

Понадобятся две виртуальные машины, объединенные в одну сеть.

1. Установить на VM1 Сервер безопасности Dallas Lock.
2. Установить Клиент Dallas Lock на VM2, выполнить подключение к Серверу безопасности.
3. Выполнить настройку Dallas Lock 8.0 на VM1 в соответствии со следующими требованиями РД АС для класса защищенности 1Г:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) – это логин, и паролю условнопостоянного действия (90 дней), длиной не менее шести буквенно-цифровых символов;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);
- должна быть обеспечена целостность программных средств СЗИ НСД. Целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

4. Далее применить эти политики на VM2.

5. Выполнить следующее требование РД АС.

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Матрица доступа:

Каталог: C:\Документы\User1		
Права доступа	User1	Полный доступ
	User2	Нет доступа
Каталог: C:\Документы\User2		
Права доступа	User1	Чтение
	User2	Полный доступ

Создать пользователей на VM1 User1, User2.

Создать папку на диске C:\ “Документы”. В папке “Документы” создать папки “User1”, “User2”. Настроить доступ к каталогам в соответствии с матрицей доступа. Проверить настройку.