ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ

Курсовая работа

«МОДЕЛИРОВАНИЕ ЭТАПОВ ШИФРОВАНИЯ ДИСКОВ И ФАЙЛОВ С ПОМОЩЬЮ СРЕДСТВ WINSERVER 2016»

Выполнил:
студент III курса группы ССА–39
специальности 09.02.06 Системное и сетевое администрирование
Щенников Максим Михайлович.

Руководитель:
Агибалова Кристина Евгеньевна.

Стерлитамак, 2020

- **Цель проекта: с**моделировать этапы шифрования дисков и файлов с помощью средств winserver 2016.

- Задачи проекта:
  - 1. Рассмотреть учебно-техническую литературу по теме курсовой работы.
  - 2. Рассмотреть понятия и способы обеспечения безопасности данных, описать особенности шифрования дисков и файлов.
  - 3. Описать технологию реализации роли «BitLocker Drive Encryption» для шифрования дисков и файлов.
  - 4. Смоделировать объекты сетевой инфраструктуры локальной сети.
  - 5. Смоделировать этапы шифрования дисков и файлов средствами Windows Server 2016

- BitLocker (точное название BitLocker Drive Encryption) – это технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft. Она впервые появилась в Windows Vista.
- С помощью BitLocker можно было шифровать тома жестких дисков, но позже, уже в Windows 7 появилась похожая технология BitLocker To Go, которая предназначена для шифрования съемных дисков и флешек.

В своей работе BitLocker использует 5 режимов работы:

– TPM + PIN (персональный идентификационный номер) + пароль

Система шифрует информацию с помощью TPM, кроме того, администратор должен ввести свой PIN-код и пароль для доступа.

– TPM + пароль

Система шифрует информацию с помощью TPM, и администратор должен предоставить код доступа.

– TPM + ключ

Система шифрует информацию с помощью TPM, и администратор должен предоставить ваш идентификатор доступа.

– Только ключ

Администратор должен предоставить пароль для доступа к управлению.

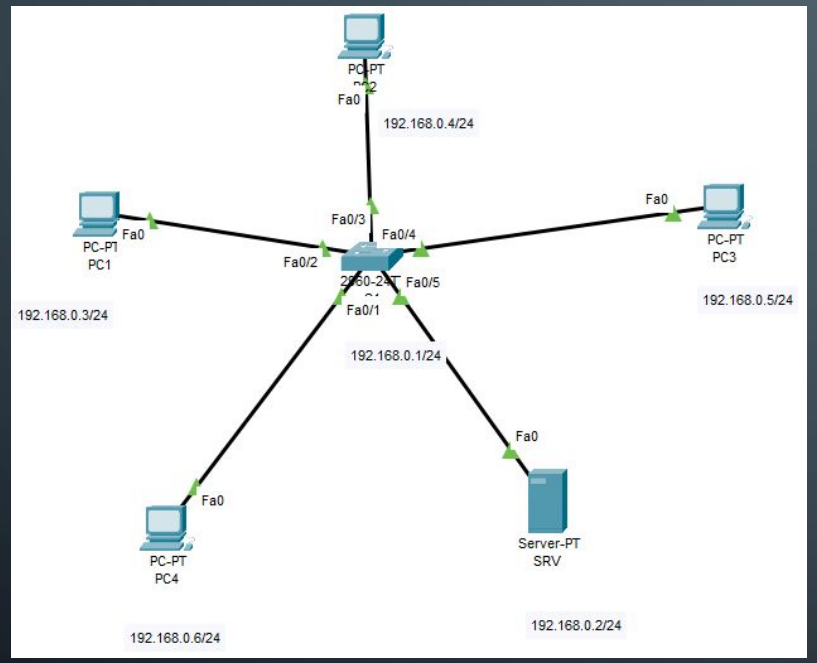
– Только TPM: никаких действий не требуется от администратора.

- С помощью BitLocker можно зашифровать весь диск с данными. С помощью групповой политики можно указать на необходимость включения BitLocker для диска, прежде чем на него будут записаны данные. В BitLocker можно настроить различные методы разблокировки для дисков с данными, при этом такие диски поддерживают несколько способов разблокировки.

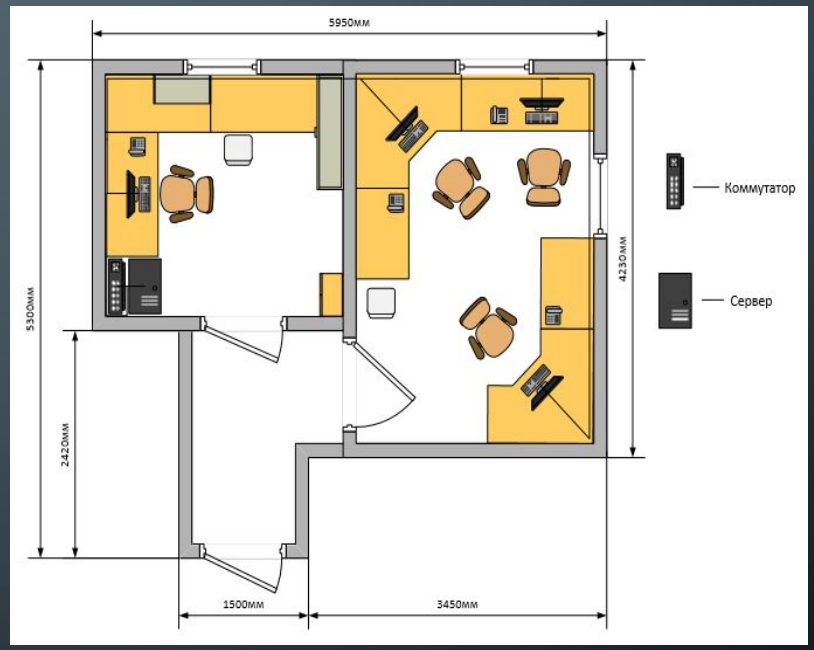
Процесс расшифровки диска

- При запуске система ищет подходящий предохранитель ключа, опрашивая TPM, проверяя порты USB или, если необходимо, запрашивая пользователя (что называется восстановлением). Обнаружение предохранителя ключа позволяет Windows расшифровать ключ VMK, которым расшифровывается ключ FVEK, которым расшифровываются данные на диске

Логическая и физическая топологии локальной сети организации можно представить в графическом виде

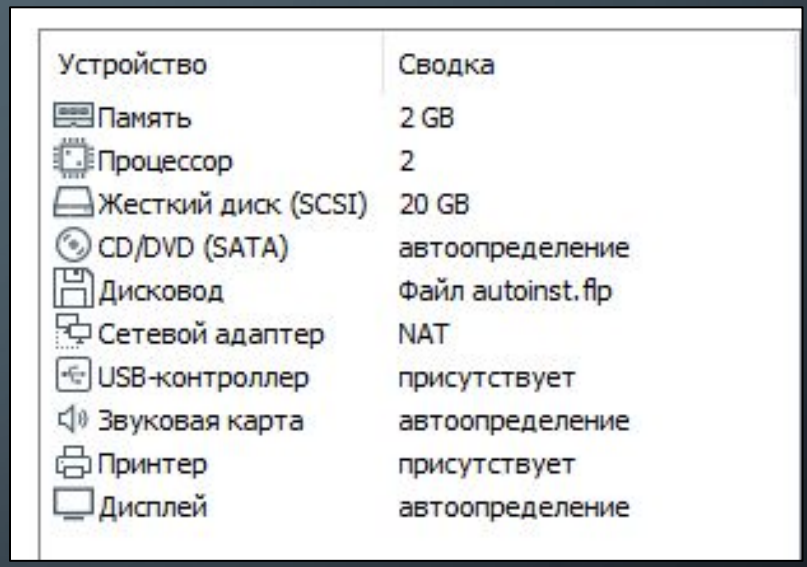


Логическая топология



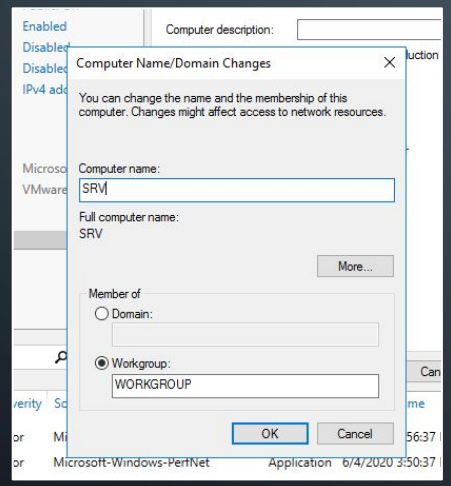
Физическая топология

Для того, чтобы виртуальная машина стабильно функционировала мы изучили минимальные системные требования Windows Server 2016, которыми являются:
процессор: 1.4 GHz 64-bit, совместимость с набором команд x64, поддержка NX и DEP, поддержка CMPXCHG16b, LAHF/SAHF и PrefetchW, поддержка Second Level Address Translation (EPT или NPT);
объём оперативной памяти: минимум 512 MB (2 GB для Server с вариантом установки Desktop Experience);
В соответствии с этими данными была создана и настроена виртуальная машина со следующими параметрами

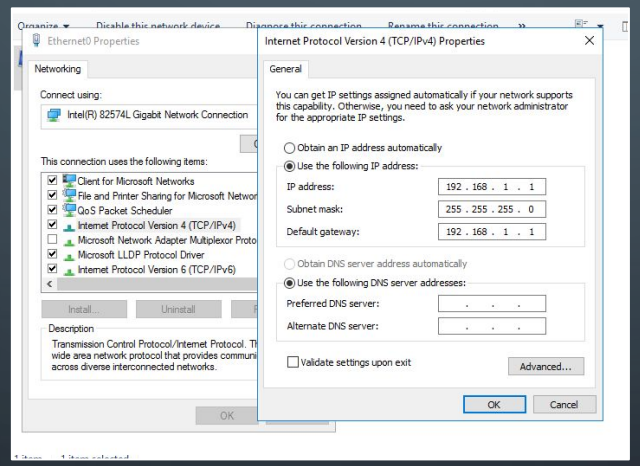


Устройство	Сводка
Память	2 GB
Процессор	2
Жесткий диск (SCSI)	20 GB
CD/DVD (SATA)	автоопределение
Дисковод	Файл autoinst.flp
Сетевой адаптер	NAT
USB-контроллер	присутствует
Звуковая карта	автоопределение
Принтер	присутствует
Дисплей	автоопределение

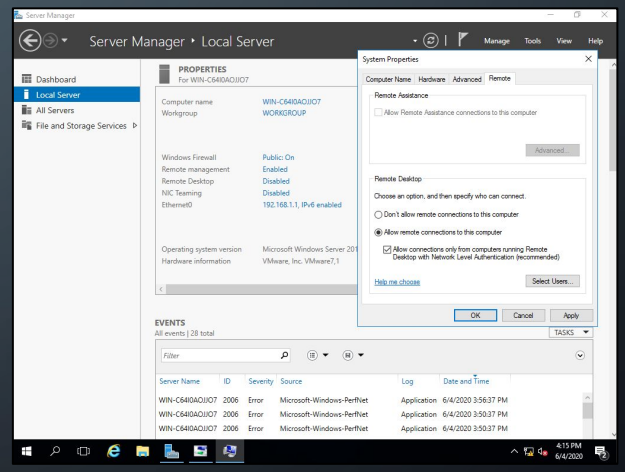
Для шифрования дисков и файлов необходимо произвести первоначальную настройку сервера для корректной установки и работы роли BitLocker Drive Encryption: необходимо изменить сетевое имя, ввести компьютер в домен, назначить статический IP-адрес и включить удалённый рабочий стол.



Изменение имени сервера



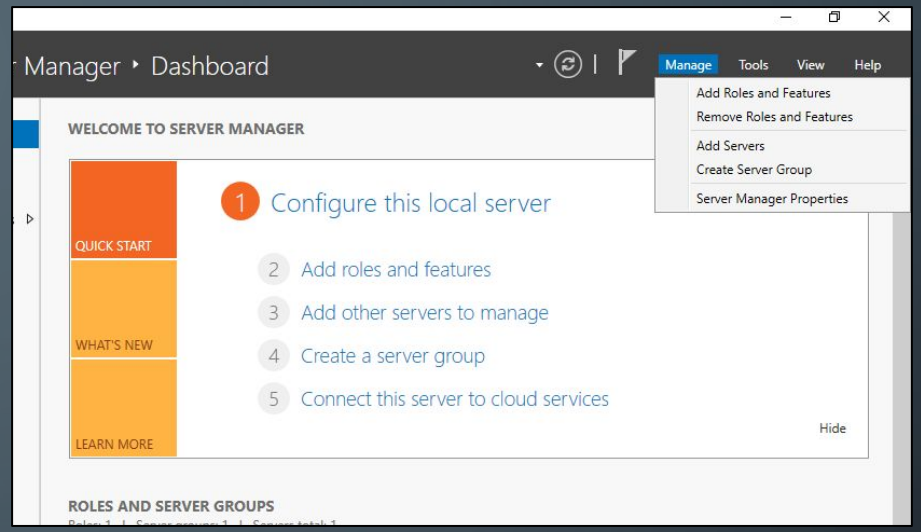
Изменение ip адреса сервера

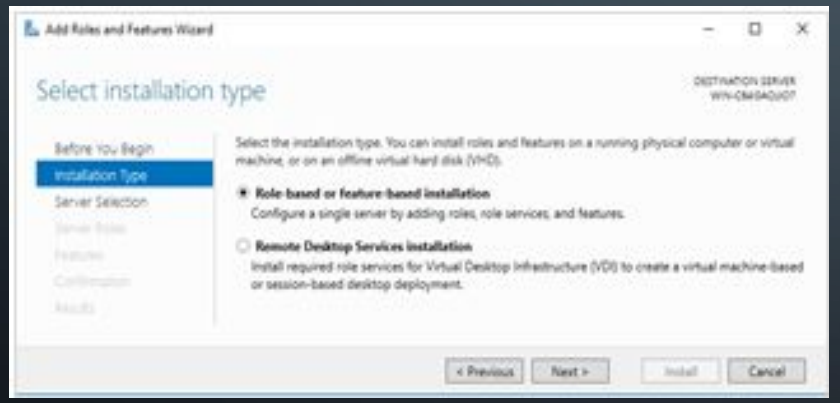


Включение удалённого рабочего стола

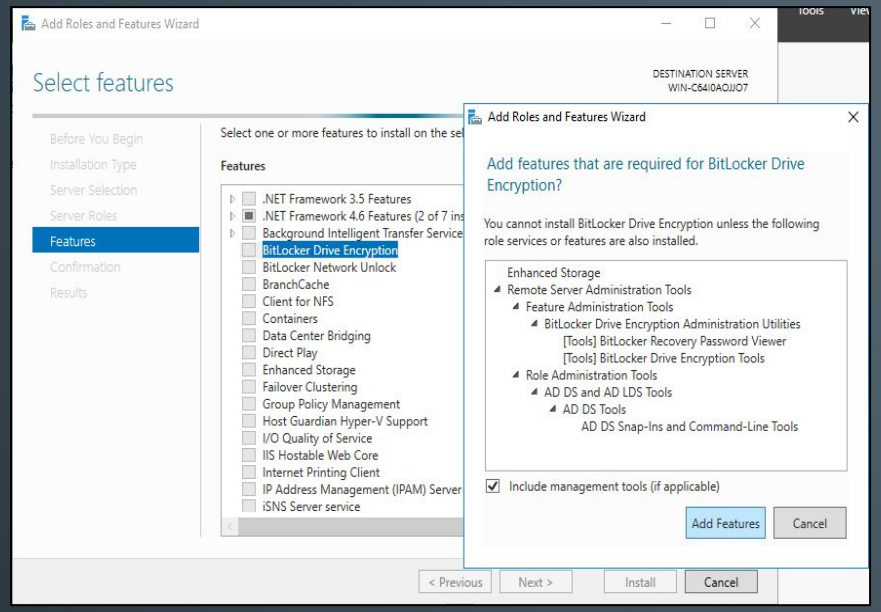
Установка роли BitLocker

Переходим к администратору сервера или диспетчеру сервера и выбираем **«Добавить роли и функции»**, расположенные в быстром запуске или в **меню «Управление»**





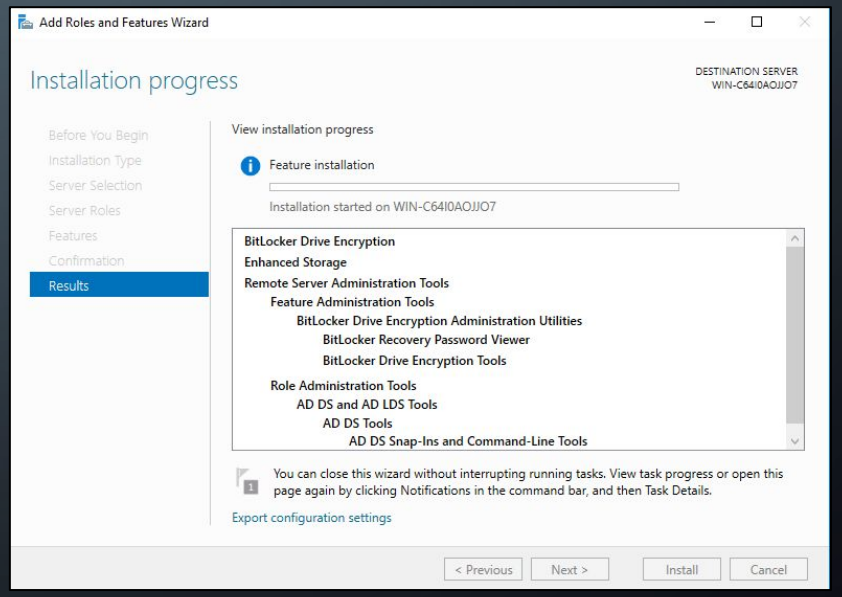
В открывшемся окне мы нажимаем далее, выбираем Установка на основе ролей или характеристик, снова нажимаем «Далее»



В следующем окне мы выбираем наш сервер и нажимаем далее, в окне роли мы нажимаем далее, потому что функция установлена, а не роль.

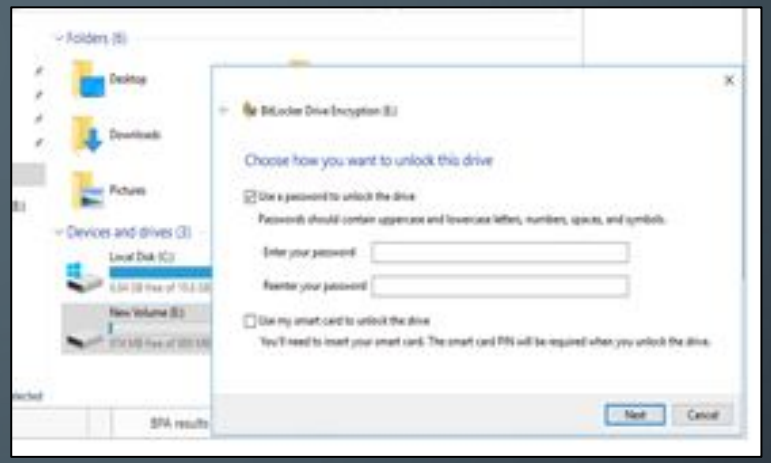
В окне «Выбор компонентов» мы выбираем параметр «Шифрование диска BitLocker»

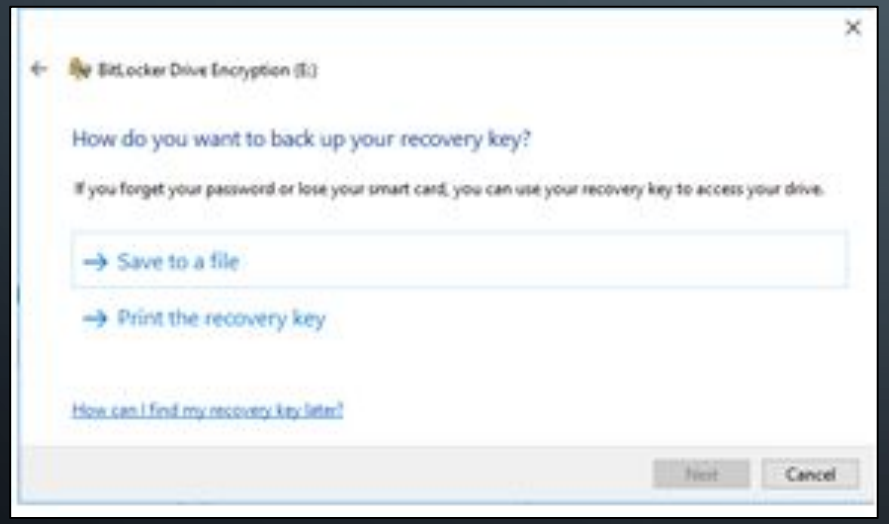
Нажимаем «Установить», чтобы начать процесс



Настройка BitLocker

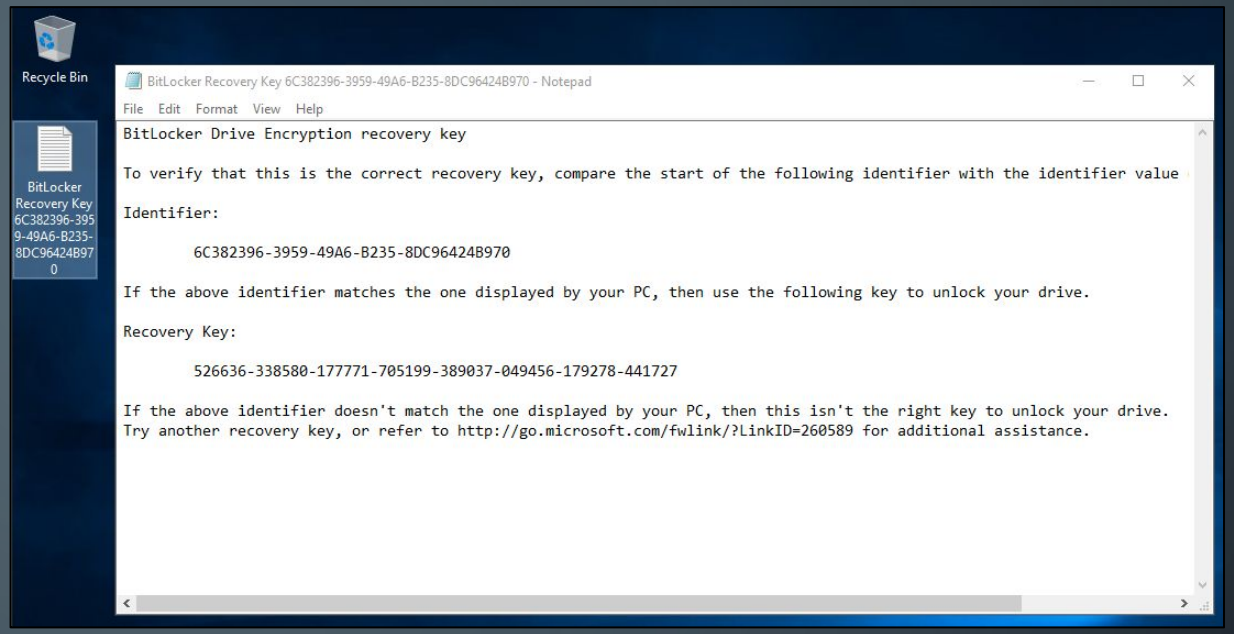
Запускаем BitLocker на созданном тестовом диске и задаём пароль

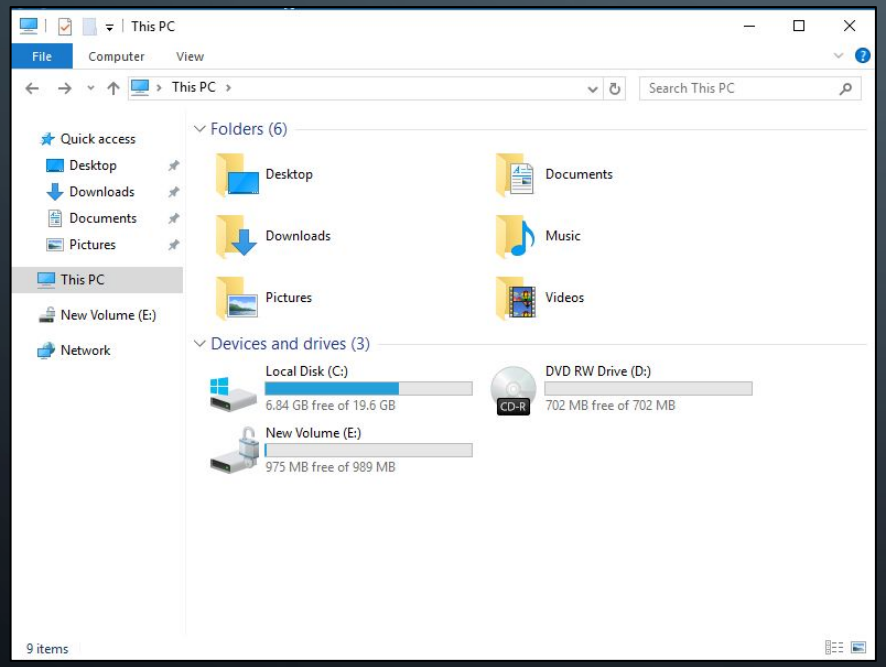




Сохраняем ключ восстановления в файл, а также можем распечатать на принтере

Ключ был сохранён на рабочем столе





Для проверки того что диск был успешно зашифрован нужно зайти в мой компьютер

Заключение

В процессе выполнения курсовой работы, были выполнены все поставленные задачи. Найдена и рассмотрена учебно-техническая литература по теме курсовой работы. С помощью статей, находящихся в глобальной сети интернет, а также используя электронно-библиотечные системы типа Znanium, была сформирована структура курсовой работы, её этапы, шаги, а также некоторые основные понятия.

В соответствии с вышеизложенным, цель курсового проекта достигнута путем решения поставленных задач, смоделирована организация сетевой безопасности организации на основе настройки роли BitLocker в Windows Server 2016.

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ

Курсовая работа

«МОДЕЛИРОВАНИЕ ЭТАПОВ ШИФРОВАНИЯ ДИСКОВ И ФАЙЛОВ С ПОМОЩЬЮ СРЕДСТВ WINSERVER 2016»

Выполнил:
студент III курса группы ССА–39
специальности 09.02.06 Системное и сетевое администрирование
Щенников Максим Михайлович.

Руководитель:
Агибалова Кристина Евгеньевна.

Стерлитамак, 2020