает ролью, которой соответствует множество прав доступа, содержащее данное право доступа к данной сущности.

г. задан порядок безопасного взаимодействия субъектов системы, обеспечивающий невозможность воздействия на систему защиты и модификацию ее параметров или конфигурации.

7) Какое из перечисленных средств является средством разграничения доступа пользователей для ОС Windows?

а. СЗИ НСД «Аккорд-АМДЗ».

б. ПАК СЗИ НСД «Аккорд-Win64».

в. ПАК СЗИ НСД «Аккорд-X».

г. ПАК «Аккорд-В.».

8) Какое из перечисленных средств является средством разграничения доступа пользователей для ОС Linux?

а. СЗИ НСД «Аккорд-АМДЗ».

б. ПАК СЗИ НСД «Аккорд-Win64».

в. ПАК СЗИ НСД «Аккорд-X».

г. ПАК «Аккорд-В.».

9) При помощи какого из перечисленных средств можно реализовать принцип непрерывности контрольных процедур в инфраструктуре виртуализации VMware vSphere?

а. СЗИ НСД «Аккорд-АМДЗ».

б. ПАК СЗИ НСД «Аккорд-Win64».

в. ПАК СЗИ НСД «Аккорд-X».

г. ПАК «Аккорд-В.».

10) Какие из перечисленных проблем возникают при проектировании системы безопасности инфраструктуры виртуализации?

а. проблема «суперпользователя» (сосредоточение максимальных привилегий в рамках одной роли).

б. проблема сегментирования (разбиения системы на сегменты и обеспечения их изоляции).

в. проблемы «суперпользователя» (сосредоточение максимальных привилегий в рамках одной роли) и сегментирования (разбиения системы на сегменты и обеспечения их изоляции).

г. проблема отсутствия прав доступа у администратора виртуальной инфраструктуры к сервису регистрации событий.