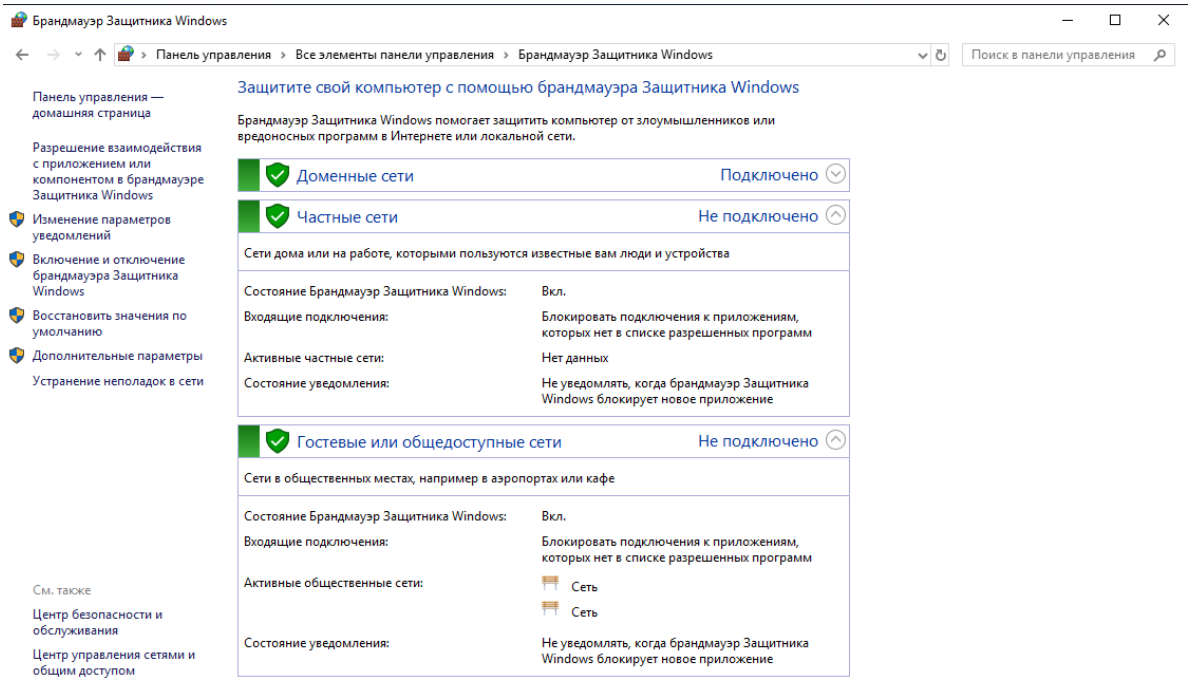
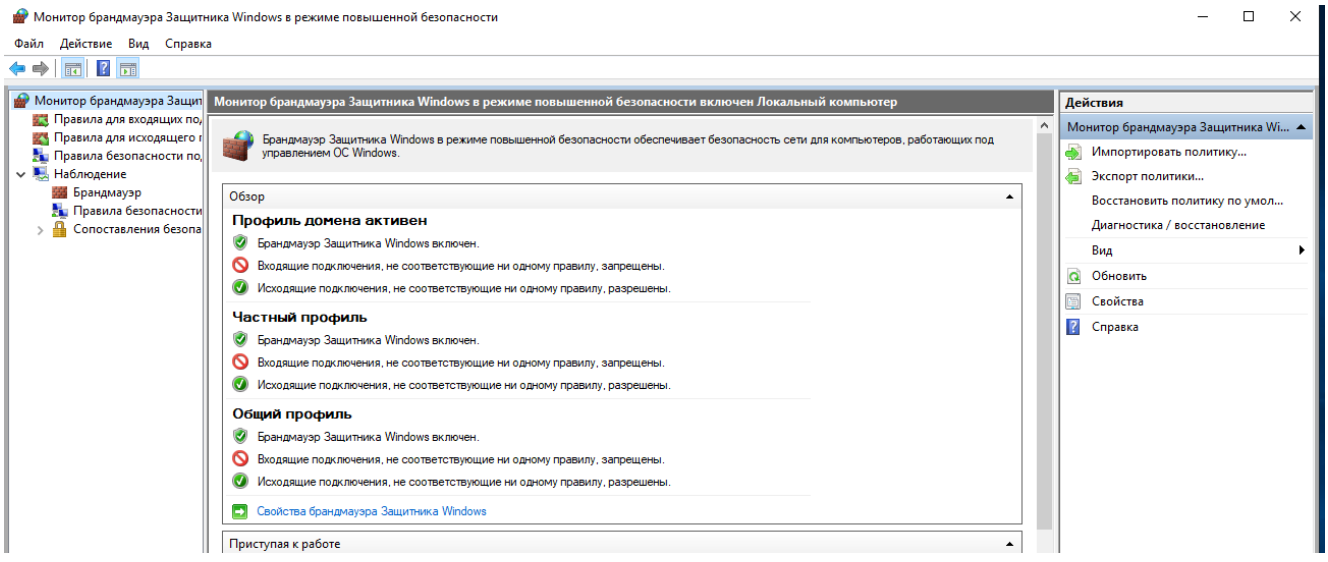
Выполнил Мешечкин Д. Инфобез-2345
Задание 1-7: Брэндмауэр и аудит
- Включите все доступные профили брандмауэра Защитника Windows
- Создайте исходящее правило для Internet Explorer
- Создайте входящее правило для Internet Explorer
- Экспотрируйте настройки брандмауэра Защитника Windows
- Через локальные политики безопасности запретите запуск Internet Explorer
- Включите установку обновлений для Windows и других продуктов Microsoft
- Включите Аудит событий входа успех\отказ

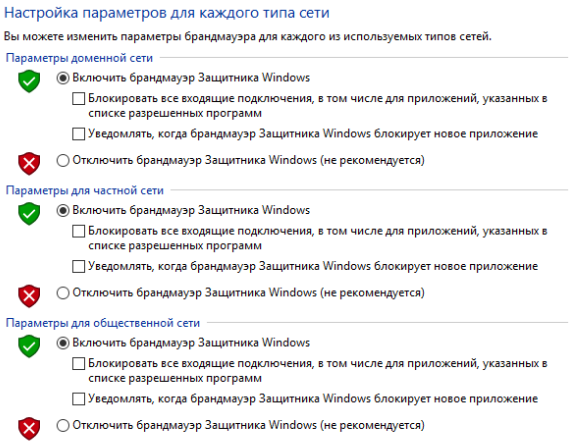
Выполнение данного ДЗ№9 также будет происходить на сервере WinServ2019GUI. Для просмотра активных и доступных профилей брэндмауэра необходимо зайти "Панель управления -> (В зависимости от выбранного отображения значков - Мелкие или Крупные значки) Брэндмауэр Защитника Windows". При открытии данной оснастки открывается окно, где будут отражены доступные профили:
- Домена (domain)
- Частный (Private)
- Общий (Public)

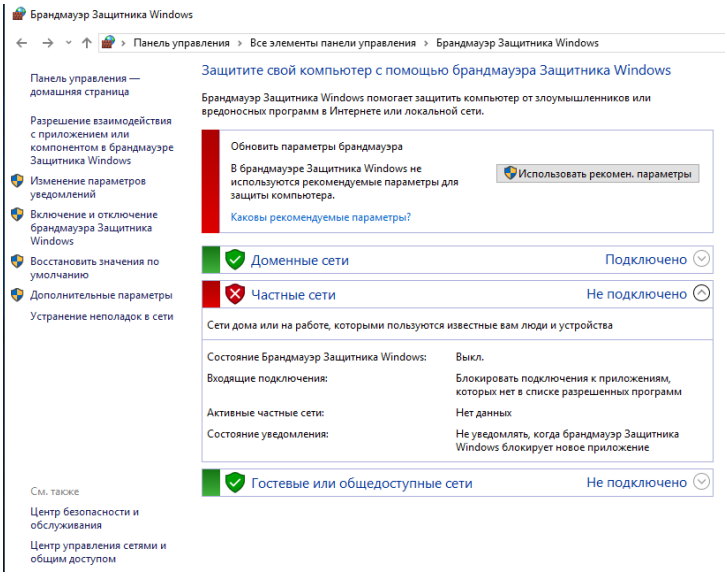


По данным монитора - все три профиля включены. Для более детального отображения и настройки в левой части окна "Дополнительные параметры". Открывается "Монитор брэндмауэра защитника Windows".

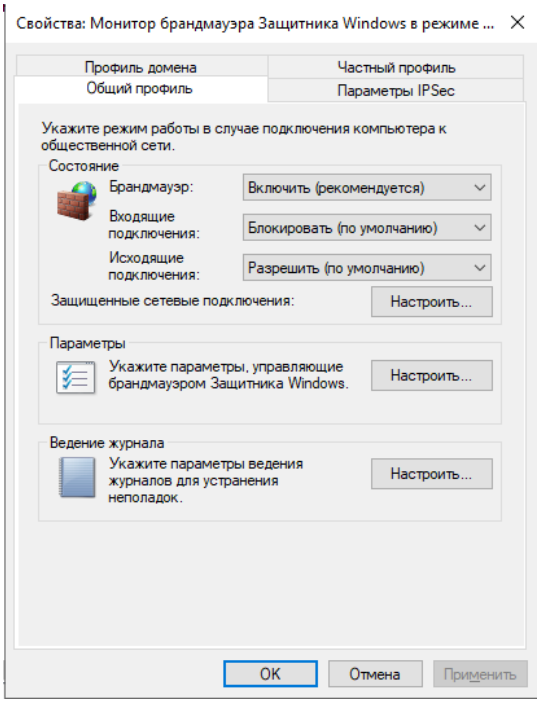


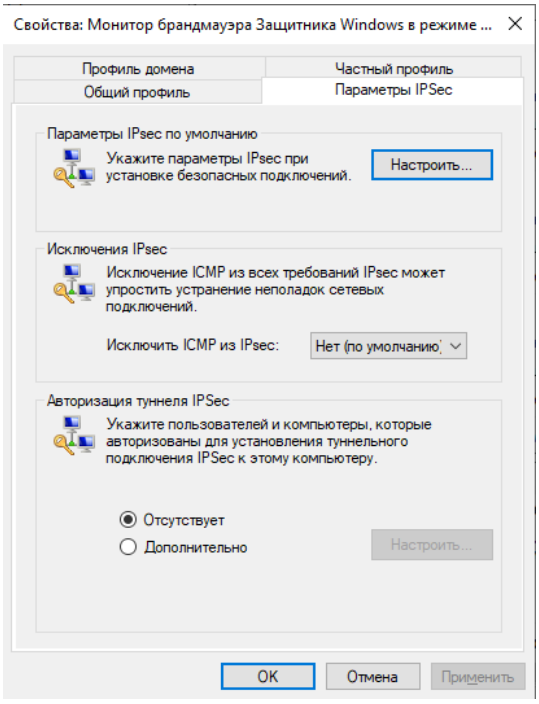
Для включения/отключения профилей аналогично в левой части окна "Включение и отключение брэндмауэра защитника" Далее уже в открывшемся окне выбираются необходимые профили, которые необходимо включить или выключить. Для пробы выключу для "частных сетей". После чего в активном окне монитора выключенный профиль изменит цвет и информацию о себе.



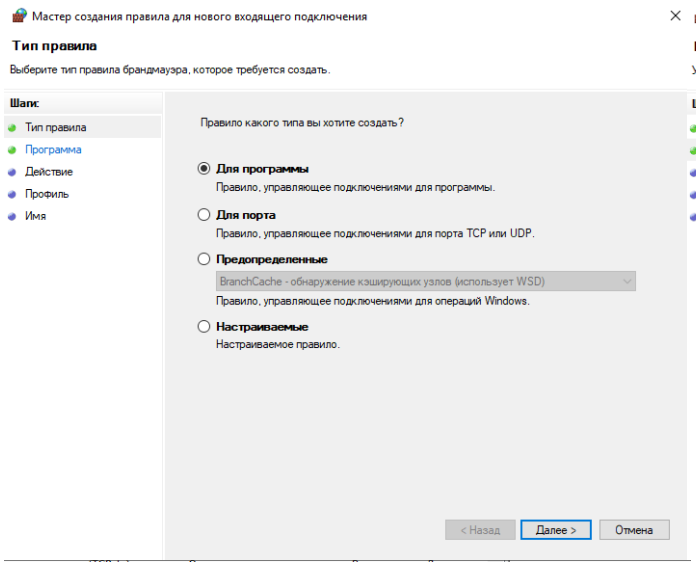


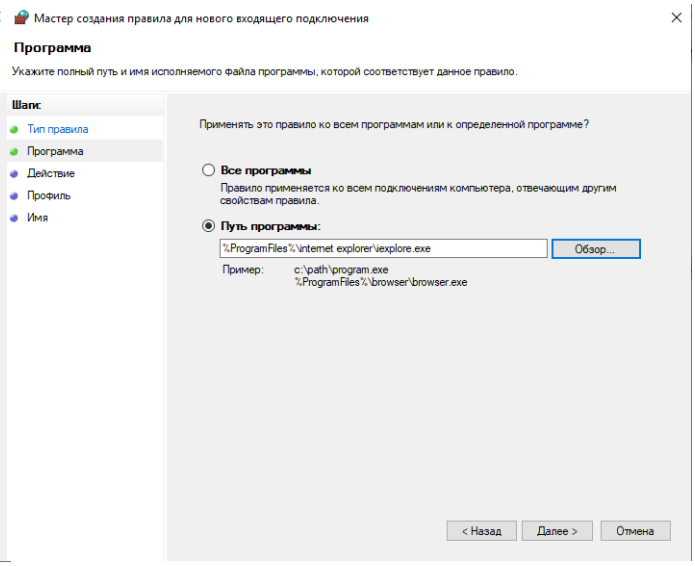
Для включения - необходимо проделать все действия в обратном порядке. Два действия.
Далее ещё один вариант просмотра включенных профилей - так же в "Мониторе", необходимо в левой части окна ПКМ на "Монитор брэндмауэра" -> Свойства. Далее открывается окно, где можно просмотреть статус профиля, активные подключения, настроить параметры и настроить ведение журнала. В данном окне свойств имеются четыре профиля:
- общий
- частный
- домена
- параметры IPSec



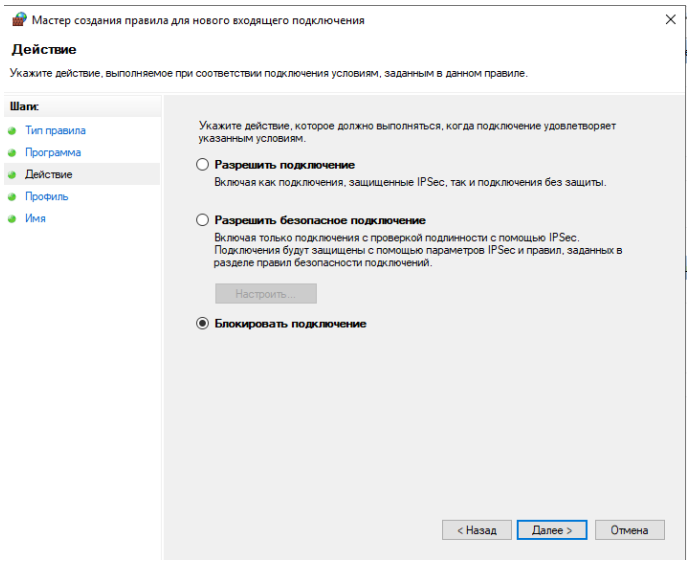


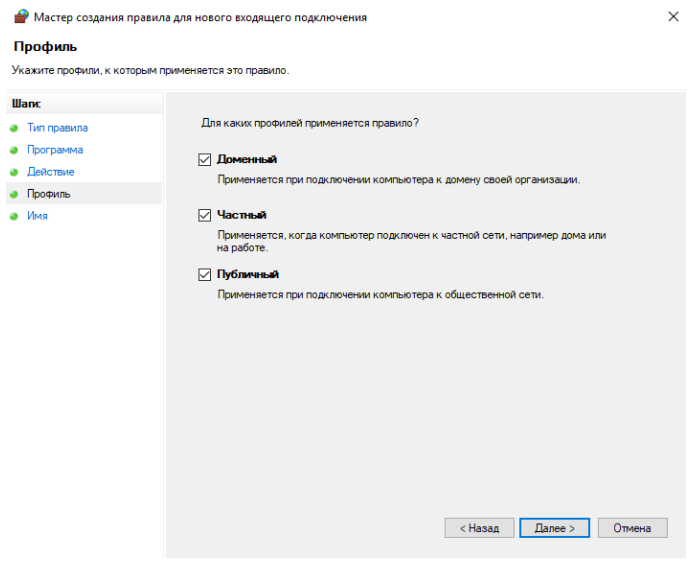
Для настройки исходящих/входящих правил в "Мониторе" в левом окне выбирается соответствующая строка "Правила для входящих/Правила для исходящих подключений".
Для создания - в правой части "Создать правило" и далее следовать подсказкам "мастера создания правил"



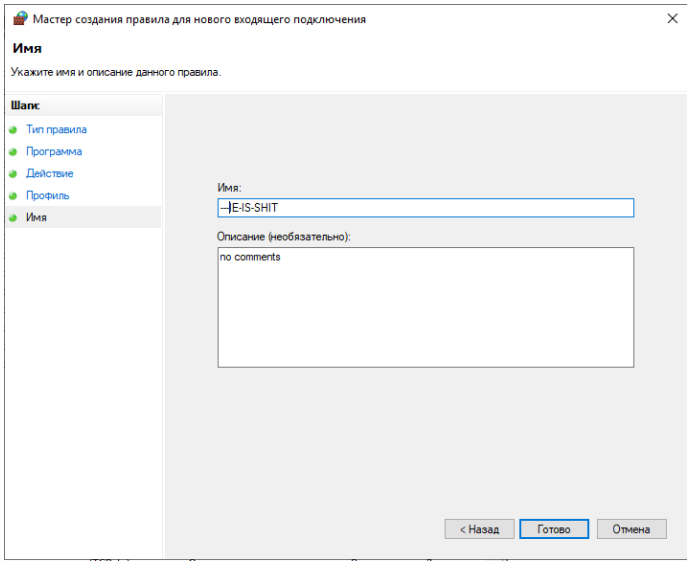


Далее в "мастере" заблокирую все подключения.

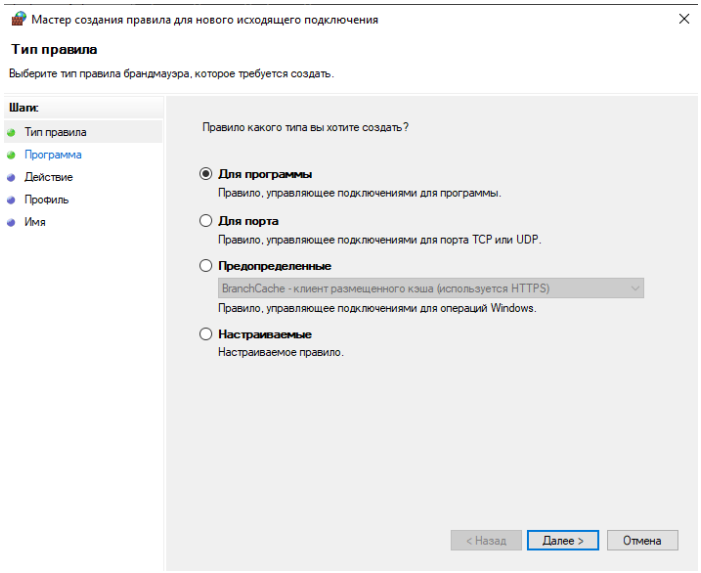


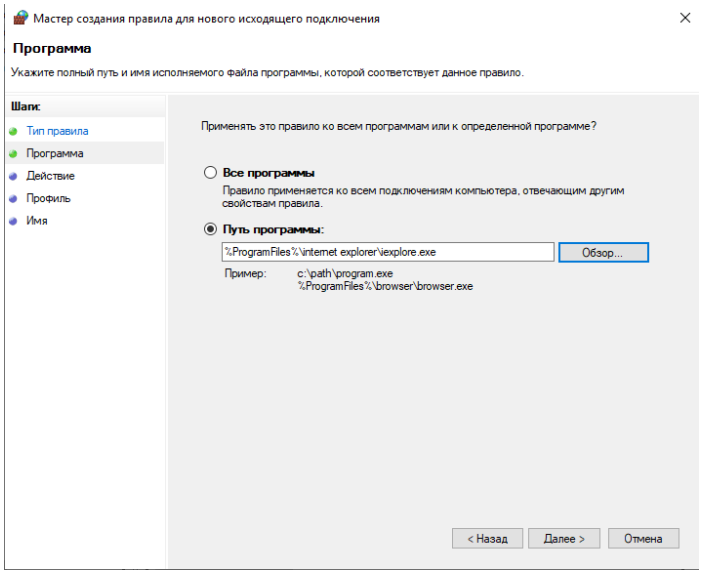


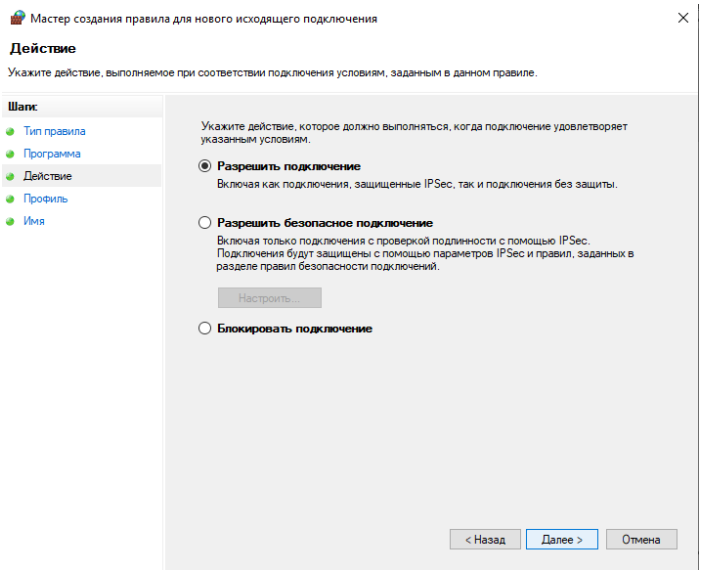
Таким образом все входящие соединения будут блокироваться для IE, в какой бы сети не происходила бы работа.

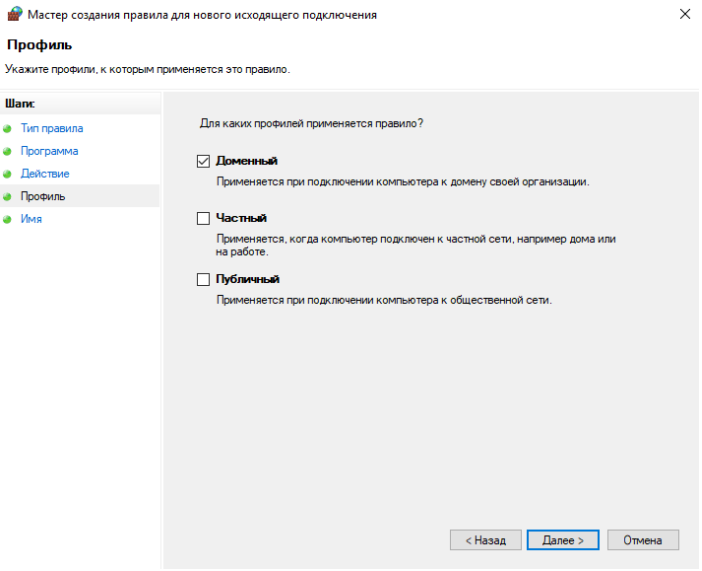


Далее создам правило для исходящих соединений для IE.

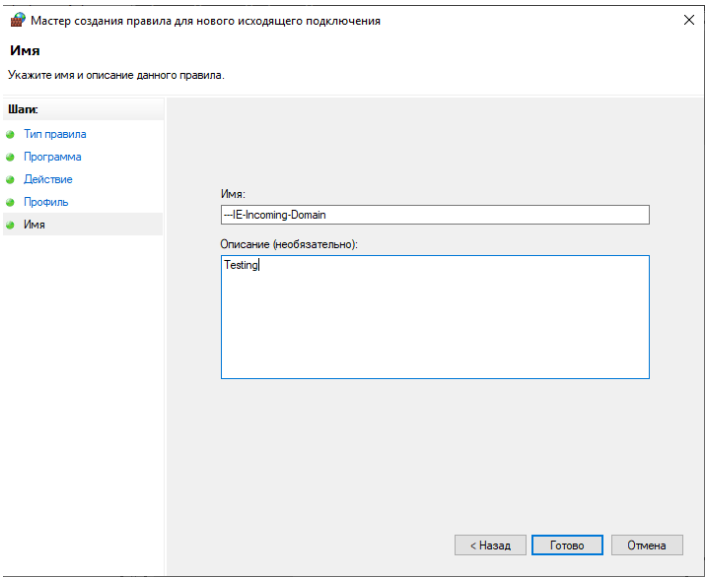




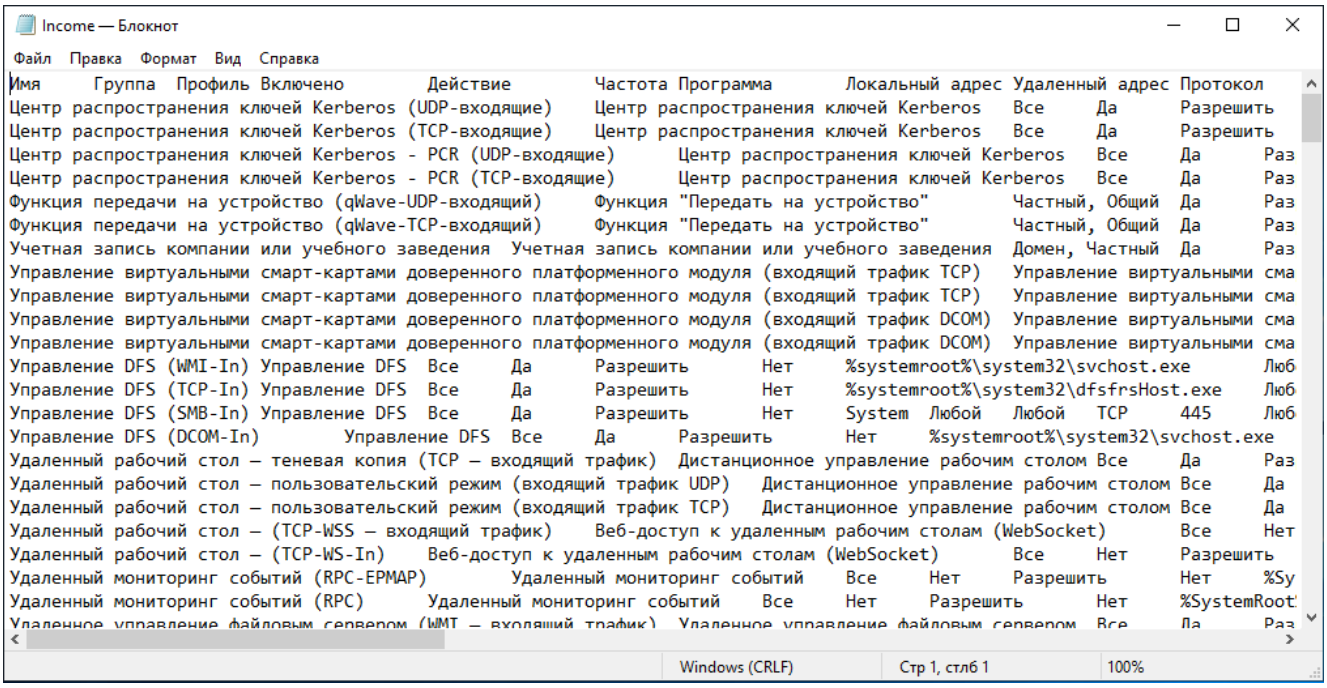




Таким образом для исходящих соединений в доменной сети будут доступно использования IE.

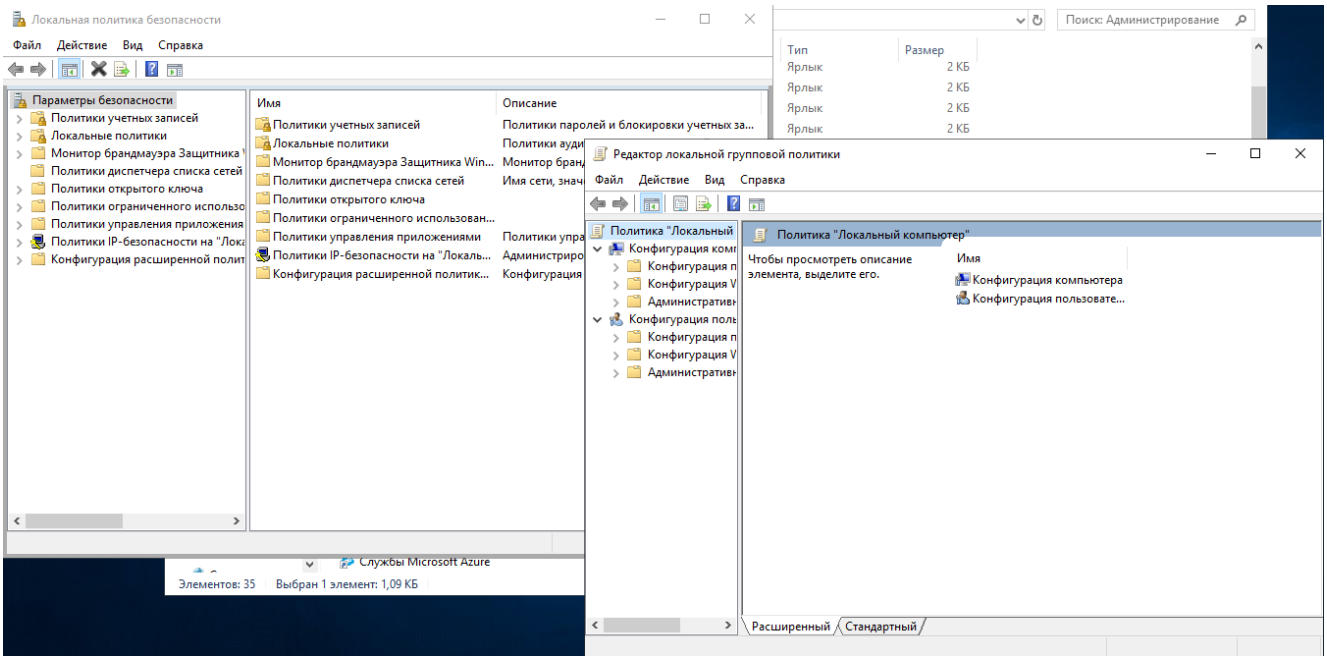


Для экспорта входящих/исходящих правил необходимо в соответствующем пункте "Монитора" выбрать в правом окне "Экспортировать список". Таким образом создастся текстовый файл с списком и настройками правил.

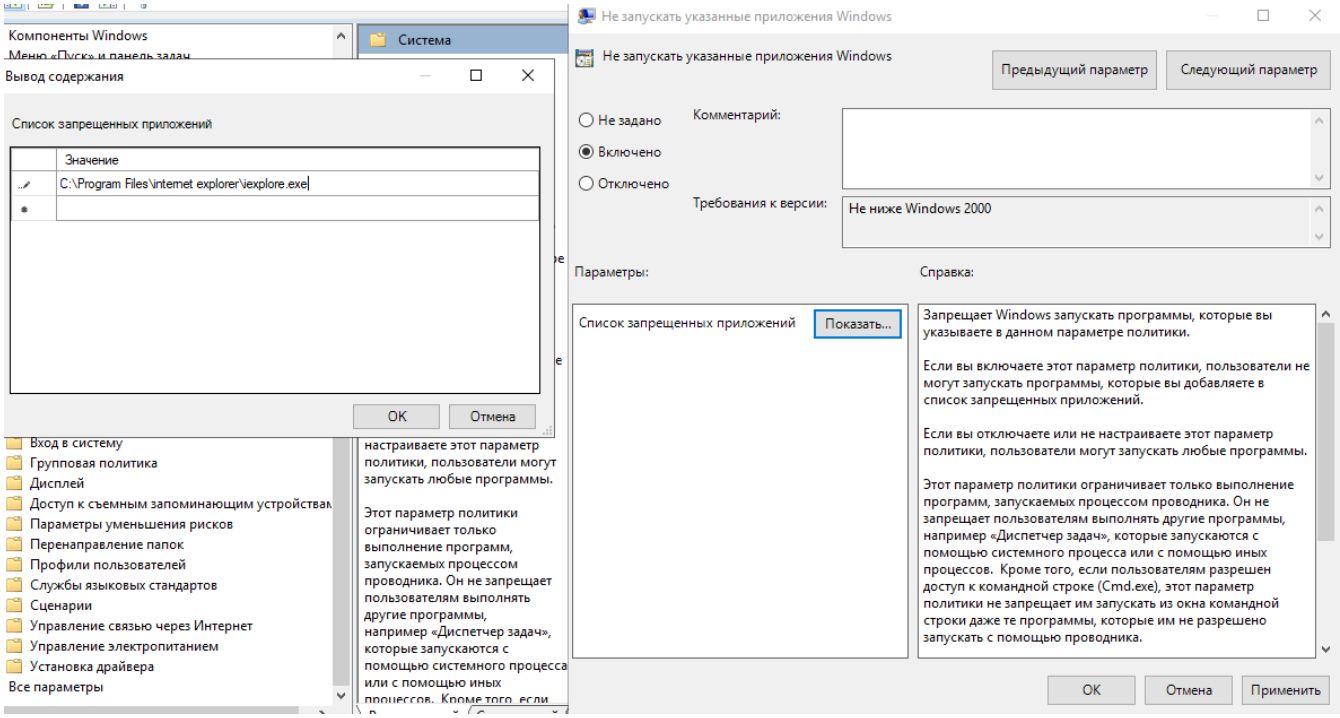


При экспортировании "общего раздела" брэндмауэра создастся файл политик *.wfw . Файл создается аналогичным образом, в правой части окна "Экспорт политики". Таким образом политики можно будет полностью импортировать на другие машины/домены/куда требуется.

Для запрета через локальную политику безопасности необходимо "Средства администрирования -> локальная политика безопасности". Вторым способом вывода окна редактирования локальных политик является вызов командой "gpedit.msc"

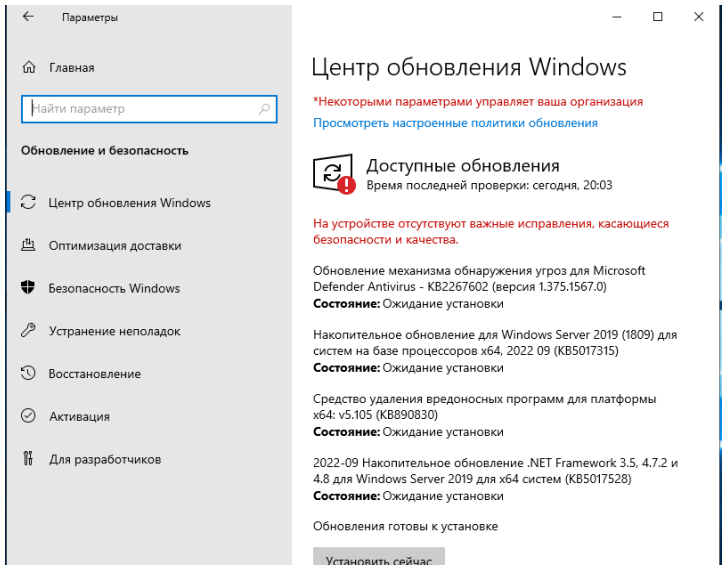


Для запрета определённых программ, будь то предустановленные на ПК или вновь принесённые юзверем на съемном носителе необходимо пройти: "Конфигурация пользователя -> Административные шаблоны -> Система". В открывшемся справа окне выбирается политика "Не запускать указанные приложение Windows".

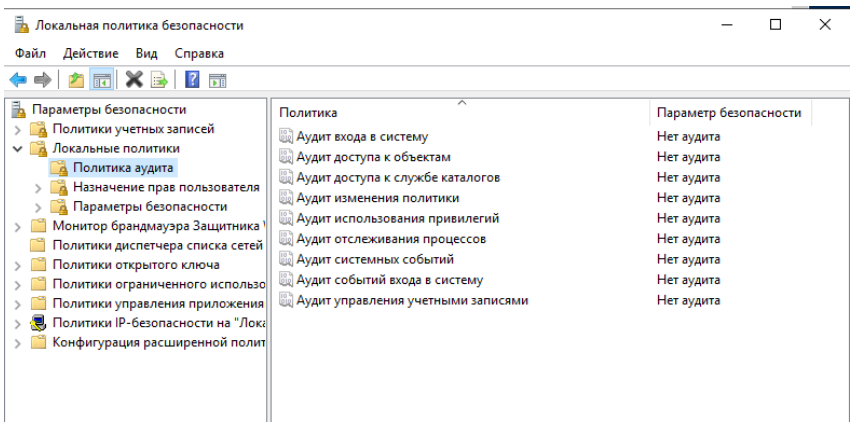


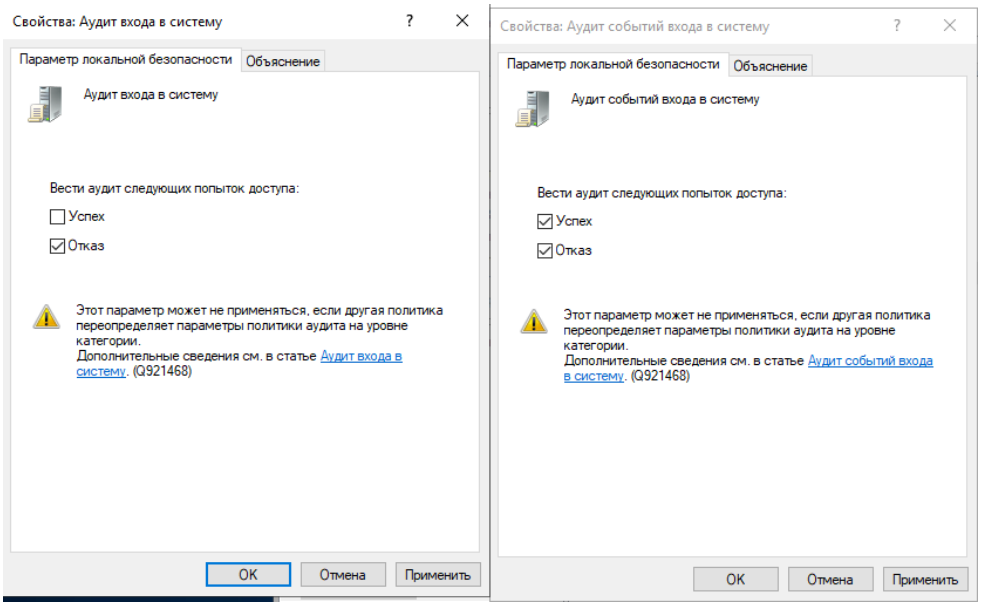
Политика активируется и в списке запрещённых приложений вносится путь до приложения. Далее необходимо обновить политики **"gpupdate /force"**. В итоге, доступ к приложению должен быть "заказан" для рядовых пользователей.

Для включения установки обновлений Windows в "Параметрах -> Обновление и безопасность" (Актуально для WinServer 2019, Win11, для более ранних версий данный пункт доступен в "Панели управления").
В данном окне можно далее настроить, включить и установить различные параметры при обновлении, включая период активности, установление лимитов на скачивание, журнал обновлений, а также список установленных обновлений, которые можно удалить.

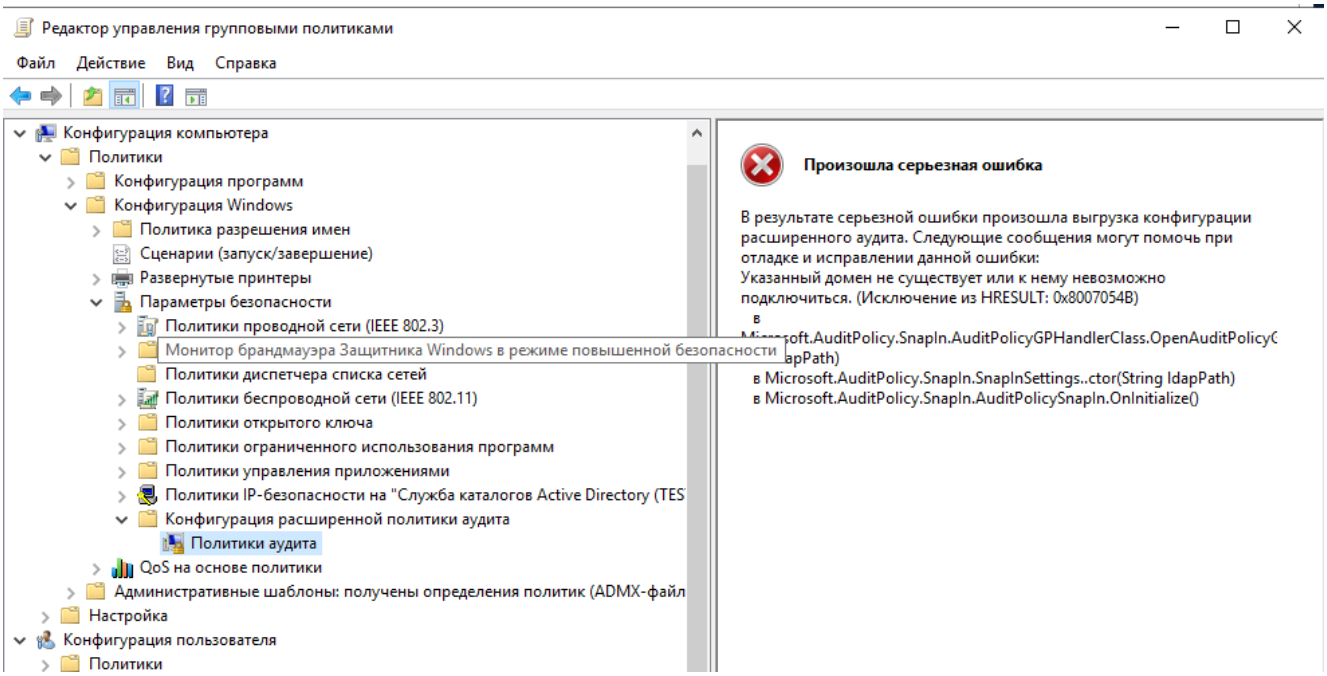


Журнал событий входа успех/отказ включается через групповую политику AD или через локальную политику безопасности. "Средства администрирования -> Локальная политика безопасности" Далее в открывшемся окне в левой части выбирается "Локальные политики -> Политика аудита" далее в открывшемся окне справа выбирается "Аудит входа в систему", "Аудит событий входа в систему". В данных

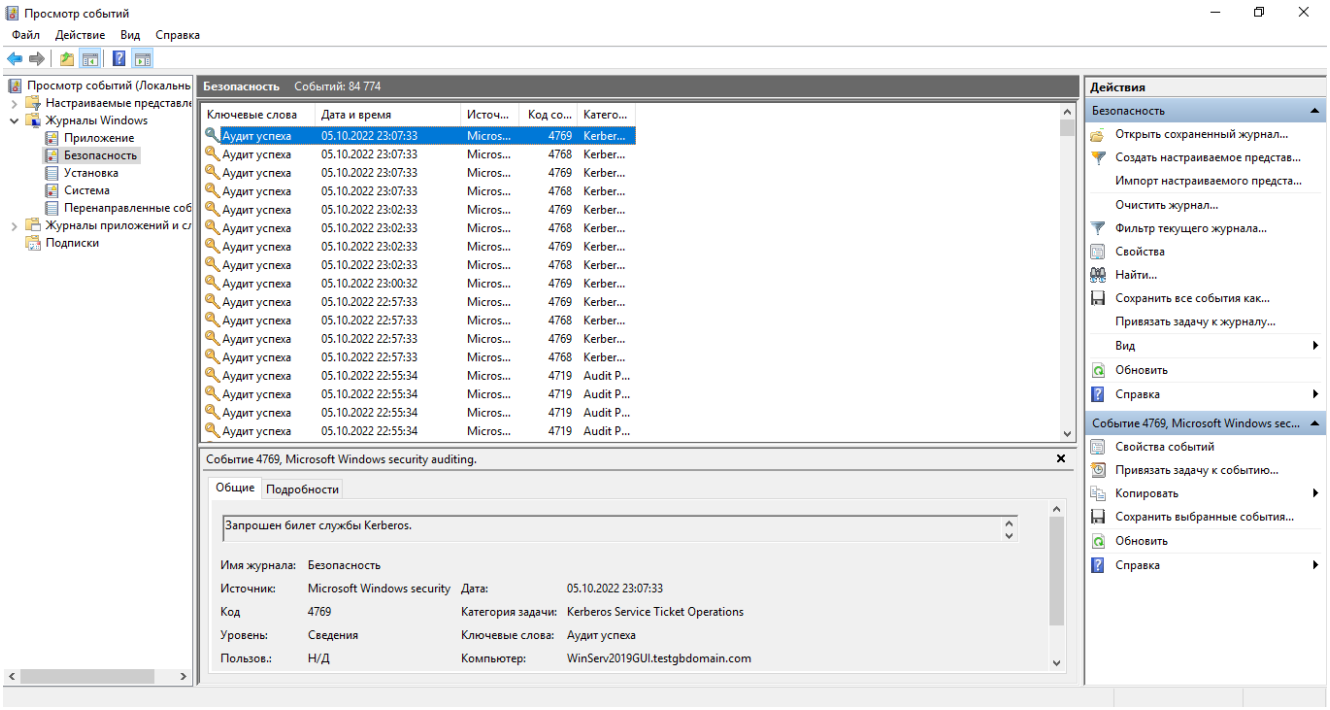




При данном варианте аудита, будет выводится "Неуспешные попытки входа в систему", а также "Успешные и не успешные попытки входа в систему".
При настройке аудита через "Управление групповой политикой" необходимо изменить "Default Domain Policy", далее "Конфигурация компьютера -> Политики -> Конфигурация Windows - > Параметры безопасности -> Конфигурация расширенной политики аудита -> Политика аудита" далее в правом окне будут доступны аналогичные варианты. В моём случае AD уже потихоньку начал сходить сума и выдавать всякую дичь. В любом случае, настройка доступа происходит таким же образом, как и выше.



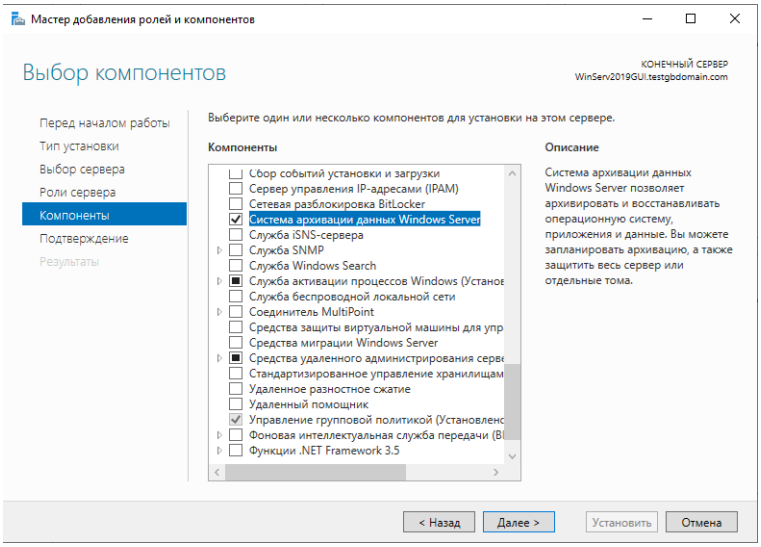
Сам журнал аудита "Win+R -> **eventvwr.msc** -> журнал Windows -> безопасность" и далее фильтровать по интересующим событиям.



Задание 8-11: Работа с архивацией данных и резервным копированием данных.

- Установите компонент «Система архивации данных Windows Server»
- Создайте задачу ежедневного резервного копирования системного диска в 23.00
- Удалите файлы с рабочего стола, затем восстановите их из резервной копии
- Восстановите состояние сервера используя загрузочный диск и ранее созданную резервную копию

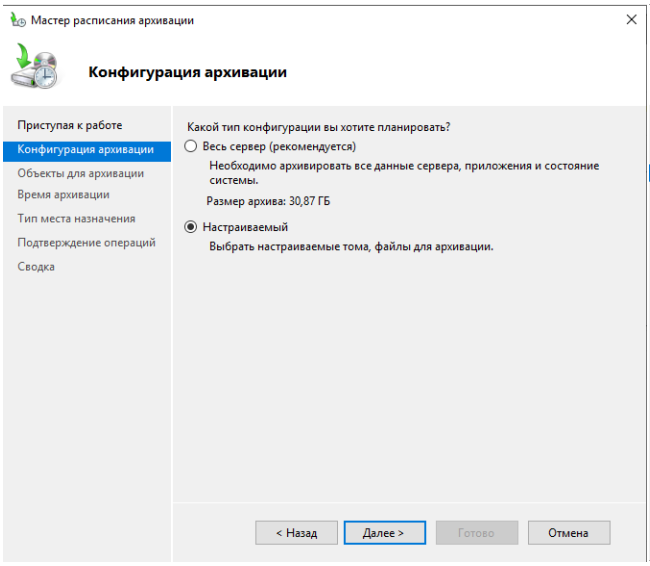
Для установки данного компонента - стандартная процедура "Диспетчер серверов -> Роли и компоненты" Далее в компонентах "Система архивации данных Windows Server". При необходимости выполнить перезагрузку.

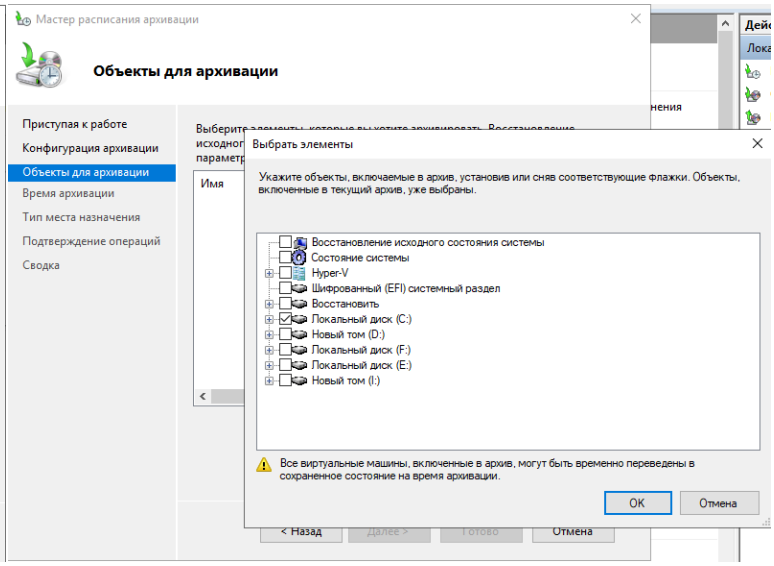


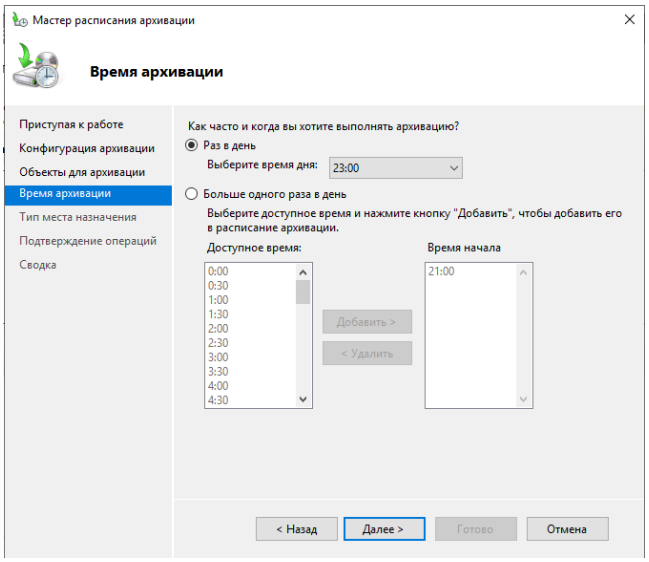
Для настройки и запуска резервного копирования необходимо перейти в "Диспетчере серверов" в "Средства->Система архивации данных Windows Server", далее в открывшемся окне выбирается "Локальная архивация" и в правой части можно настроить расписание архивации, однократную архивацию сейчас выполнить или же восстановление системы.

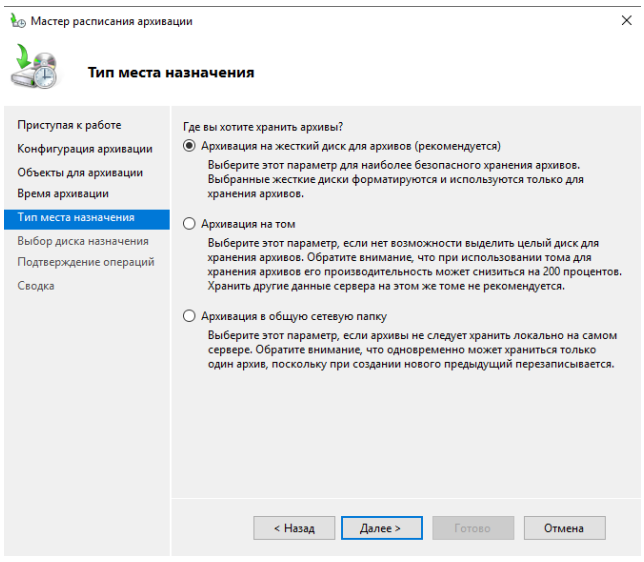
Для создания задания по резервному копированию системного диска в 23:00 производится следующим образом с помощью "Мастера расписания архивации"

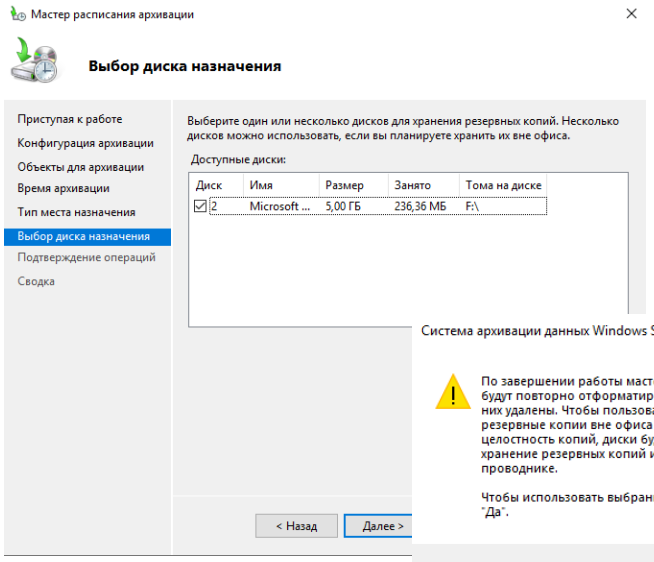
В первом окне выбирается настраиваемая, далее выбираются объекты для архивации, время расписания, тип места хранения архивации, место архивации, после чего мастер предупредит о форматировании конечного тома, куда будет производиться архивация, и выведет итоговое окно.

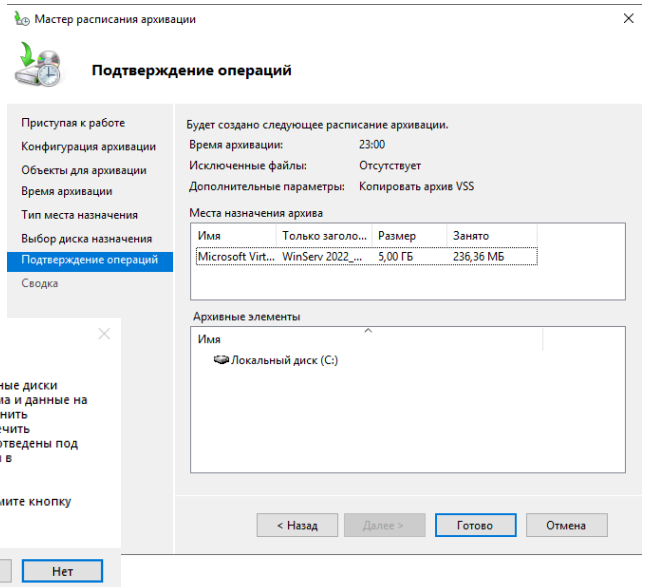


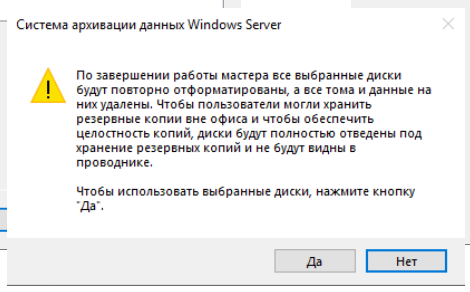




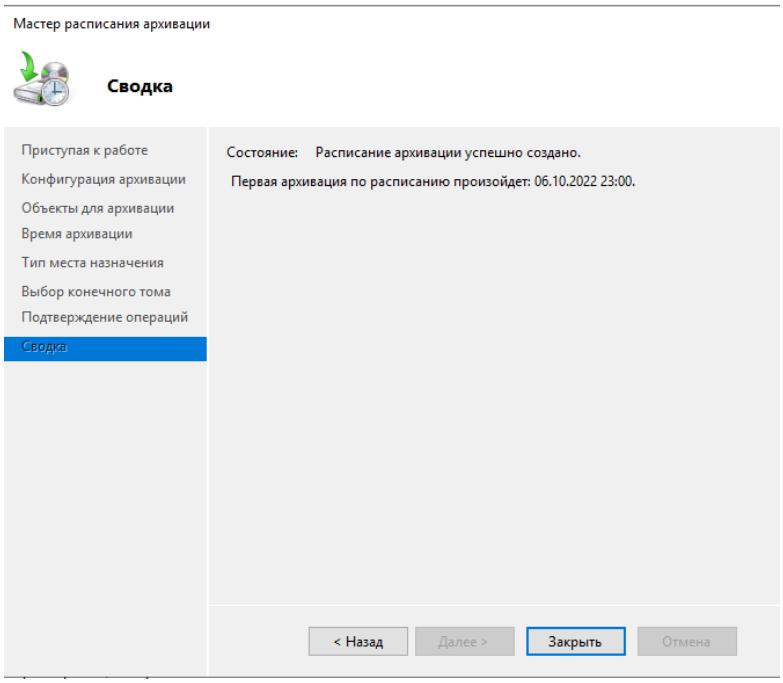


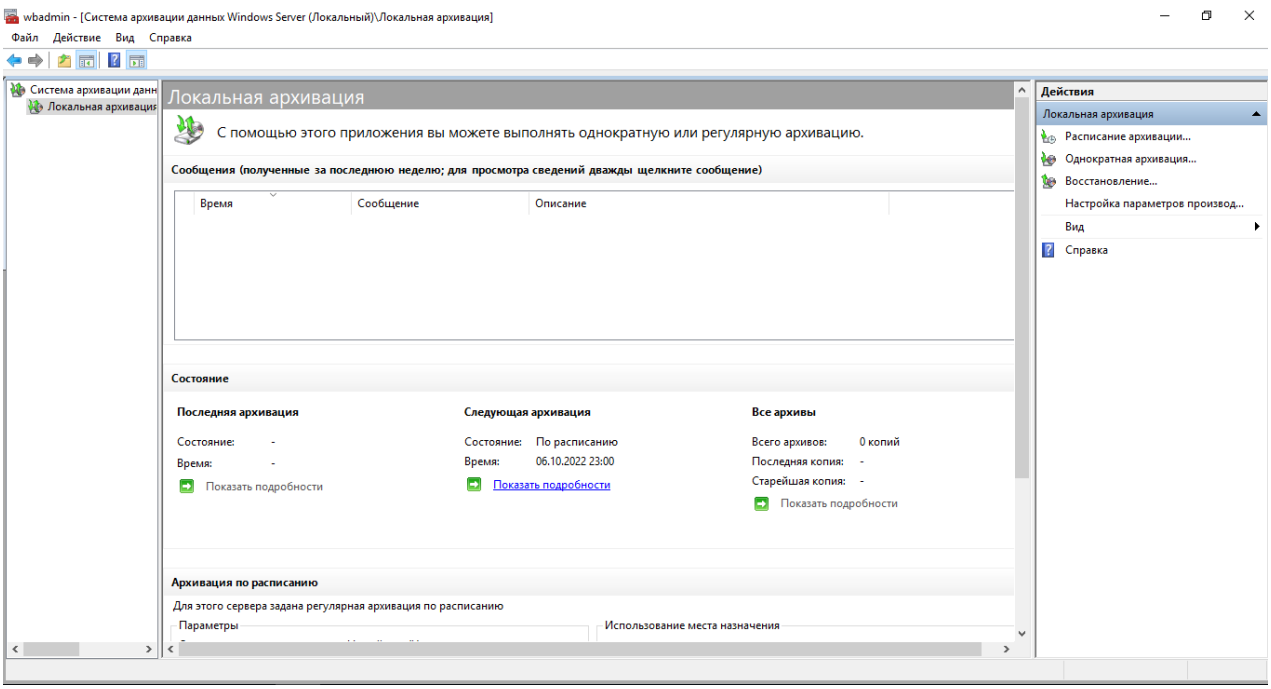




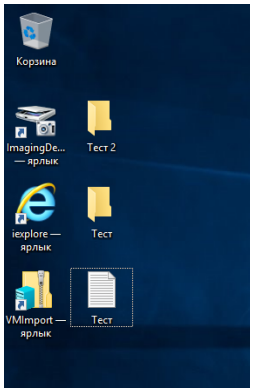


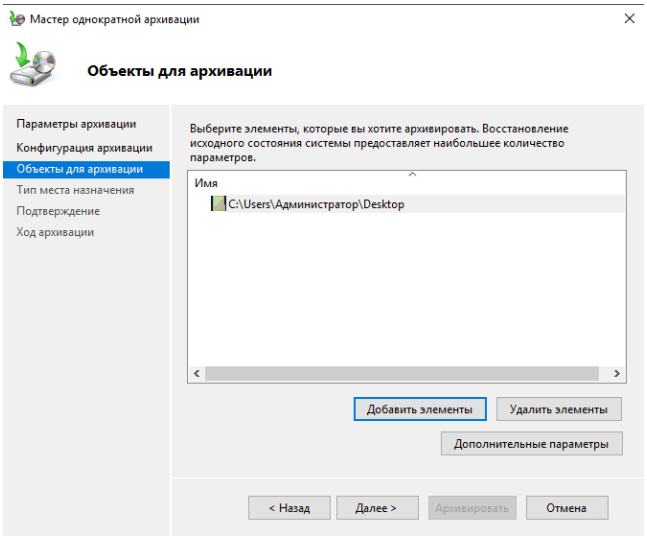
В моём случае сохранение системного диска не было нормально создано в резервное копирование, т.к. места на втором диске меньше, чем занимает сама система. В случае нормальных размеров мастер оповестит о времени первой архивации и успешном создании расписания архивации. Кроме того, в окне локальной архивации будет также отображаться время следующей архивации, количество уже созданных архивов и время предыдущей архивации.

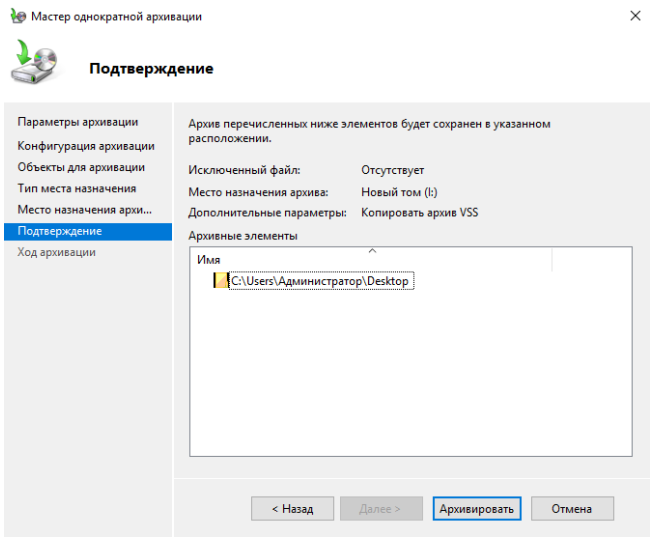




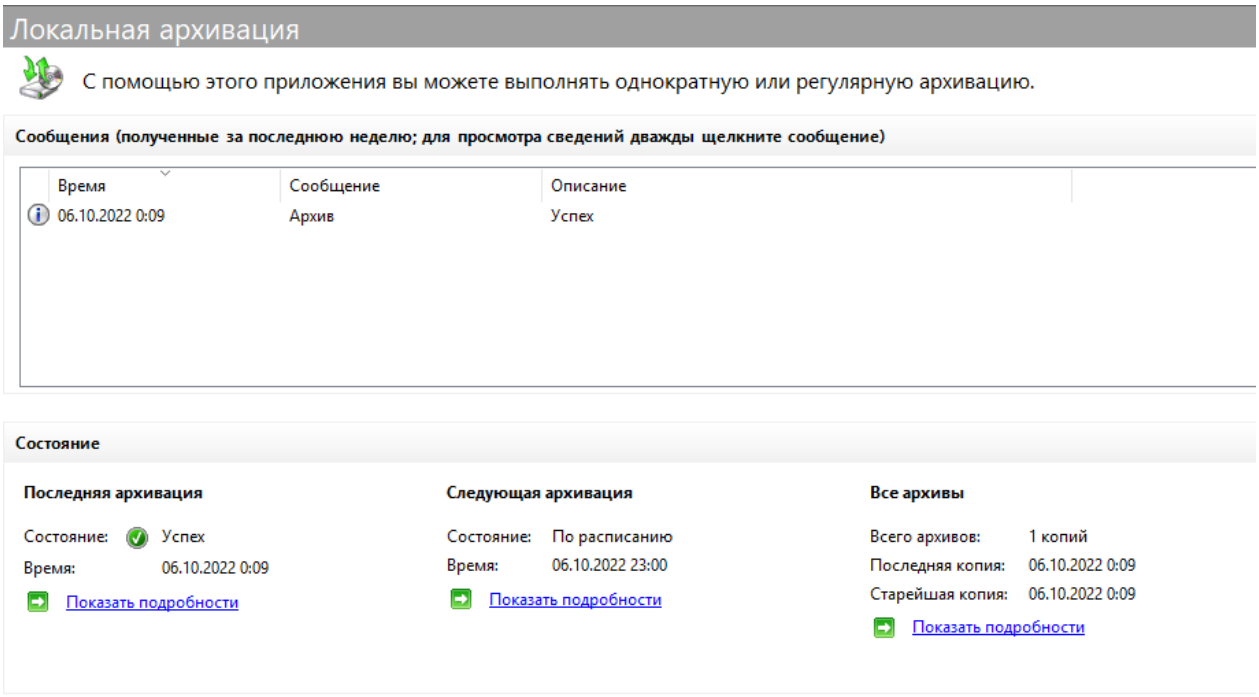
Для следующего задания создам на рабочем столе несколько файлом, директорий. После чего создам "однократной архивацией" резервную копию, только рабочего стола (иначе опять не создаст резерв).



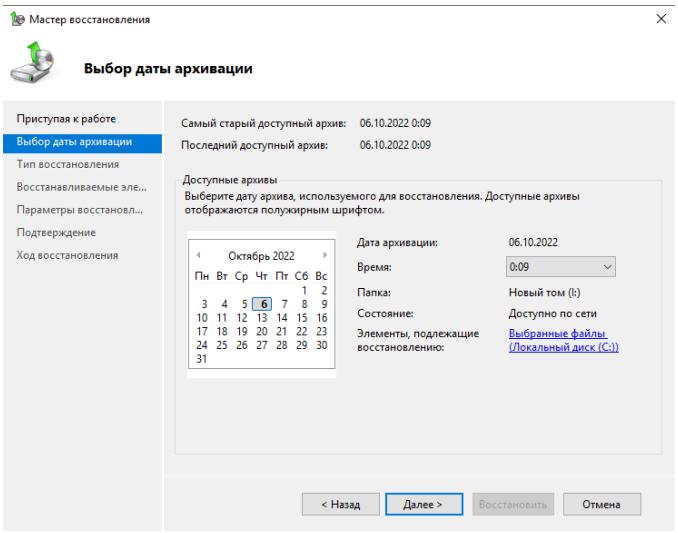


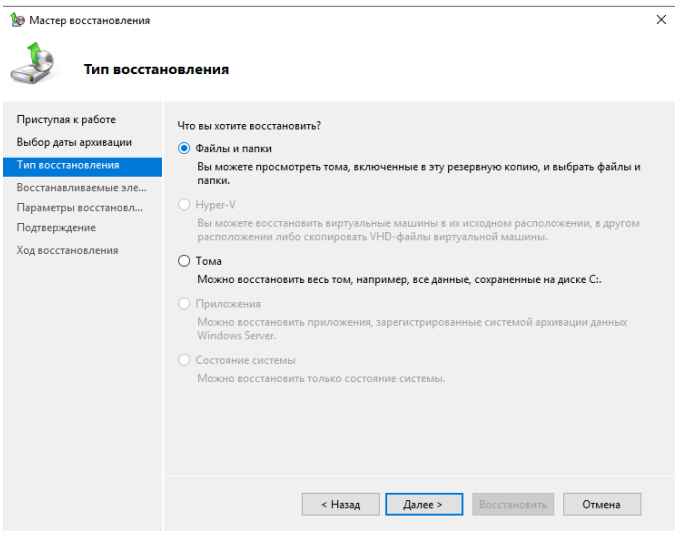


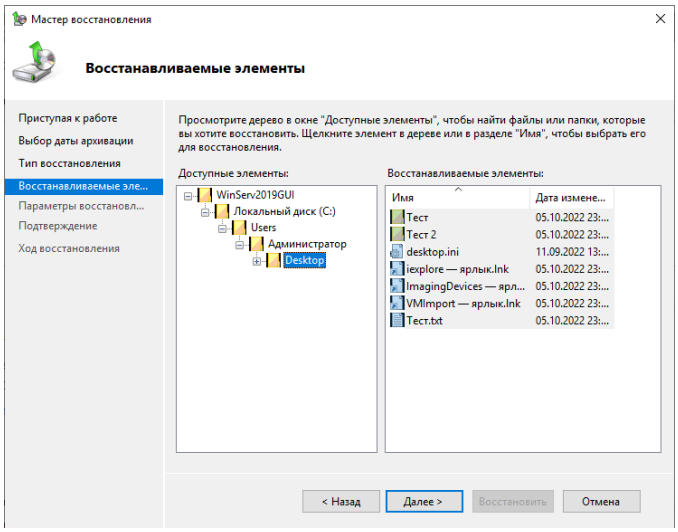
После чего будет создана резервная копия "рабочего стола".

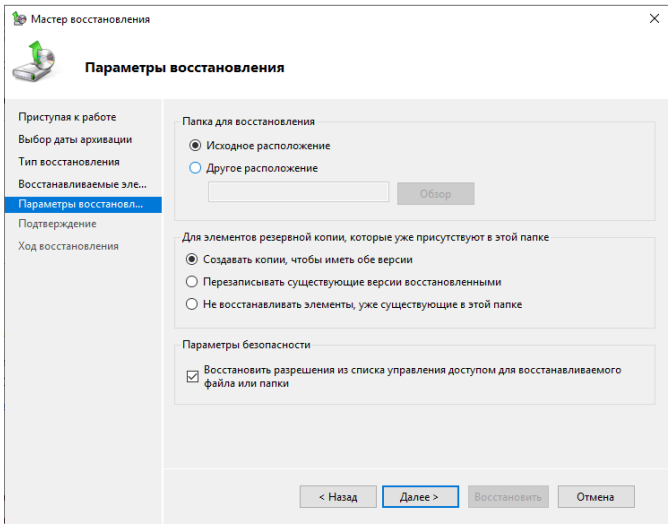


После чего удаляю созданные файлы и ярлыки и из карзины тоже. После чего воспользуюсь восстановлением данных, и собственно "мастером восстановления". Мастер указывает на созданный 5 минут назад архив, его и использовать буду.

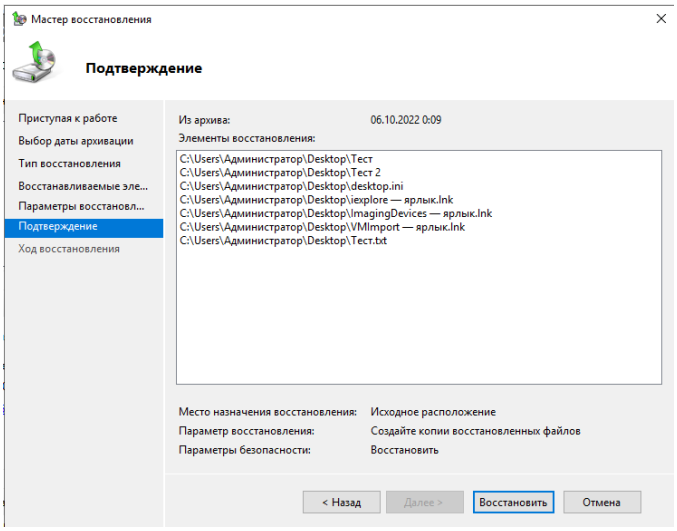


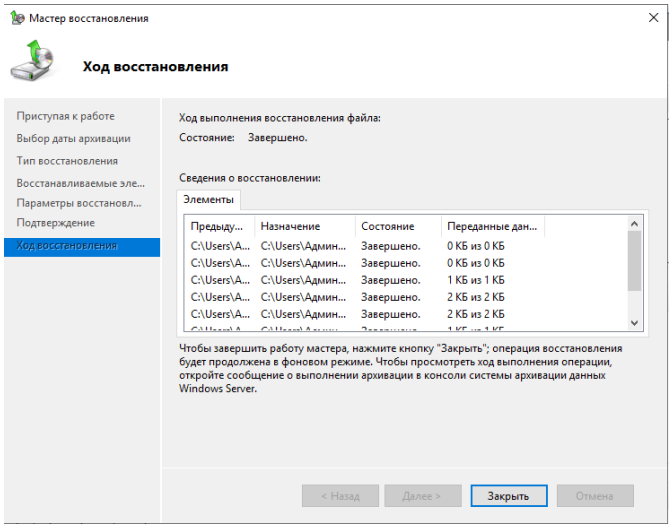




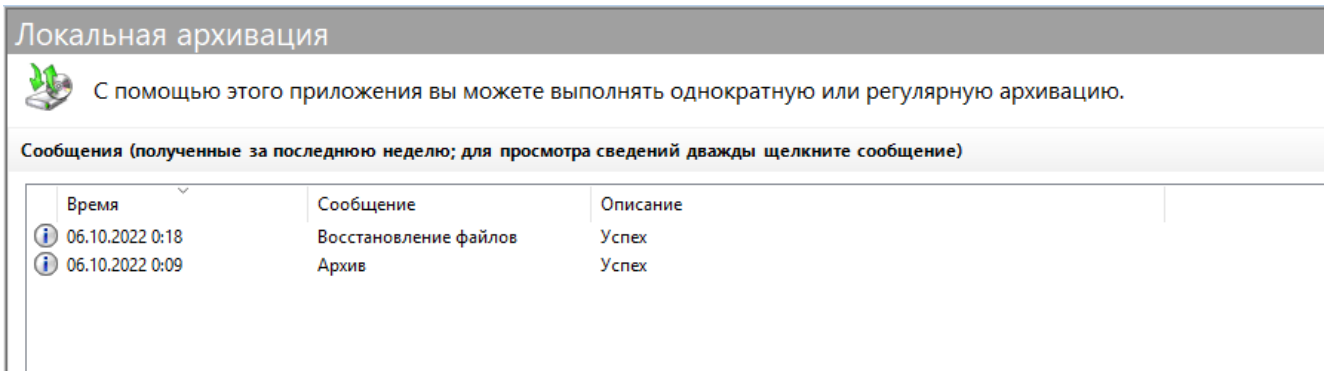


Далее следуя подсказкам мастера, файлы должны вернуться на место.





И в окне "локальной архивации" также будет оповещение об успешном восстановлении из архива.
А на рабочий стол вернуться удалённые данные.



Задание 12-14: Работа с утилитой WBadmin
- Испльзуя утилиту WBadmin создайте резервную копию системы
- Посмотрите, какое количество резервных копий "видит" система
- Удалите самую старую резервную копию.

В PoSh от администратора при вводе команды
wbadmin /?
результатом представит вывод списка поддерживаемых команд

```
PS C:\Users\Администратор> wbadmin /?
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

---- Поддерживаемые команды ----

ENABLE BACKUP          -- создает или изменяет расписание ежедневной архивации.
DISABLE BACKUP          - отключает выполнение архивации по расписанию.
START BACKUP              - запускает выполнение однократной архивации.
STOP JOB                  -- останавливает текущую операцию архивации или
                             восстановления.
GET VERSIONS              – Выводит сведения о резервных копиях, которые
                            можно восстановить из указанного расположения.
GET ITEMS                - отображение списка элементов, содержащихся в архиве.
START RECOVERY            - запускает восстановление.
GET STATUS                - отображение состояния текущей операции.
GET DISKS                 - просмотр списка подключенных к сети дисков.
GET VIRTUALMACHINES       – Вывод списка текущих виртуальных машин Hyper-V.
START SYSTEMSTATERECOVERY - запускает восстановление состояния системы.
START SYSTEMSTATEBACKUP   - запускает создание архива состояния системы.
DELETE SYSTEMSTATEBACKUP  - удаляет один или несколько архивов состояния
                            системы.
DELETE BACKUP             – Удаление одной или нескольких резервных копий.
PS C:\Users\Администратор>
```

Для начала, вводом команды
wbadmin get versions
озадачу PoSh поиском доступных версий резервных копий. При выводе обнаруживается созданная копия "рабочего стола", записанная на диск :I\, так же при выводе указывается время создания архива, что именно можно с помощью него восстановить, где храниться архив и ID образа архива резервного копирования.

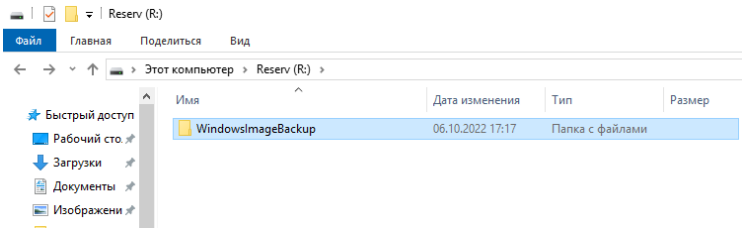
```
PS C:\Users\Администратор> wbadmin get versions
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Время архивации: 06.10.2022 0:09
Конечный объект архивации: Несъемный диск с именем Новый том(I:)
Идентификатор версии: 10/05/2022-21:09
Возможность восстановления: Тома, Файл(ы)
ИД снимка: {fc299d31-6f5a-4aff-be11-ae734f229bf9}

PS C:\Users\Администратор> _
```

Для нормальной попытки резервного копирования, создам ещё один виртуальный жесткий диск **(R:)**, который будет пообъемней подключаемых ранее в предыдущих ДЗ.
Далее командой
wbadmin start backup /?
можно посмотреть, какие дополнительные параметры можно добавить к команде **start backup**
wbadmin start backup -backupTarget:R: -include:C: -allCritical –quiet
Вводом подобной команды будет создан резервный образ диска I: и записан на диск D: , включая все важные тома (**-allCritical**), и игнорируя вывод запросов пользователю при выполнении команды (**-quite**).

```
PS C:\Users\Администратор> wbadmin start backup -backupTarget:R: -include:C: -allCritical -quiet
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Получения сведений о томе...
Будет выполнена архивация (Шифрованный (EFI) системный раздел),Восстановить (499.00 МБ),(C:) на R:.
Начинается архивация на R:.
Создание теневой копии томов, подлежащих архивации...
Создание теневой копии томов, подлежащих архивации...
Создание теневой копии томов, подлежащих архивации...
Создание теневой копии томов, подлежащих архивации...
Создание теневой копии томов, подлежащих архивации...
Создание теневой копии томов, подлежащих архивации...
Выполняется архивация тома (Шифрованный (EFI) системный раздел) (99.00 МБ), (скопировано 0%).
Выполняется архивация тома (Шифрованный (EFI) системный раздел) (99.00 МБ), (скопировано 0%).
Выполняется архивация тома (Шифрованный (EFI) системный раздел) (99.00 МБ), (скопировано 100%).
Сжатие виртуального жесткого диска для тома (Шифрованный (EFI) системный раздел) (99.00 МБ) завершено (0%).
Архивация тома (Шифрованный (EFI) системный раздел) (99.00 МБ) успешно завершена.
Выполняется архивация тома Восстановить (499.00 МБ), (скопировано 50%).
Архивация тома Восстановить (499.00 МБ) успешно завершена.
Выполняется архивация тома (C:), (скопировано 0%).
Выполняется архивация тома (C:), (скопировано 1%).
Выполняется архивация тома (C:), (скопировано 1%).
```

```
Выполняется архивация тома (C:), (скопировано 93%).
Выполняется архивация тома (C:), (скопировано 98%).
Выполняется архивация тома (C:), (скопировано 100%).
Сводка по архивации:
------------------

Архивация успешно завершена.
Архивация тома (Шифрованный (EFI) системный раздел) (99.00 МБ) успешно завершена.
Архивация тома Восстановить (499.00 МБ) успешно завершена.
Архивация тома (C:) успешно завершена.
Список файлов, успешно включенных в архив:
C:\Windows\Logs\WindowsServerBackup\Backup-06-10-2022_14-16-25.log

PS C:\Users\Администратор>
```

Таким образом на диск R: была записана архивная копия с диска C:



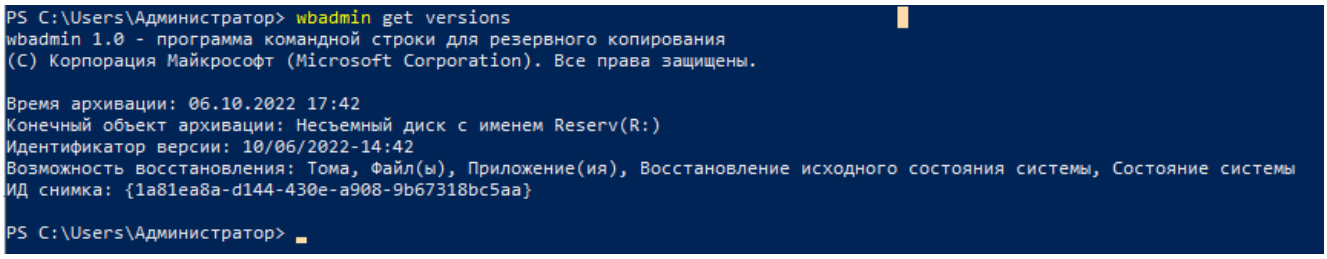
На самом диске, через "проводник" стала доступна директория "WindowsImageBackup", собственно и являющейся архивом образа.
Снова проверю
wbadmin get versions
появилась вторая версия архива резерва.

```
PS C:\Users\Администратор> wbadmin get versions
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Время архивации: 06.10.2022 0:09
Конечный объект архивации: Несъемный диск с именем Новый том(I:)
Идентификатор версии: 10/05/2022-21:09
Возможность восстановления: Тома, Файл(ы)
ИД снимка: {fc299d31-6f5a-4aff-be11-ae734f229bf9}

Время архивации: 06.10.2022 17:16
Конечный объект архивации: Несъемный диск с именем Reserv(R:)
Идентификатор версии: 10/06/2022-14:16
Возможность восстановления: Тома, Файл(ы), Приложение(ия), Восстановление исходного состояния системы, Состояние системы
ИД снимка: {ace829bc-97b1-4cf3-8164-2a2615a4e8c1}

PS C:\Users\Администратор>
```

Для удаления самой старой версии резервного копирования вводится команда
wbadmin delete backup –backupTarget:R: –deleteOldest -quiet
Для удаления резервных копий, кроме определённого количества последних
wbadmin delete backup -keepversions:2
в данном варианте удаляются все копии, кроме последних двух, в случае указания **-keepversions:0** - удаляются все резервные копии.
В моём случае, что диск I:, что диск R: имеют по одной резервной копии. Создам вторую копию на диск R:, после чего удалю все резервные копии, оставив только одну.
wbadmin delete backup -keepversions:1

```
PS C:\Users\Администратор> wbadmin delete backup -keepversions:1
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Идет перечисление резервных копий...
Обнаружено резервных копий: 3,
останется после операции удаления: 1.
Вы хотите удалить резервные копии?
[Y] – да; [N] – нет y

Удаление версии 10/05/2022-21:09 резервной копии (1 из 2)...
Сбой удаления версии 10/05/2022-21:09 резервной копии.
Ошибка: Указан недопустимый тип носителя.
.
Вы хотите удалить запись архивации из каталога?
(При этом место в расположении хранения не освобождается.)
[Y] – да; [N] – нет y

Удаление версии 10/06/2022-14:16 резервной копии (2 из 2)...
Удаление резервных копий завершено.
Удалено резервных копий: 2
PS C:\Users\Администратор>
```

Далее снова посмотрю количество доступных версий резервного копирования
wbadmin get versions



Осталась одна копия резервного копирования. Аналогично, думаю, сработало бы и с вариантом
wbadmin delete backup –backupTarget:R: –deleteOldest -quiet
За исключением того, что осталась бы резервная копия на диске I: , тут мой промах, не учёл и не добавил таргет в синтаксис с указанием локации работы команды **–backupTarget:R:**