Acronis

1. Установить Acronis (с использованием серийного номера)
2. Создать план резервного копирования. Параметры для плана выбираются администратором системы, поскольку в нормативных документах не прописаны.
3. Удалить Acronis
   В отчете представить пояснения к выбранным параметрам.

Dallas Lock

Запустить WMPlayer. Открыть виртуальную машину.

1. Создать пользователя DLadmin с правами администратора.
2. Установить Dallas Lock из-под пользователя DLadmin
3. Создать пользователей User01 и User02
4. Настроить Dallas Lock в соответствии с требованиями к классу 1Г и матрицей доступа

Пользователь	**PDocs**	**SDocs**	**SSDocs**
User01	R--	RWX	---
User02	R--	---	RWX
DLadmin	RWX	RWX	RWX

5. Зайти поочередно под пользователями User01 и User02 и проверить, имеет ли каждый из них доступ к папкам PDOcs, SDocs и SSDocs.
6. Сделать скриншоты вкладок, где отображены настройки
7. Удалить Dallas Lock, созданные папки и пользователей

Secret Net

Установить SecretNet на виртуальной машине VMware Player.

1. Настроить политику паролей:
   срок действия 7 дней;
   мин. длина пароля 6 символов;
   пароль должен отвечать требованиям сложности.
2. Создать нового пользователя user_257;
3. Ознакомиться с механизмом полномочного разграничения доступа:
   Назначить пользователю уровень допуска “конфиденциально”, присвоить различные категории конфиденциальности («строго конфиденциально», «конфиденциально», «неконфиденциально») ресурсам (папкам), проверить, к каким из ресурсов пользователь имеет доступ, если заходит в сессии «открытые данные» и «конфиденциально»;

4. Дополнительное задание. На примере одного устройства (USB-накопитель) выполнить настройку механизма контроля аппаратной конфигурации: настроить политику контроля; включить «мягкий»/ «жесткий» режим работы механизма, проверить, как ведет себя система при подключении USB-накопителя.

Удалить Secret Net и созданного пользователя!

В отчете представить сравнение Dallas Lock и Secret Net (либо в форме пояснения, какое средство защиты показалось вам удобнее, либо в форме таблицы сравнения по функционалу)

Vipnet

Работа в парах.

1. На компьютере 1 установить сканер уязвимостей XSpider.
2. Провести сканирование компьютера 2. Сохранить результаты.
3. Установить на компьютер 2 межсетевой экран Vipnet Personal Firewall.
4. С компьютера 1 провести повторное сканирование компьютера 2, сохранить результаты.
5. На компьютере 2 в фильтр межсетевого экрана добавить адрес компьютера 1. Еще раз провести сканирование компьютера 2.
6. Удалить XSpider и Vipnet Personal Firewall.

В отчете представить сравнение результатов сканирования в трех случаях.

Trust Access

Работа на виртуальной машине

1. Установить межсетевой экран Trust Access. (сервер-админ-агент)
2. Настроить межсетевой экран таким образом, чтобы все входящие TCP, UDP и ICMP пакеты были запрещены, а DHCP пакеты разрешены
3. Проверить с другого компьютера доступность защищенного компьютера с помощью ping запроса
4. Разрешить ICMP запросы в межсетевом экране
5. Проверить с другого компьютера доступность защищенного компьютера с помощью ping запроса
6. **Удалить Trust Access**

В отчете представить скриншоты настроенных правил и сравнение Trust Access и Vipnet Personal Firewall.