

16.02.2024

Курс:

Практическая работа к уроку № Lesson_9

--

Аудит безопасности Windows

Задание:

1. Включите все доступные профили брандмауэра Защитника Windows
2. Создайте исходящее правило для Internet Explorer
3. Создайте входящее правило для Internet Explorer
4. Экспотрируйте настройки брандмауэра Защитника Windows
5. Через локальные политики безопасности запретите запуск Internet Explorer
6. Включите установку обновлений для Windows и других продуктов Microsoft
7. Включите Аудит событий входа успех\отказ
8. Установите компонент «Система архивации данных Windows Server»
9. Создайте задачу ежедневного резервного копирования системного диска в 23.00
10. Удалите файлы с рабочего стола, затем восстановите их из резервной копии
11. Восстановите состояние сервера используя загрузочный диск и ранее созданную резервную копию
12. Используя утилиту WBadmin создайте резервную копию системы
13. Посмотрите, какое количество резервных копий "видит" система
14. Удалите самую старую резервную копию.

Serv1: win2019serv01 (gui)

Параметры сетевого адаптера	
Индекс адаптера	1
Описание	Intel(R) PRO/1000 MT Desktop Adapter
IP-адрес	192.168.56.16 fe80::f814:7e3c:885d:9286
Маска подсети	255.255.255.0
DHCP включен	Ложь
Шлюз по умолчанию	192.168.56.4
Основной DNS-сервер	192.168.56.1
Альтернативный DNS-сервер	8.8.8.8

Задание_1:

Включите все доступные профили брандмауэра Защитника Windows

Брандмауэр Защитника Windows

← → ⌂ ⌃ ⌄ << Все элементы панели ... > Брандмауэр Защитника Windows ⌅ ⌋ Помощь в панели управления ⌋

Панель управления —
домашняя страница

Разрешение взаимодействия
с приложением или
компонентом в брандмауэре
Защитника Windows

Изменение параметров
уведомлений

Включение и отключение
брандмауэра Защитника
Windows

Восстановить значения по
умолчанию

Дополнительные параметры

Устранение неполадок в сети

Задайте свой компьютер с помощью брандмауэра Защитника Windows

Брандмауэр Защитника Windows помогает защитить компьютер от злоумышленников или вредоносных программ в Интернете или локальной сети.

	Доменные сети	Подключено
Сети на рабочем месте, подключенные к домену		
Состояние Брандмауэр Защитника Windows:		Вкл.
Входящие подключения:		Блокировать подключения к приложениям, которых нет в списке разрешенных программ
Активные доменные сети:		domain.local01
Состояние уведомления:		Не уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение
	Частные сети	Не подключено
	Гостевые или общедоступные сети	Не подключено

См. также

Центр безопасности и
обслуживания

Центр управления сетями и
общим доступом

The screenshot shows the Windows Registry Editor window. The title bar reads "Редактор реестра" (Registry Editor). The menu bar includes "Файл", "Правка", "Выход", "Избранное", and "Справка". The address bar displays the path "Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History". The left pane shows a tree view of registry keys, with "History" selected. The right pane displays a table of registry entries:

	Имя	Тип	Значение
ab	(По умолчанию)	REG_SZ	(значение не присвоено)
hi	CurrentWaitAtSt...	REG_DWORD	0xffffffff (4294967295)
ab	DCName	REG_SZ	\w2019serv01.domain.local01
hi	IsSlowLink	REG_DWORD	0x00000000 (0)
ab	MachineDomain	REG_SZ	domain.local01
ab	NetworkName	REG_SZ	
hi	PolicyOverdue	REG_DWORD	0x00000000 (0)

The entry "MachineDomain" is highlighted with a red box.



Настройка параметров для каждого типа сети

Вы можете изменить параметры брандмауэра для каждого из используемых типов сетей.

Параметры доменной сети



Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение



Отключить брандмауэр Защитника Windows (не рекомендуется)

Параметры для частной сети



Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение



Отключить брандмауэр Защитника Windows (не рекомендуется)

Параметры для общественной сети



Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение



Отключить брандмауэр Защитника Windows (не рекомендуется)



Настройка параметров для каждого типа сети

Вы можете изменить параметры брандмауэра для каждого из используемых типов сетей.

Параметры доменной сети

Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение

Отключить брандмауэр Защитника Windows (не рекомендуется)

Параметры для частной сети

Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение

Отключить брандмауэр Защитника Windows (не рекомендуется)

Параметры для общественной сети

Включить брандмауэр Защитника Windows

Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ

Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение

Отключить брандмауэр Защитника Windows (не рекомендуется)

The screenshot shows the Windows Firewall Monitor window. The title bar reads "Монитор брандмауэра Защитника Windows в режиме повышенной безопасности включен Локал...". The menu bar includes "Файл", "Действие", "Вид", and "Справка". The toolbar has icons for back, forward, search, and refresh. The left sidebar has a tree view with "Правила для входящих подключений", "Правила для исходящего подключения", "Правила безопасности по сети", and "Наблюдение". The main pane displays the following sections:

- Обзор**
 - Профиль домена активен**
 - Брандмауэр Защитника Windows включен.
 - Входящие подключения, не соответствующие ни одному правилу, запрещены.
 - Исходящие подключения, не соответствующие ни одному правилу, разрешены.
 - Частный профиль**
 - Брандмауэр Защитника Windows включен.
 - Входящие подключения, не соответствующие ни одному правилу, запрещены.
 - Исходящие подключения, не соответствующие ни одному правилу, разрешены.
 - Общий профиль**
 - Брандмауэр Защитника Windows включен.
 - Входящие подключения, не соответствующие ни одному правилу, запрещены.
 - Исходящие подключения, не соответствующие ни одному правилу, разрешены.
- Приступая к работе**
 - Проверка подлинности при передаче данных между компьютерами**

Создайте правила безопасности подключения, чтобы указать, как и когда выполняется проверка

The right sidebar lists "Действия" with options: "Монитор брандмауэра Защитника Wi...", "Импортируйте политику...", "Экспорт политики...", "Восстановить политику по умолчанию", "Диагностика / восстановление", "Вид", "Обновить", "Свойства", and "Справка". A status bar at the bottom right says "Активация Windows" and "Чтобы активировать Windows, перейдите в раздел 'Параметры'.".

Монитор брандмауэра Защитника Windows в режиме повышенной безопасности

Файл Действие Вид Справка

Монитор брандмауэра Защищенный

- Правила для входящих портов
- Правила для исходящего трафика
- Правила безопасности портов
- Брандмаузер**
- Правила безопасности
- Сопоставления безопасности

Действия

Брандмаузер

- Вид
- Обновить
- Экспортировать список...
- Справка

Имя	Профиль	Действие	Частота	Направление
DHCP-сервер - Удаленное управление ...	Все	Разрешить	Нет	Входящие
DHCP-сервер (RPCSS-входящий)	Все	Разрешить	Нет	Входящие
DHCP-сервер (RPC-входящий)	Все	Разрешить	Нет	Входящие
DHCP-сервер (SMB — входящий трафик)	Все	Разрешить	Нет	Входящие
DHCP-сервер v4 (UDP-входящий)	Все	Разрешить	Нет	Входящие
DHCP-сервер v4 (UDP-входящий)	Все	Разрешить	Нет	Входящие
DHCP-сервер v6 (UDP-входящий)	Все	Разрешить	Нет	Входящие
DHCP-сервер v6 (UDP-входящий)	Все	Разрешить	Нет	Входящие
DNS (TCP, входящие)	Все	Разрешить	Нет	Входящие
DNS (UDP-In)	Домен	Разрешить	Нет	Входящие
RPC (TCP, входящие)	Все	Разрешить	Нет	Входящие
RPC Endpoint Mapper (TCP, входящие)	Все	Разрешить	Нет	Входящие
SmBindOpenException	Все	Разрешить	Нет	Входящие
Безопасность Windows	Домен, Ч...	Разрешить	Нет	Входящие
Безопасность Windows	Домен, Ч...	Разрешить	Нет	Входящие
Ваша учетная запись	Домен, Ч...	Разрешить	Нет	Входящие
Ваша учетная запись	Домен, Ч...	Разрешить	Нет	Входящие
Веб-службы Active Directory (TCP - вх...	Все	Разрешить	Нет	Входящие
Веб-средство просмотра классических...	Все	Разрешить	Нет	Входящие
Веб-средство просмотра классических...	Все	Разрешить	Нет	Входящие
Инструментарий управления Windows ...	Все	Разрешить	Нет	Входящие

Задание_2:

- Создайте исходящее правило для Internet Explorer
- Создайте входящее правило для Internet Explorer

Internet Explorer

Файл Главная Поделиться Вид

Program Files (x86) > Internet Explorer

Файл Главная Поделиться Вид

Локальный диск (C:) > Program Files > internet explorer

Имя	Дата изменения	Тип	Имя	Дата изменения	Тип
Быстрый доступ	15.09.2018 19:43	Папка с файлами	Быстрый доступ	15.09.2018 19:43	Папка с файлами
Рабочий стол	15.09.2018 10:19	Папка с файлами	Рабочий стол	15.09.2018 10:19	Папка с файлами
Загрузки	15.09.2018 19:44	Папка с файлами	Загрузки	15.09.2018 19:44	Папка с файлами
Документы	11.02.2024 14:14	Папка с файлами	Документы	09.02.2024 16:26	Папка с файлами
Изображения	15.09.2018 10:13	Приложение	Изображения	15.09.2018 10:12	Приложение
System32	15.09.2018 10:13	Расширение г...	System32	15.09.2018 10:12	Расширение при...
Локальный диск (C:			Локальный диск (C:		
Этот компьютер			Этот компьютер		
Сеть			Сеть		
ie9props.propdesc	15.09.2018 10:13	Файл "PROPD1	ie9props.propdesc	09.02.2024 16:12	Приложение
ieinstal	15.09.2018 10:13	Приложение	ieinstal	15.09.2018 10:12	Приложение
ielowutil	15.09.2018 10:13	Приложение	ielowutil	15.09.2018 10:12	Приложение
IEShims.dll	09.02.2024 16:14	Расширение г...	IEShims.dll	09.02.2024 16:12	Расширение при...
explorer	09.02.2024 16:15	Приложение	explorer	09.02.2024 16:15	Приложение
sqmapi.dll	15.09.2018 10:13	Расширение г...	sqmapi.dll	15.09.2018 10:12	Расширение при...

https://ya.ru/

Яндекс

Поиск...

Войти



найдётся всё

Internet Explorer

Войти

Содержимое указанного ниже веб-сайта блокируется конфигурацией усиленной безопасности Internet Explorer.

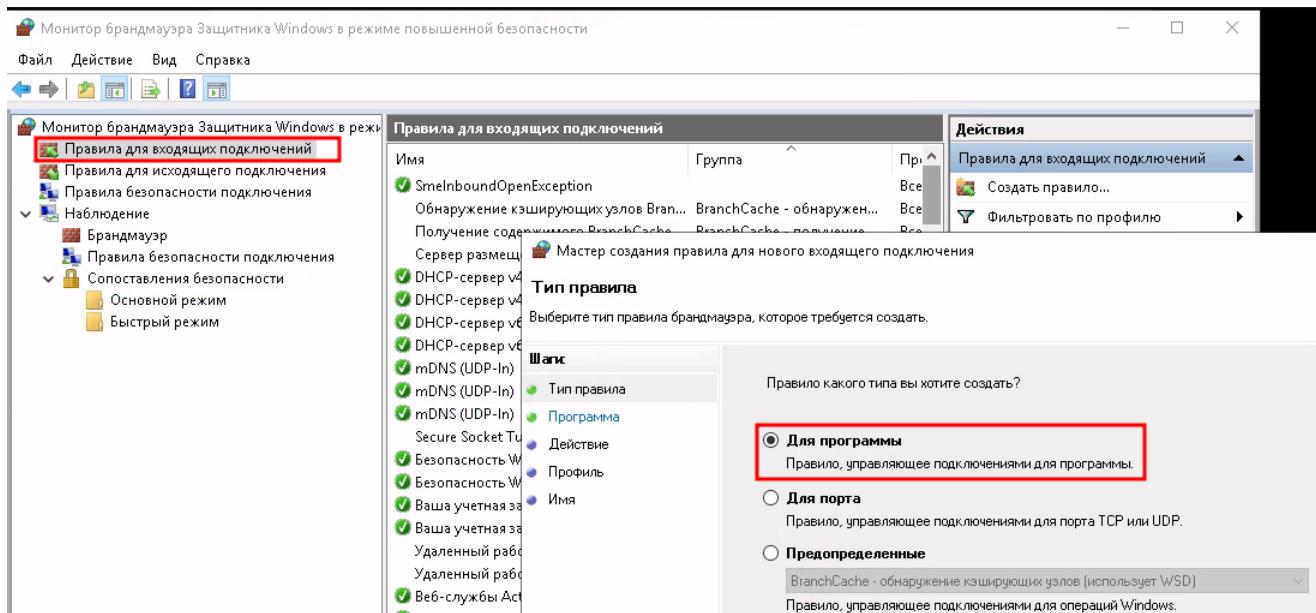
<https://yandex.ru>

Сообщать о блокировке содержимого веб-сайта

[Подробнее о конфигурации усиленной безопасности Internet Explorer...](#)

Если вы доверяете этому веб-сайту, к нему можно понизить требования безопасности, добавив его в зону надежных сайтов. Если этот веб-сайт принадлежит

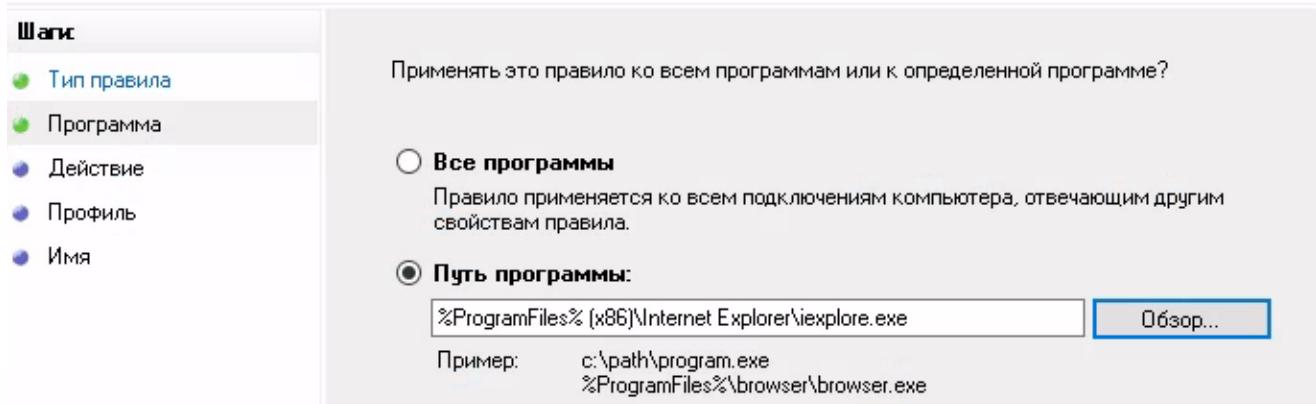
Добавить...



Мастер создания правила для нового входящего подключения

Программа

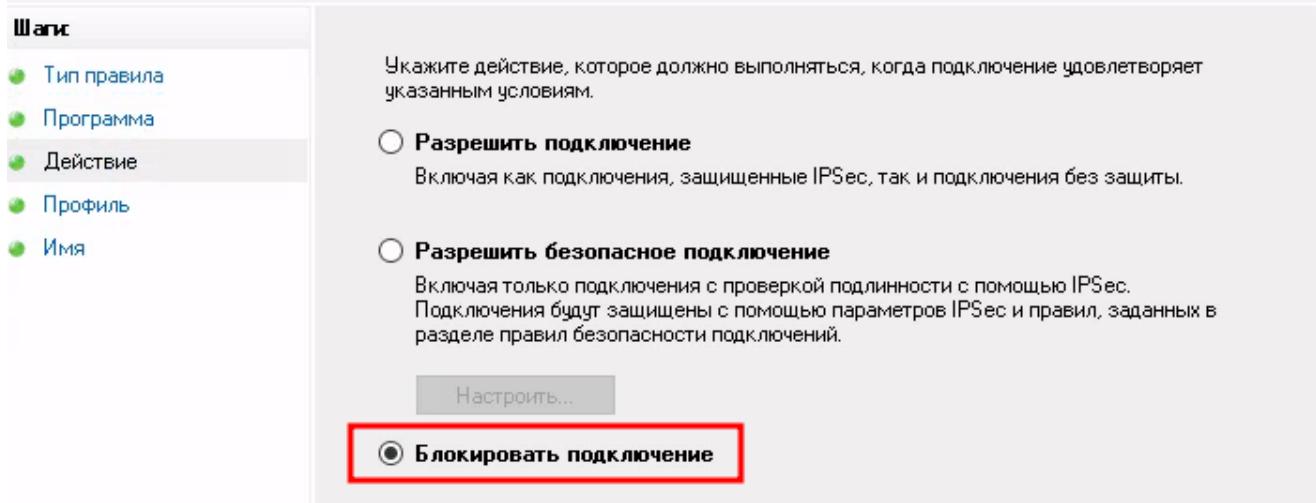
Укажите полный путь и имя исполняемого файла программы, которой соответствует данное правило.



Мастер создания правила для нового входящего подключения

Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.



Мастер создания правила для нового входящего подключения

Профиль

Укажите профили, к которым применяется это правило.

Шаги

Тип правила

Программа

Действие

Профиль

Имя

Для каких профилей применяется правило?

Доменный

Применяется при подключении компьютера к домену своей организации.

Частный

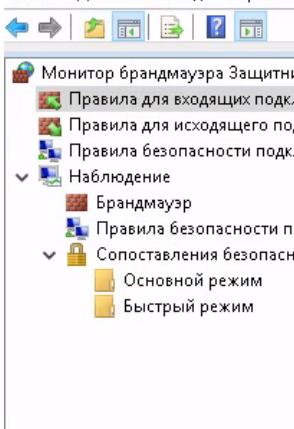
Применяется, когда компьютер подключен к частной сети, например дома или на работе.

Публичный

Применяется при подключении компьютера к общественной сети.

Монитор брандмауэра Защитника Windows в режиме повышенной безопасности

Файл Действие Вид Справка



Мастер создания правила для нового входящего подключения

Имя

Укажите имя и описание данного правила.

Шаги

Тип правила

Программа

Действие

Профиль

Имя

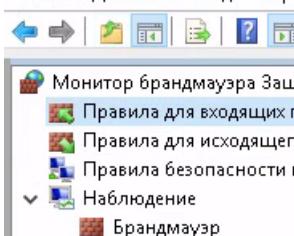
Имя:

Blocking 32x Iexplorer

Описание (необязательно):

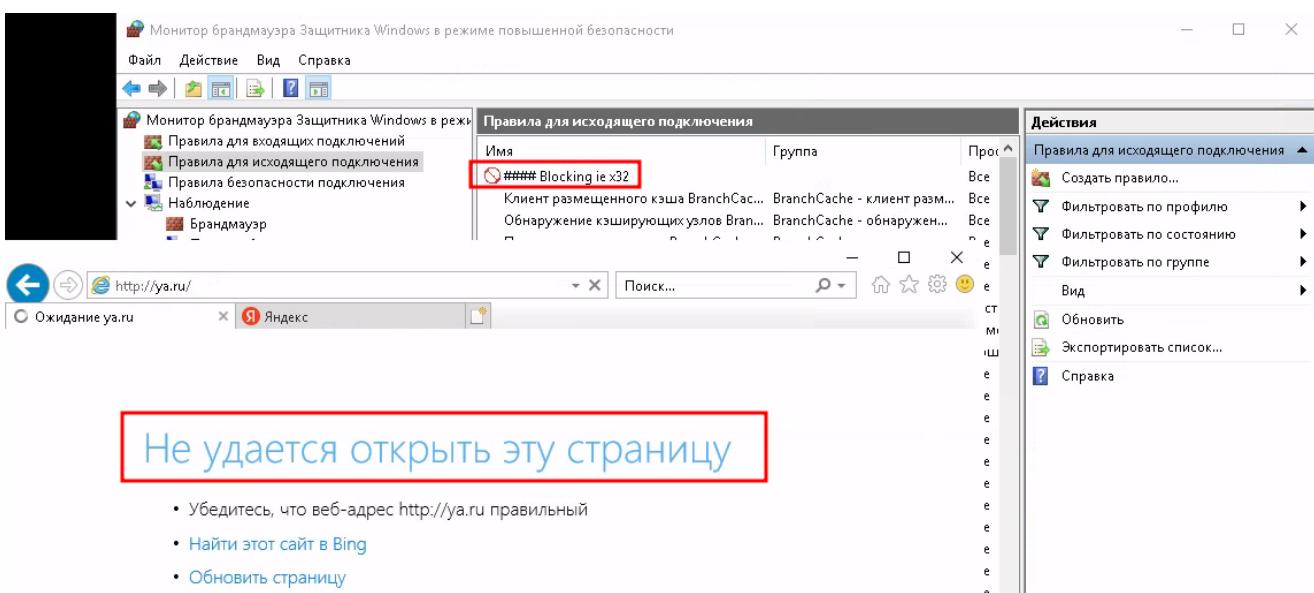
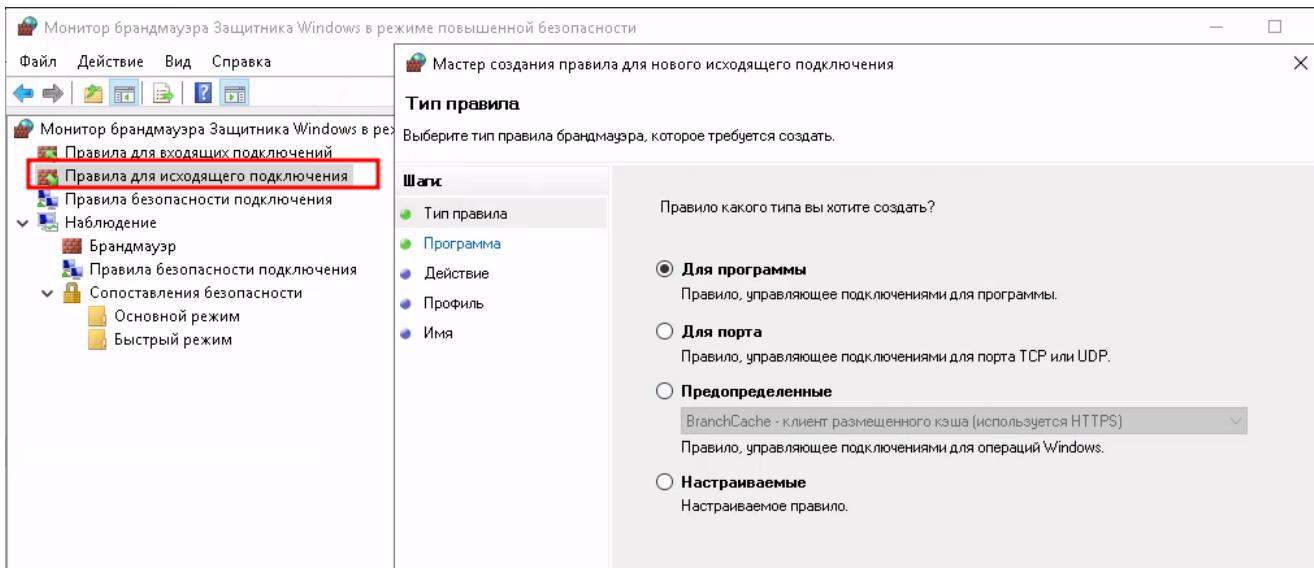
Монитор брандмауэра Защитника Windows в режиме повышенной безопасности

Файл Действие Вид Справка



Правила для входящих подключений

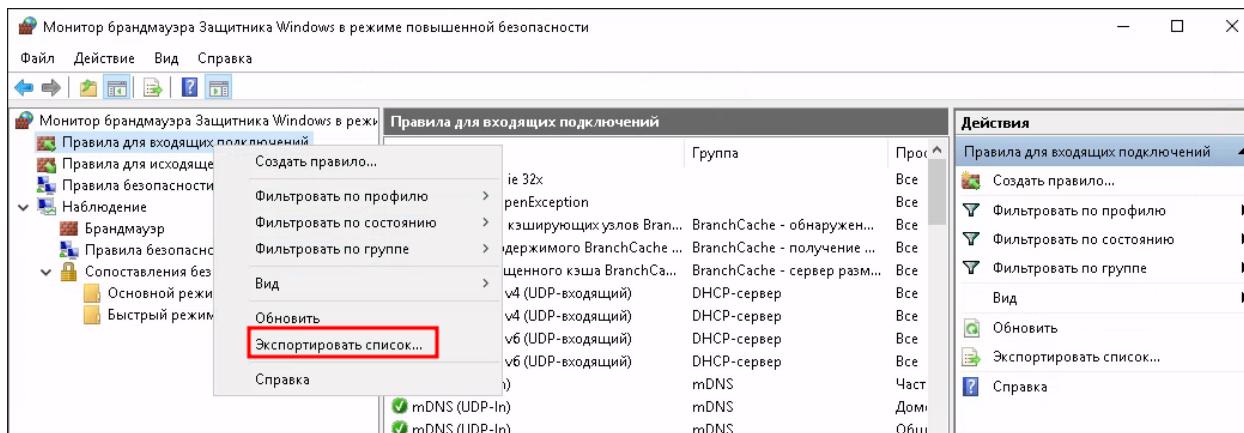
Имя	Группа	Примечание
##### Blocking 32x Iexplorer	Все	
SmelnhboundOpenException	Все	Обнаружение кэширующих узлов BranchCache - обнаружен...

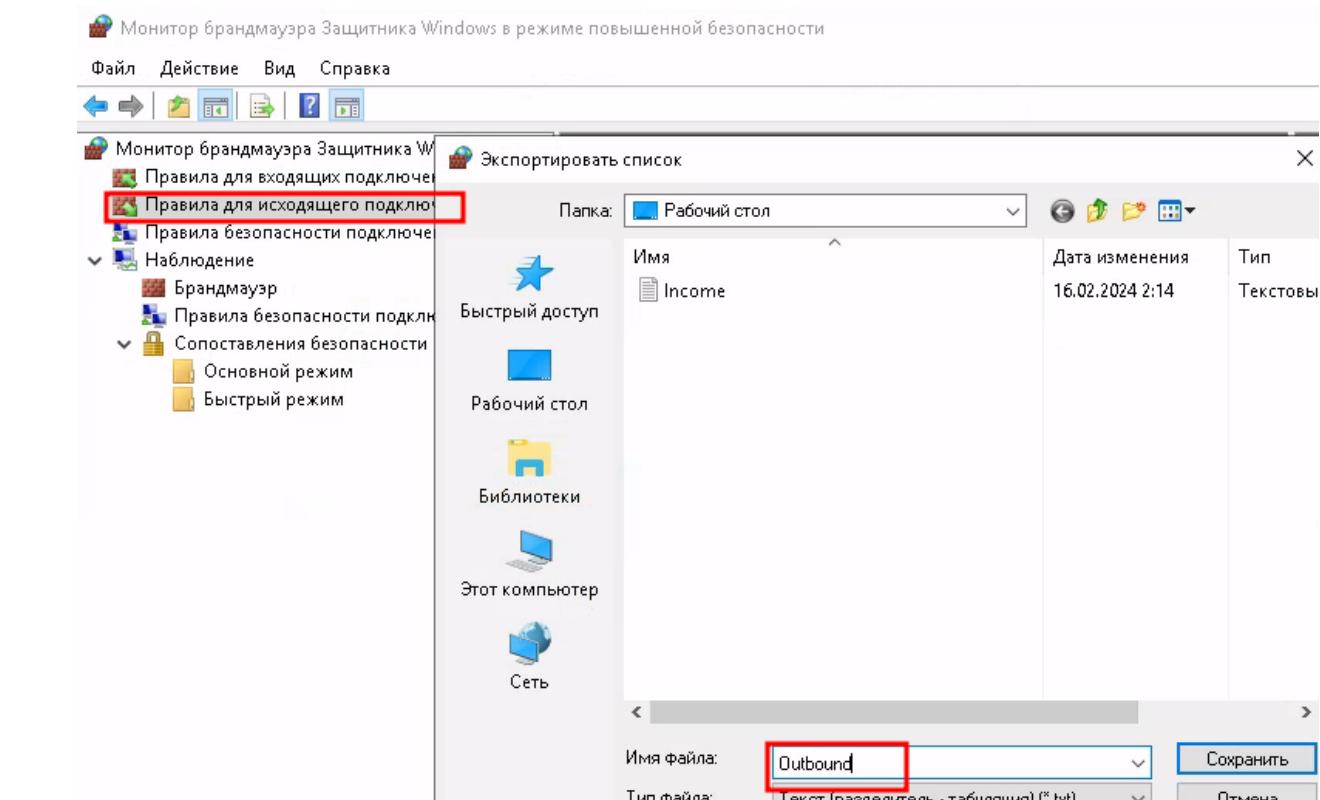


Задание_3:

Экспотрируйте настройки брандмауэра Защитника Windows

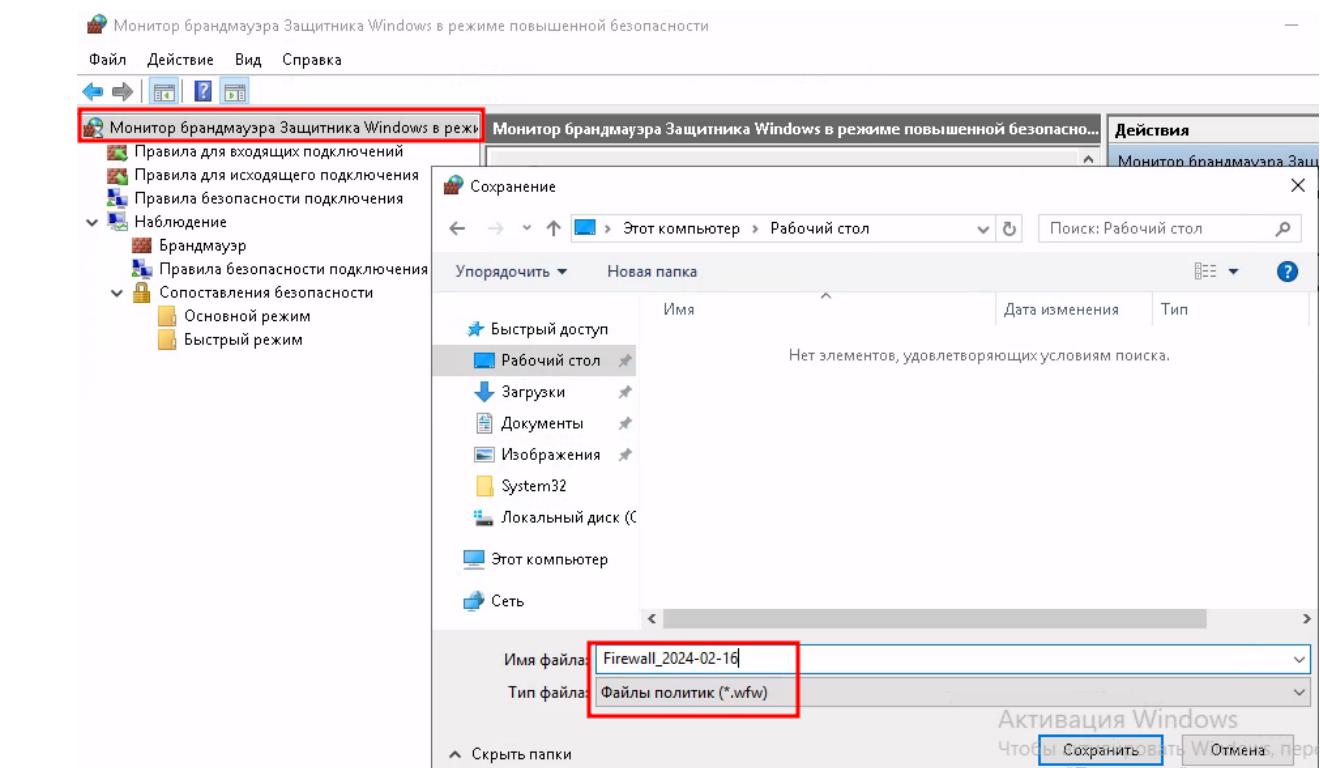
- txt File





Имя	Группа	Профиль	Включено	Действие	Частота	Программа	Локальный адрес	Удаленный адрес	Протокол	Локальный порт	Удай
##### Blocking ie 32x		Все	Да	Блокировать	Нет	%ProgramFiles% (x86)\Internet Explorer\iexplore.exe	Любой	Любой	Люб:	Любой	Люб:
Smb1boundOpenException		Все	Да	Разрешить	Нет	Любой	Любой	Любой	Люб:	Любой	Люб:
Обнаружение каширующих узлов BranchCache (входящий трафик WSD)						BranchCache - обнаружение каширующих узлов (использует WSD)	BranchCache - обнаружение каширующих узлов (использует WSD)	Все	Нет	Разр:	
Получение содержимого BranchCache (входящий трафик HTTP)						BranchCache - получение содержимого (использует HTTP)	BranchCache - получение содержимого (использует HTTP)	Все	Нет	Разр:	
Сервер размещенного кеша BranchCache (входящий трафик HTTP)						BranchCache - сервер размещенного кеша (используется HTTPS)	BranchCache - сервер размещенного кеша (используется HTTPS)	Все	Нет	Разр:	
DHCP-сервер v4 (UDP-входящий)	DHCP-сервер	Все	Да	Разрешить	Нет	%systemroot%\system32\svchost.exe	Любой	Любой	Люб:	Любой	Люб:
DHCP-сервер v4 (UDP-входящий)	DHCP-сервер	Все	Да	Разрешить	Нет	%systemroot%\system32\svchost.exe	Любой	Любой	Люб:	Любой	Люб:
DHCP-сервер v6 (UDP-входящий)	DHCP-сервер	Все	Да	Разрешить	Нет	%systemroot%\system32\svchost.exe	Любой	Любой	Люб:	Любой	Люб:
DHCP-сервер v6 (UDP-входящий)	DHCP-сервер	Все	Да	Разрешить	Нет	%systemroot%\system32\svchost.exe	Любой	Любой	Люб:	Любой	Люб:
mDNS (UDP-In)	mDNS	Частный	Да	Разрешить	Нет	%SystemRoot%\system32\svchost.exe	Любой	Локальная подсеть	UDP	535:	
mDNS (UDP-In)	mDNS	Домен	Да	Разрешить	Нет	%SystemRoot%\system32\svchost.exe	Любой	Люб:	UDP	535:	
mDNS (UDP-In)	mDNS	Общий	Да	Разрешить	Нет	%SystemRoot%\system32\svchost.exe	Любой	Локальная подсеть	UDP	535:	

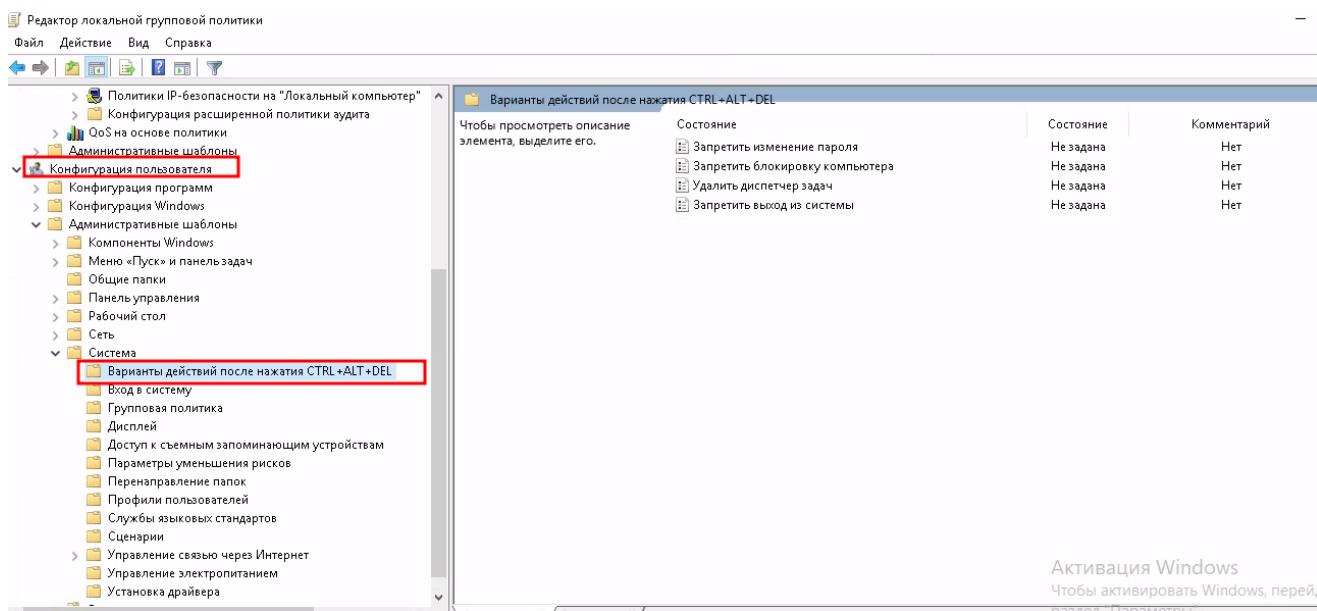
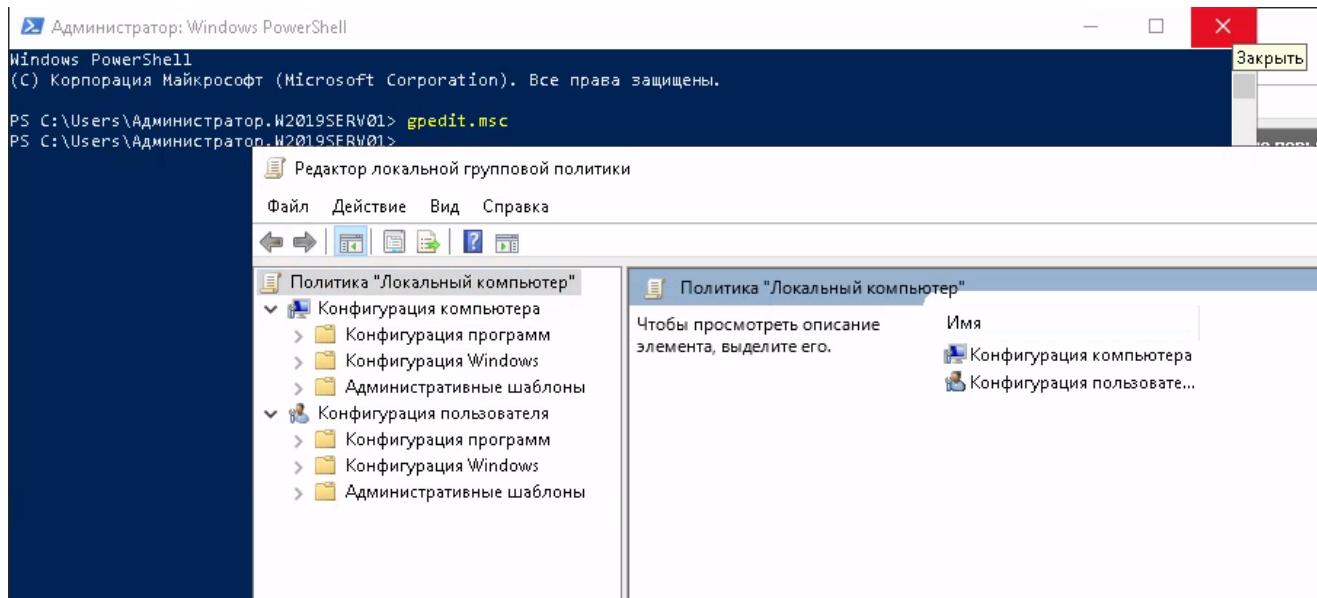
• wfw File



Задание_4

Через локальные политики безопасности запретите запуск Internet Explorer

```
gpedit.msc  
gpupdate /force
```



Редактор локальной групповой политики

Файл Действие Вид Справка

Система

Чтобы просмотреть описание элемента, выделите его.

	Состояние	Комментарий
Варианты действий после нажатия CTRL+ALT+DEL	Не задана	Нет
Вход в систему	Не задана	Нет
Групповая политика	Не задана	Нет
Дисплей	Не задана	Нет
Доступ к съемным запоминающим устройствам	Не задана	Нет
Параметры уменьшения рисков	Не задана	Нет
Перенаправление папок	Не задана	Нет
Профили пользователей	Не задана	Нет
Службы языковых стандартов	Не задана	Нет
Сценарии	Не задана	Нет
Управление связью через Интернет	Не задана	Нет
Управление электропитанием	Не задана	Нет
Установка драйвера	Не задана	Нет
Загрузка отсутствующих компонентов модели COM	Не задана	Нет
Интерпретация столетия для 2000 года	Не задана	Нет
Запретить запуск из справки перечисленных программ	Не задана	Нет
Не показывать экран приветствия «Приступая к работе...»	Не задана	Нет
Настраиваемый интерфейс пользователя	Не задана	Нет
Запретить использование командной строки	Не задана	Нет
Запретить доступ к средствам редактирования реестра	Не задана	Нет
Не запускать указанные приложения Windows	Включено	Нет
Выполнять только указанные приложения Windows	Не задана	Нет
Автоматическое обновление Windows	Не задана	Нет

Активизация Windows

Чтобы активировать Windows, перейди

локальной групповой политики

Свойства

Не запускать указанные приложения Windows

Комментарий:

Включено

Требования к версии:

Не ниже Windows 2000

Параметры:

Список запрещенных приложений Показать...

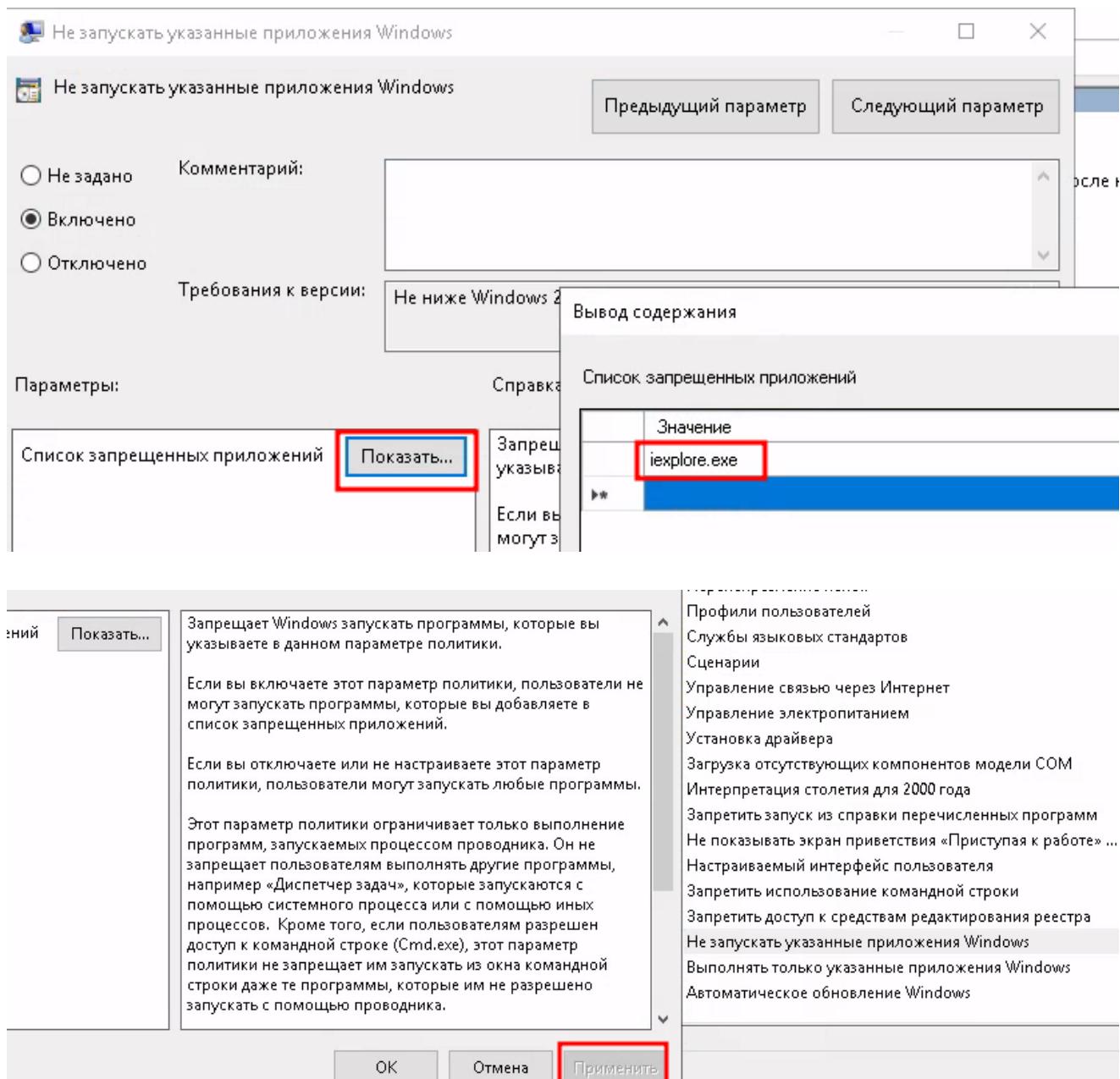
Справка:

Запрещает Windows запускать программы, которые вы указываете в данном параметре политики.

Если вы включаете этот параметр политики, пользователи не могут запускать программы, которые вы добавляете в список запрещенных приложений.

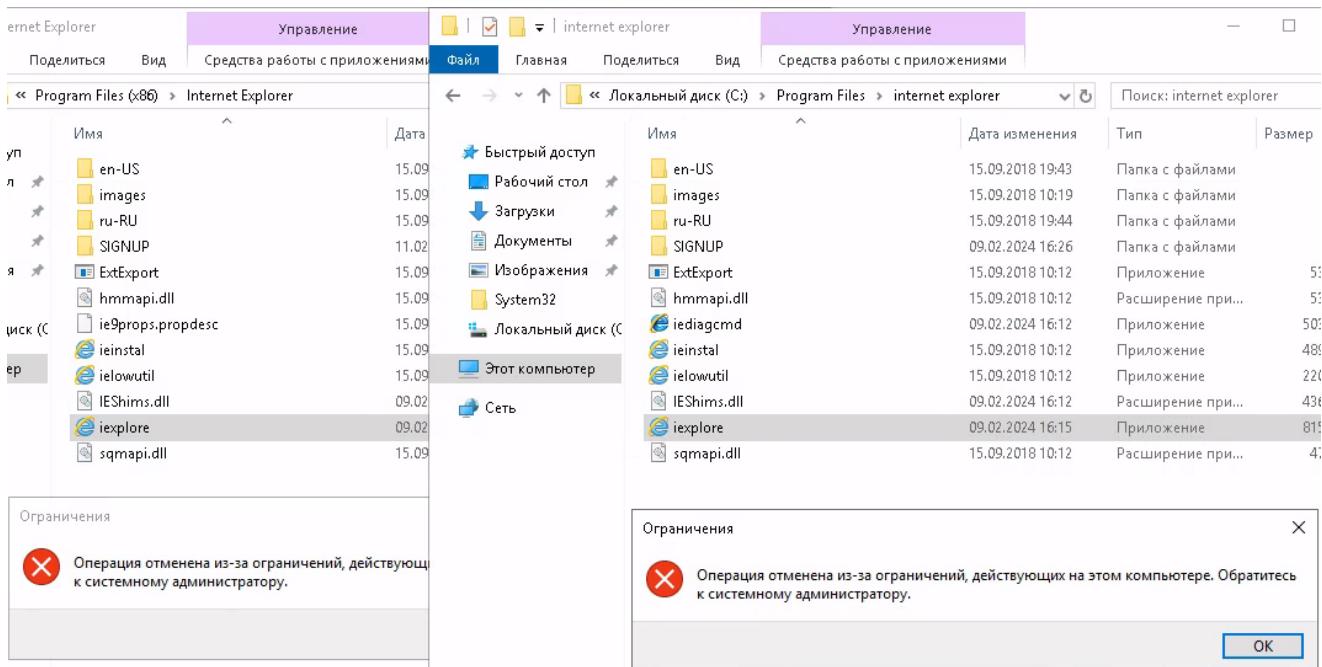
Если вы отключаете или не настраиваете этот параметр политики, пользователи могут запускать любые программы.

Этот параметр политики ограничивает только выполнение



```
PS C:\Users\Администратор.W2019SERV01> gpupdate /Force
Выполняется обновление политики...

Обновление политики для компьютера успешно завершено.
```



Дополнительно:

Права Администратора. Разграничение прав, если есть несколько Админов.

Политика	Параметр безопасности
Kontroller домена: запретить изменение пароля учетных записей компьютера	Не определено
Kontroller домена: разрешать уязвимые подключения по защищенным каналам NetLogon	Не определено
Kontroller домена: разрешить операторам сервера задавать выполнение заданий по расписанию	Не определено
Kontroller домена: разрешить повторное использование учетной записи компьютера во время присоединения ...	Не определено
Kontroller домена: требование цифровой подписи для LDAP-сервера	Нет
Kontroller домена: требования к токенам привязки канала для LDAP-сервера	Не определено
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Включен
Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав	Включен
Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышен...	Включен
Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения ад...	Запрос согласия для и...
Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей	Запрос учетных данных
Контроль учетных записей: повышение прав для UIAccess-приложений только при установке в безопасных местах	Включен
Контроль учетных записей: повышение прав только для подписаных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: разрешение UIAccess-приложениям запрашивать повышение прав, не используя без...	Отключен
Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Не определено
Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик огран...	Отключен
Параметры системы: необязательные подсистемы	
Сервер сети Microsoft: время бездействия до приостановки сеанса	15 мин.

Задание_5:

Включите установку обновлений для Windows и других продуктов Microsoft

Параметры

Главная

Найти параметр

Обновление и безопасность

Центр обновления Windows

Оптимизация доставки

Безопасность Windows

Устранение неполадок

Восстановление

Активация

Для разработчиков

Центр обновления Windows 1

*Некоторыми параметрами управляет ваша организация

Просмотреть настроенные политики обновления

У вас установлены все последние обновления
Время последней проверки: вчера 11:56

Проверить наличие обновлений

Изменить период активности

Просмотр журнала обновлений

Дополнительные параметры 2

Ищете информацию о последних обновлениях?
[Подробнее](#)

Ссылки по теме

[Проверка хранилища](#)

[Информация о сборке ОС и системе](#)

Активация Windows

▷ Дополнительные параметры

*Некоторыми параметрами управляет ваша организация

[Просмотреть настроенные политики обновления](#)

Варианты обновления

При обновлении Windows предоставить обновления для других продуктов Майкрософт.



Автоматически скачивать обновления даже через лимитные подключения данных (может взиматься плата)



Уведомления об обновлениях

Показать уведомление, когда компьютеру требуется перезагрузка для завершения обновления



Установленные обновления

Панель управления — домашняя страница

1 Удаление обновления

2

Удаление программы

Для удаления обновления выберите его в списке и щелкните "Удалить" или "Изменить".

Включение или отключение компонентов Windows

Установка новой программы из сети

Имя	Программа	Версия	Издатель	Установле...
Microsoft Windows (5)	Microsoft Windows		Microsoft Corporation	14.02.2024
Обновление безопасности для Microsoft Windows (KB5034768)	Microsoft Windows		Microsoft Corporation	14.02.2024
Обновление для Microsoft Windows (KB5034619)	Microsoft Windows		Microsoft Corporation	14.02.2024
Servicing Stack 10.0.17763.5441	Microsoft Windows		Microsoft Corporation	09.02.2024
Servicing Stack 10.0.17763.5084	Microsoft Windows		Microsoft Corporation	07.03.2020
Обновление безопасности для Microsoft Windows (KB4539571)	Microsoft Windows		Microsoft Corporation	

Дополнительно:

Проверка на вирусы

Параметры

Главная

Найти параметр

Обновление и безопасность

Центр обновления Windows

Оптимизация доставки

Безопасность Windows

Устранение неполадок

Восстановление

Активация

Для разработчиков

Безопасность Windows

Служба "Безопасность Windows" — это исходная точка просмотра информации о безопасности и работоспособности устройства, а также управления соответствующими компонентами.

Открыть службу "Безопасность Windows"

Области защиты

Защита от вирусов и угроз
Никаких действий не требуется.

Брандмауэр и защита сети
Никаких действий не требуется.

Управление приложениями и браузером
Никаких действий не требуется.

Безопасность устройства
Никаких действий не требуется.

Защита устройства от угроз

Задача выполнена успешно

Быстрая проверка...
Приблизительное оставшееся время: 00:01:41
4335 файлов просканировано

Отмена

Вы можете продолжать работу, пока мы сканируем ваше устройство.

Журнал угроз

Активация V
Чтобы активировать параллель "Параметры"

Блокировка или предупреждение приложений

The screenshot shows the Windows Settings interface under 'Обновление и безопасность' (Update & Security). The 'Безопасность Windows' (Windows Security) option is selected. The 'Области защиты' (Protection areas) section lists four items: 'Защита от вирусов и угроз' (Antivirus and threat protection), 'Брандмаэр и защита сети' (Firewall and network protection), 'Управление приложениями и браузером' (Application and browser management), and 'Безопасность устройства' (Device security). The fourth item is highlighted with a red box. On the right, a separate window titled 'Управление приложениями/браузером' (Manage applications/browser) shows options for 'Блокировать' (Block), 'Предупредить' (Warn), and 'Выключить' (Turn off), with 'Предупредить' selected.

Задание_6:

Включите Аудит событий входа успех\отказ

The screenshot shows the Windows Event Viewer interface. A red circle labeled '1' highlights the 'Управление компьютером' (Computer Management) icon in the left navigation pane. A red circle labeled '2' highlights the 'Служебные программы' (System services) node in the tree view. A red circle labeled '3' highlights the 'Аудит успеха' (Audit success) event listed in the main pane. The event details show it was generated by Microsoft Windows security auditing on 16.02.2024 at 2:55:45. The event properties pane shows the event ID is 4634, the source is Microsoft Windows security, and the category is Logoff. The status bar at the bottom indicates 'Активация Windows... чтобы активировать Windows, перейдите в Параметры' (Activate Windows... to activate Windows, go to Settings).

Базируется на Symantec

← Параметры

Главная

Найти параметр

Обновление и безопасность

- Центр обновления Windows
- Оптимизация доставки
- Безопасность Windows
- Устранение неполадок
- Восстановление
- Активация
- Для разработчиков

Безопасность Windows

Служба "Безопасность Windows" — это исходная точка для просмотра информации о безопасности и работоспособности устройства, а также управления соответствующими функциями.

Открыть службу "Безопасность Windows"

Области защиты

Защита от вирусов и угроз
Никаких действий не требуется.

Брандмауэр и защита сети
Никаких действий не требуется.

Управление приложениями и браузером
Никаких действий не требуется.

Безопасность устройства
Никаких действий не требуется.

Настроим Аудит

Управление компьютером (локальным)

Файл Действие Вид Справка

Служебные программы

Просмотр событий

Настраиваемые представления

Журналы Windows

Приложение

Безопасность

Установка

Система

Перенаправленные события

Журналы приложений и служб

Подписки

Общие папки

Производительность

Диспетчер устройств

Запоминающие устройства

Система архивации данных Windows Server

Управление дисками

Службы и приложения

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	16.02.2024 11:43:20	Microsoft Windows...	5379	User Account Man...
Аудит успеха	16.02.2024 11:43:20	Microsoft Windows...	5379	User Account Man...
Аудит успеха	16.02.2024 11:43:20	Microsoft Windows...	5379	User Account Man...
Аудит успеха	16.02.2024 11:43:20	Microsoft Windows...	5379	User Account Man...
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4634	Logoff
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4634	Logoff
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4634	Logoff
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4634	Logoff
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4624	Logon
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4672	Special Logon
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4634	Logoff
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4624	Logon
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4672	Special Logon
Аудит успеха	16.02.2024 11:43:14	Microsoft Windows...	4624	Logon

Свойства событий

Привязать задачу к событию...

Копировать

Сохранить выбранные события...

Обновить

Справка

Действия

Безопасность

Открыть сохранен...

Создать настраив...

Импорт настраив...

Очистить журнал...

Фильтр текущего ...

Свойства

Найти...

Сохранить все соб...

Привязать задачу к...

Вид

Обновить

Справка

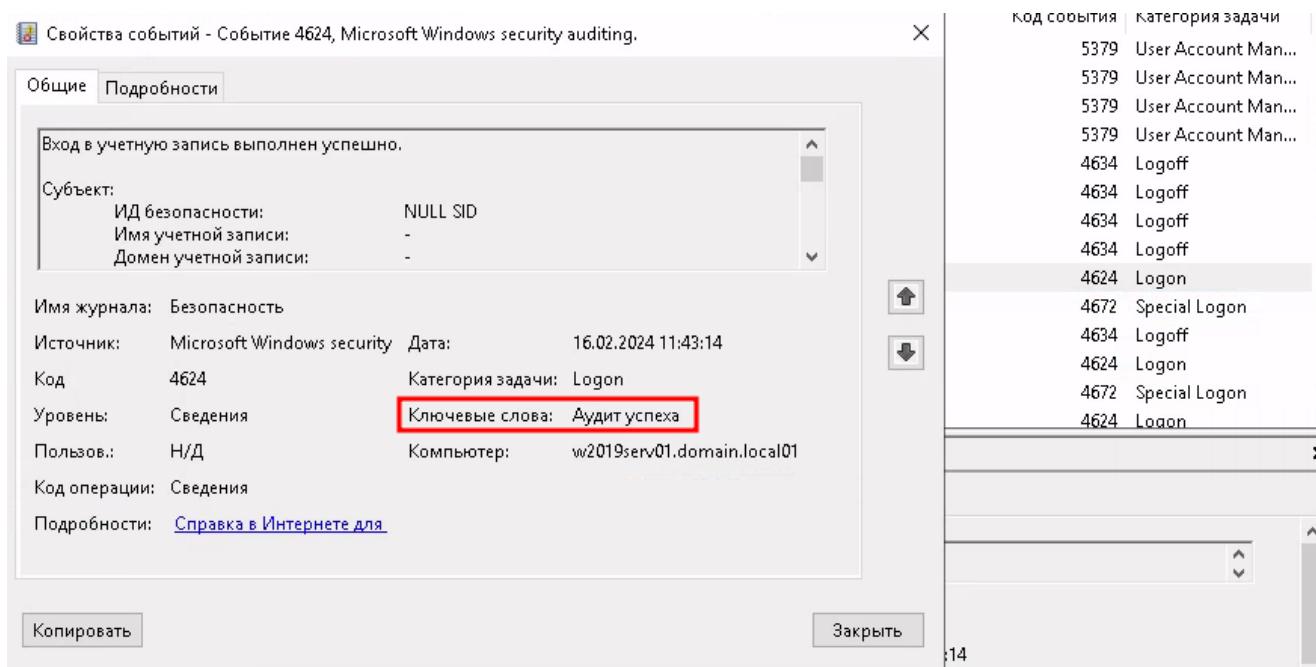
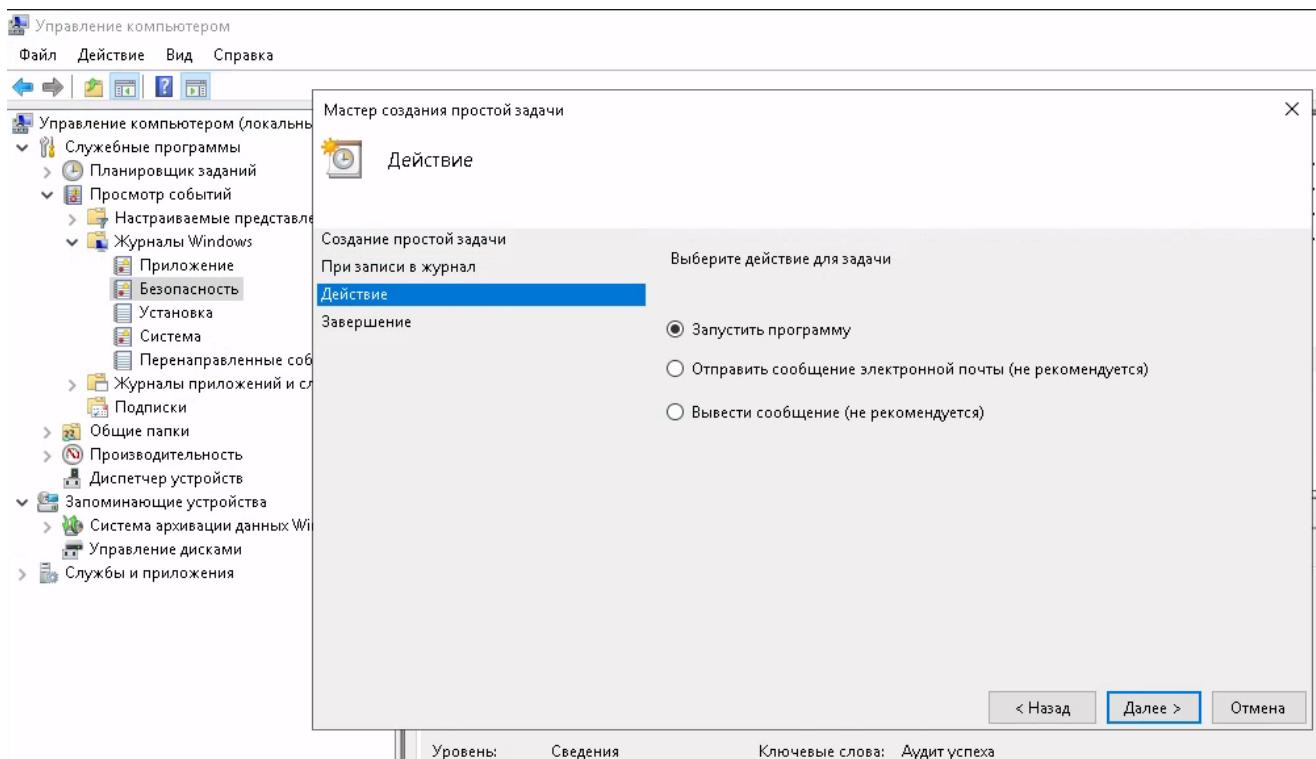
Событие 4624, Microsoft...

Свойства событий

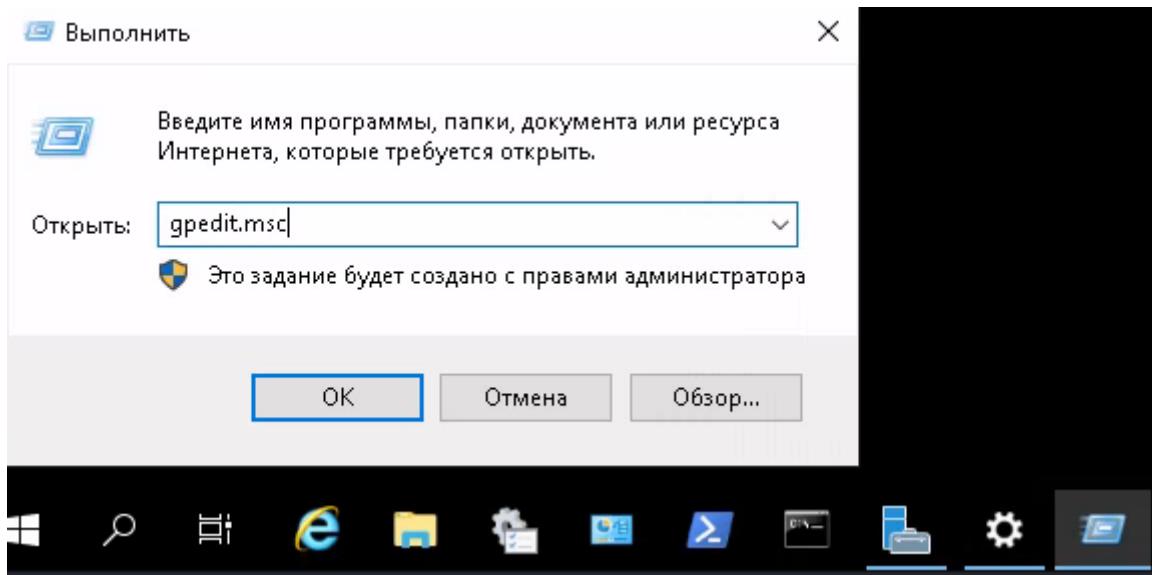
Привязать задачу к...

Копировать

Сохранить выбранны...



Event ID	Описание
4624	A successful account logon event
4625	An account failed to log on
4648	A logon was attempted using explicit credentials
4634	An account was logged off
4647	User initiated logoff



GPO и перейдите в раздел *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Logon/Logoff*

Редактор локальной групповой политики

Файл Действие Вид Справка

Политика "Локальный компьютер"

- Конфигурация компьютера
 - Конфигурация программ
 - Конфигурация Windows
 - Политика разрешения имен
 - Сценарии (запуск/завершение)
 - Развернутые принтеры
 - Параметры безопасности
 - Политики учетных записей
 - Локальные политики
 - Монитор брандмауэра Защитника Windows в режиме повышенной безопасности
 - Политики диспетчера списка сетей
 - Политики открытого ключа
 - Политики ограниченного использования программ
 - Политики управления приложениями
 - Политики IP-безопасности на "Локальный компьютер"
 - Конфигурация расширенной политики аудита
 - Политики аудита системы - Объект локальной групповой политики
 - Вход/выход
 - Доступ к объектам
 - Изменение политики
 - Использование привилегий
 - Система
 - Доступ к глобальным объектам

Подкатегория	События аудита
Аудит блокировки учетных записей	Не настроено
Аудит заявок пользователей или устройств на доступ	Не настроено
Членство в группе аудита	Не настроено
Аудит расширенного режима IPsec	Не настроено
Аудит основного режима IPsec	Не настроено
Аудит быстрого режима IPsec	Не настроено
Аудит выхода из системы	Не настроено
Аудит входа в систему	Не настроено
Аудит сервера политики сети	Не настроено
Аудит других событий входа и выхода	Не настроено
Аудит специального входа	Не настроено

Редактор локальной групповой политики

Файл Действие Вид Справка

Свойства: Аудит входа в систему

Политика Пояснение

Аудит входа в систему

Настроить следующие события аудита:

- Успех
- Отказ

Подкатегория	События аудита
Аудит блокировки учетных записей	Не настроено
Аудит заявок пользователей или устройств на доступ	Не настроено
Членство в группе аудита	Не настроено
Аудит расширенного режима IPsec	Не настроено
Аудит основного режима IPsec	Не настроено
Аудит быстрого режима IPsec	Не настроено
Аудит выхода из системы	Успех
Аудит входа в систему	Успех и отказ
Аудит сервера политики сети	Не настроено
Аудит других событий входа и выхода	Не настроено
Аудит специального входа	Не настроено

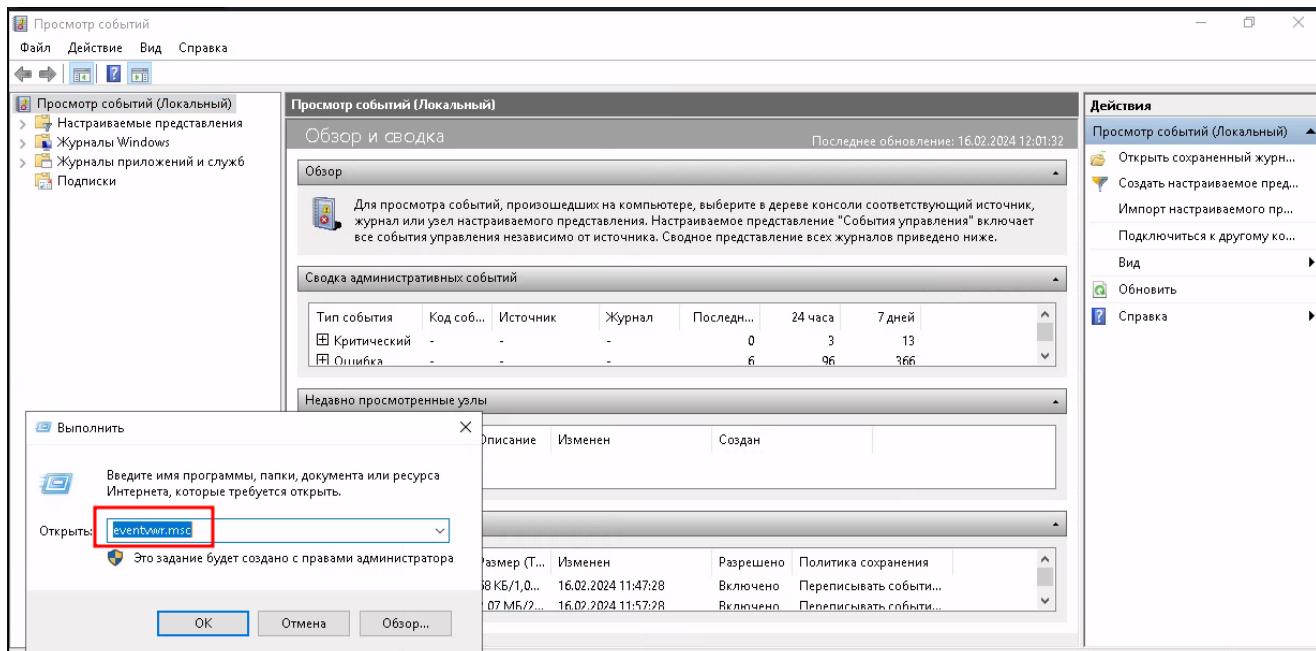
Свойства: Аудит выхода из системы

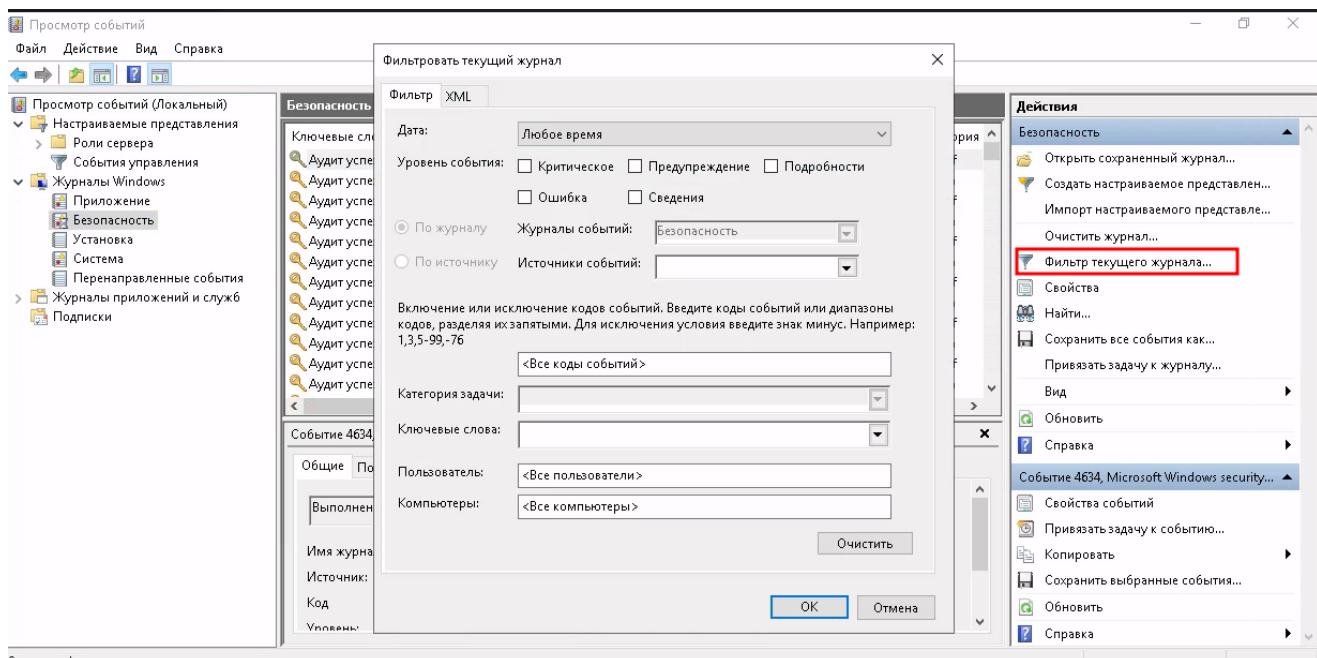
Политика	Пояснение	Подкатегория	События аудита
	Аудит выхода из системы	Аудит блокировки учетных записей	Не настроено
<input checked="" type="checkbox"/> Настроить следующие события аудита:	<input checked="" type="checkbox"/> Успех	Аудит заявок пользователей или устройств на доступ	Не настроено
	<input type="checkbox"/> Отказ	Членство в группе аудита	Не настроено
		Аудит расширенного режима IPsec	Не настроено
		Аудит основного режима IPsec	Не настроено
		Аудит быстрого режима IPsec	Не настроено
		Аудит выхода из системы	Не настроено
		Аудит входа в систему	Не настроено
		Аудит сервера политики сети	Не настроено
		Аудит других событий входа и выхода	Не настроено
		Аудит специального входа	Не настроено

Поиск событий входа пользователей в журнале событий Windows

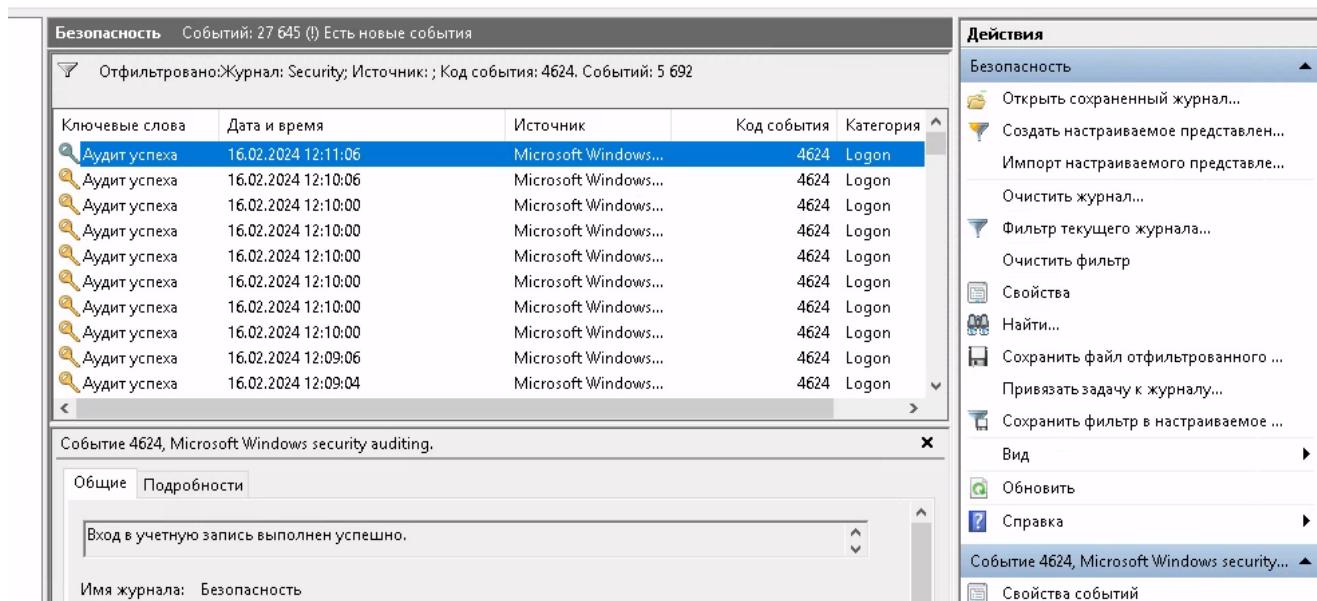
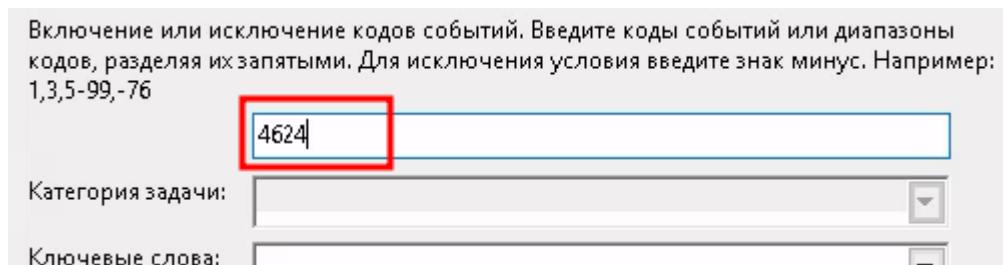
После того как вы включили политики аудита входа, при каждом входе пользователя в Windows в журнале Event Viewer будет появляться запись о входе. Посмотрим, как она выглядит.

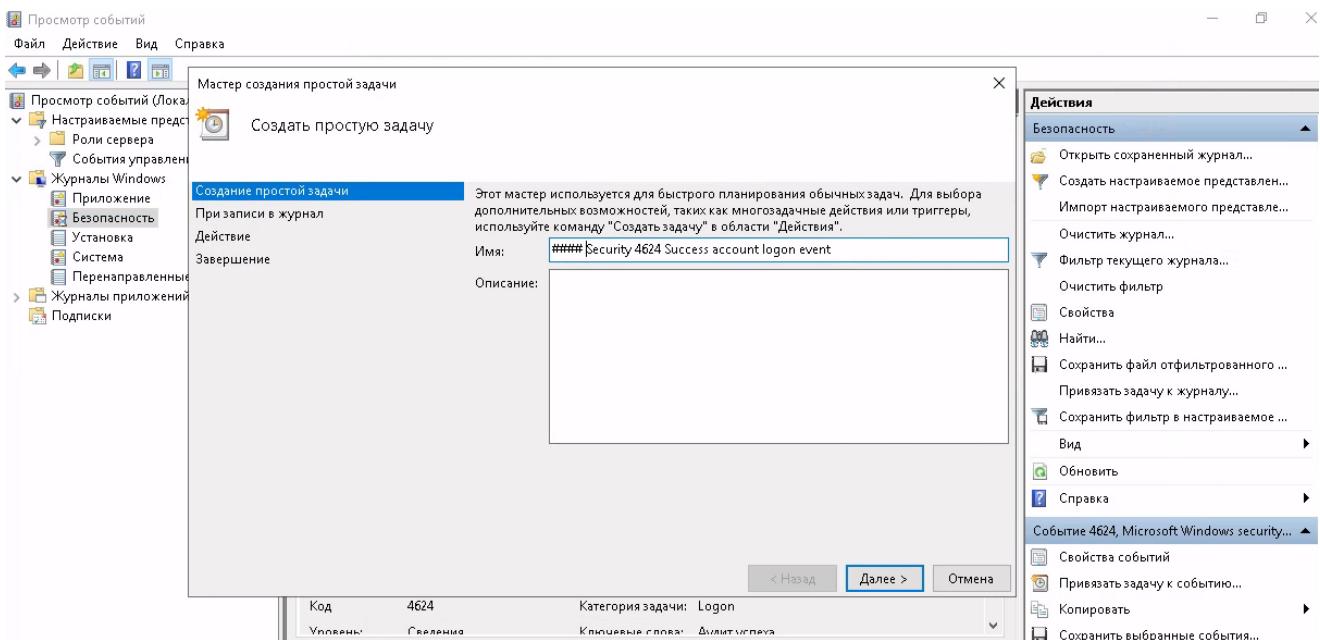
1. Откройте оснастку Event Viewer (`eventvwr.msc`);
2. Разверните секцию Windows Logs и выберите журнал **Security**;
3. Щелкните по нему правой клавишей и выберите пункт **Filter Current Log**;
4. В поле укажите ID события **4624** и нажмите OK;





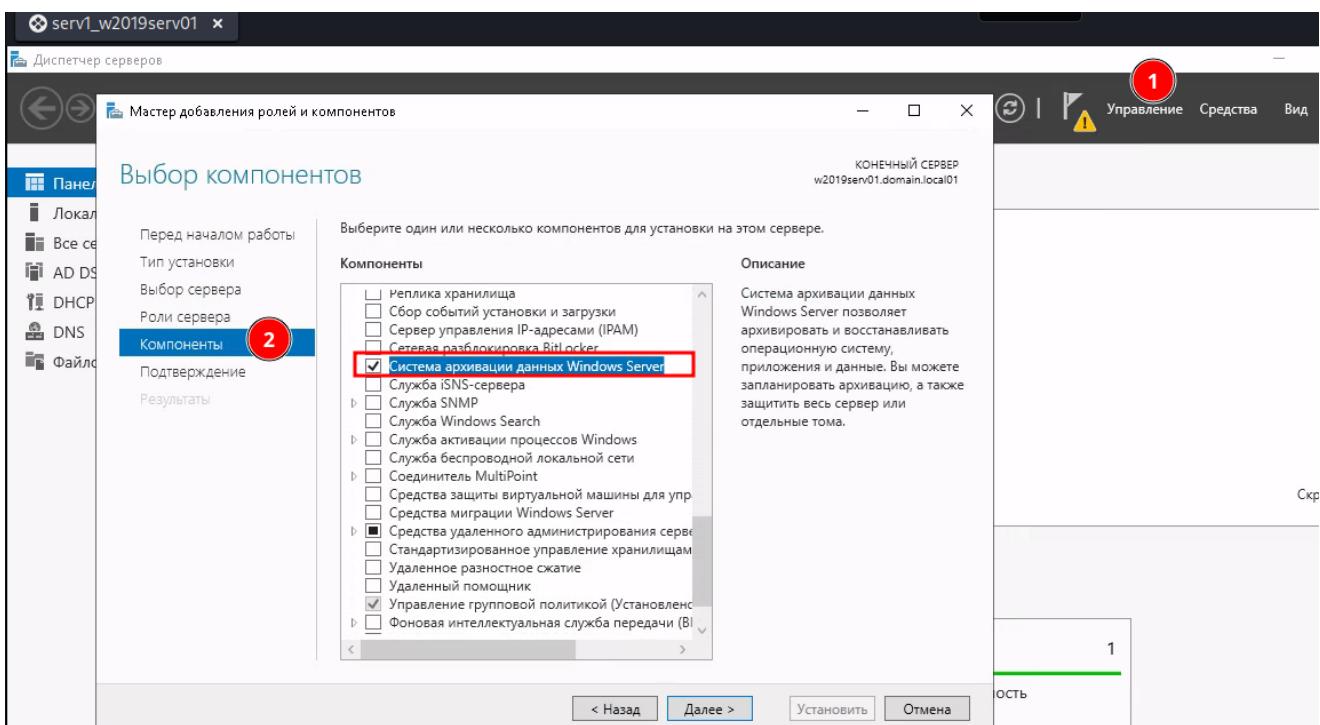
Создание фильтра.

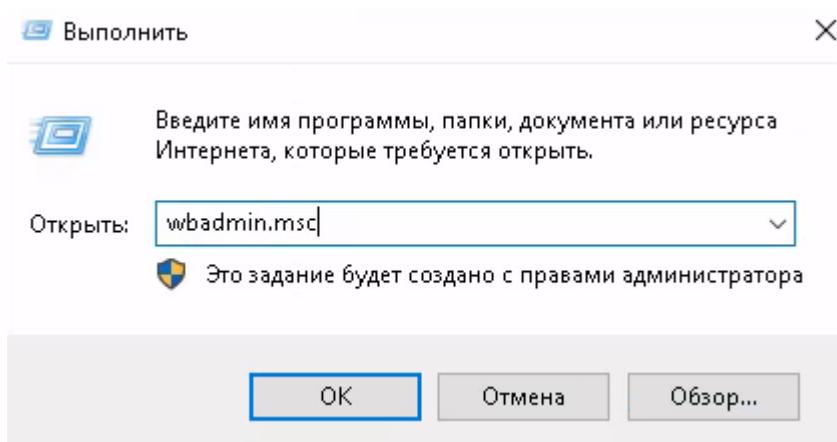
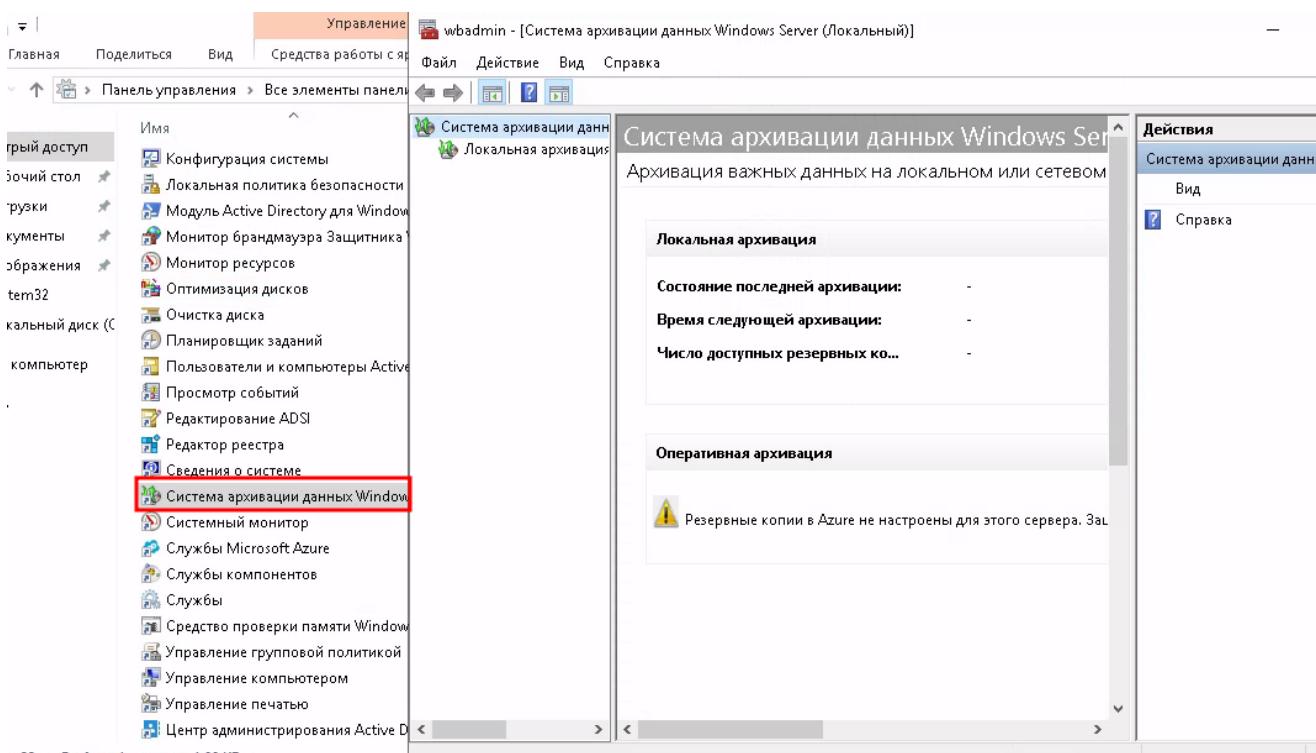
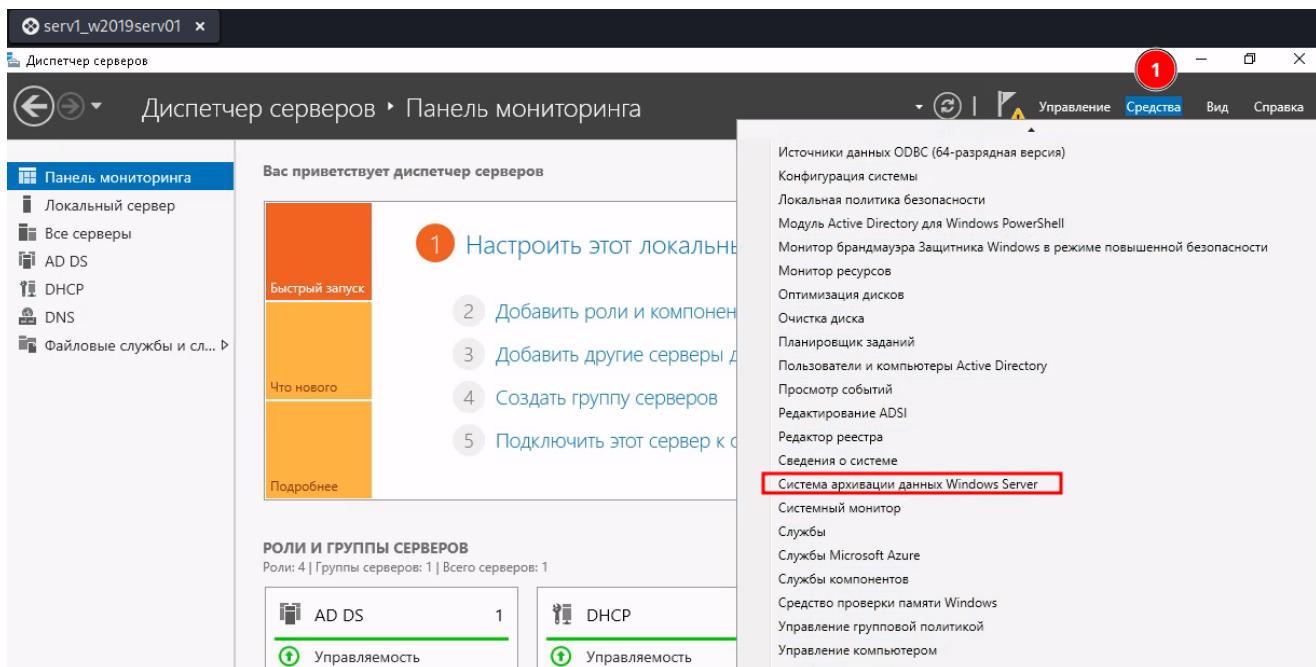


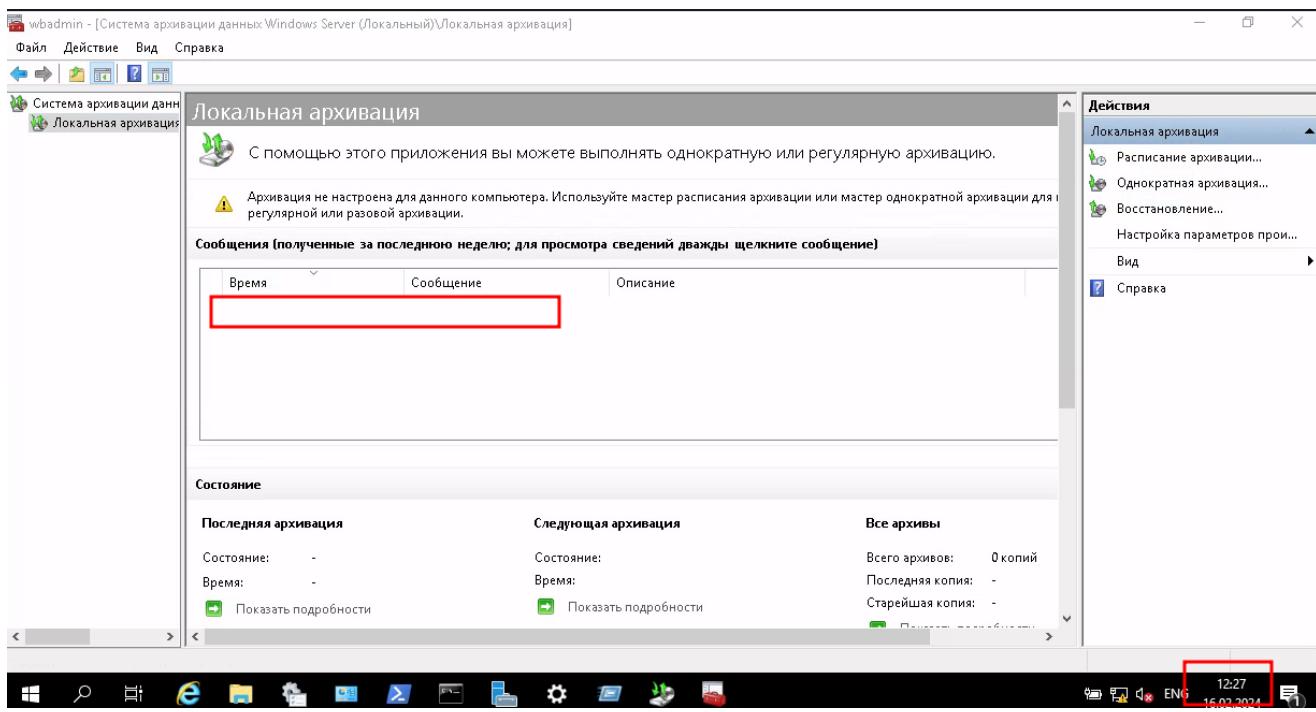


Задание_7:

- 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
- Используя утилиту WBadmin создайте резервную копию системы
- Посмотрите, какое количество резервных копий "видит" система
- Удалите самую старую резервную копию.

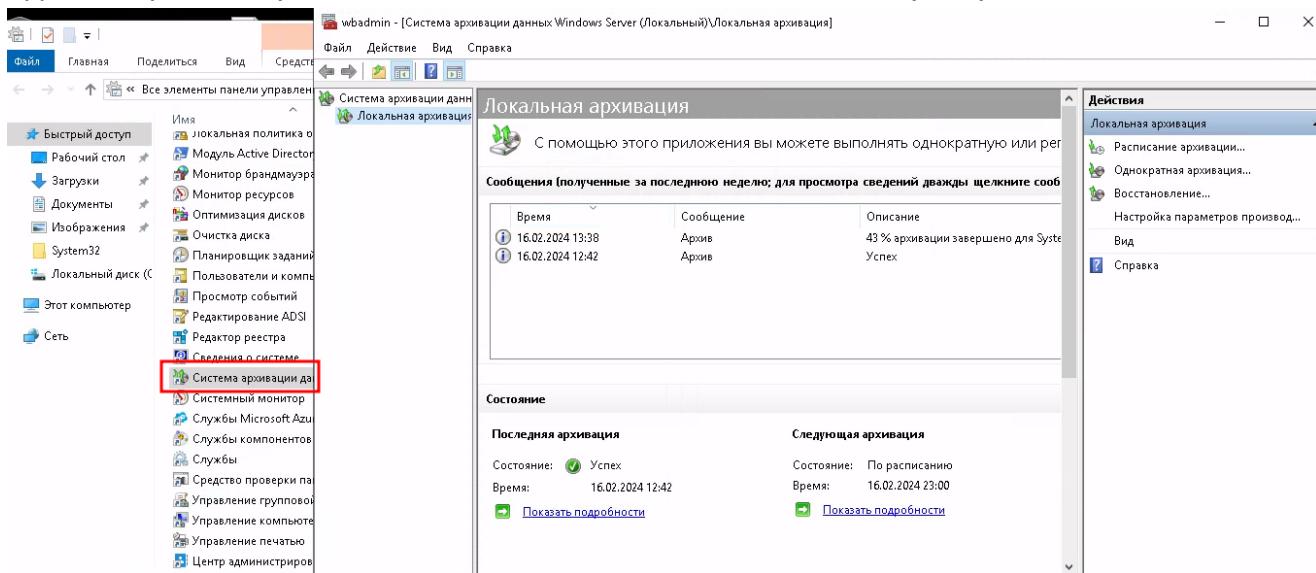


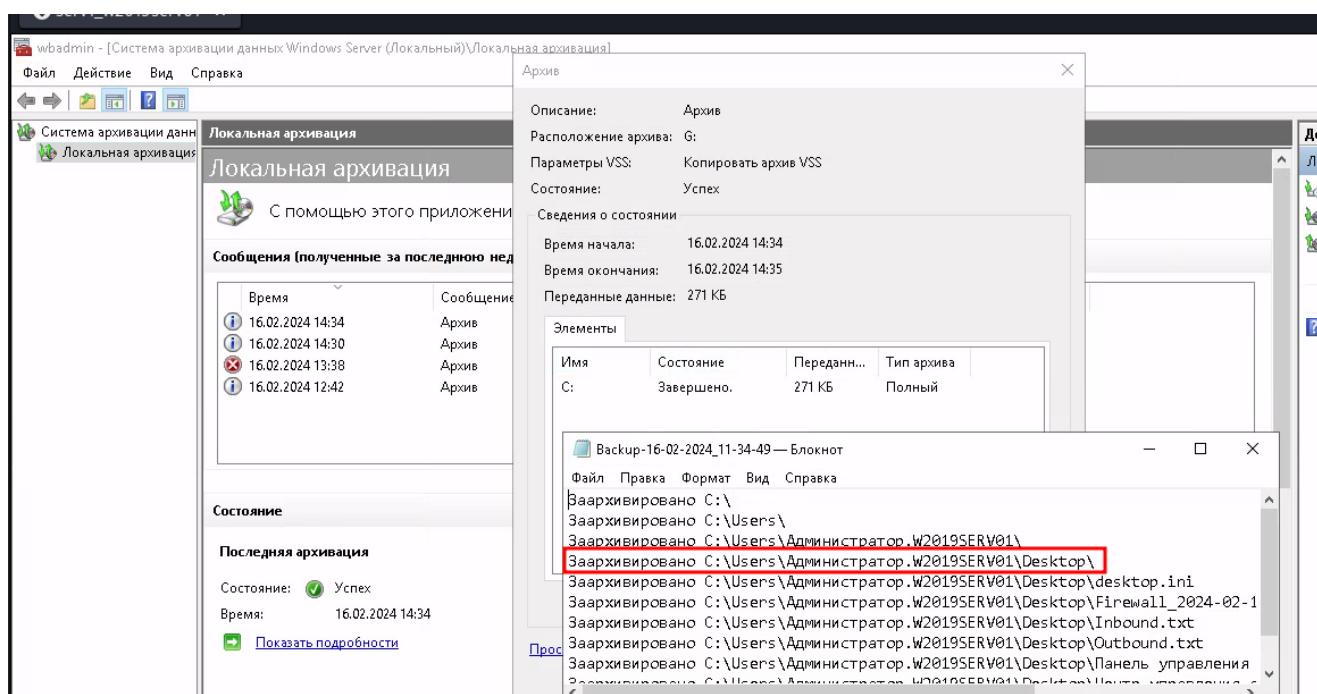
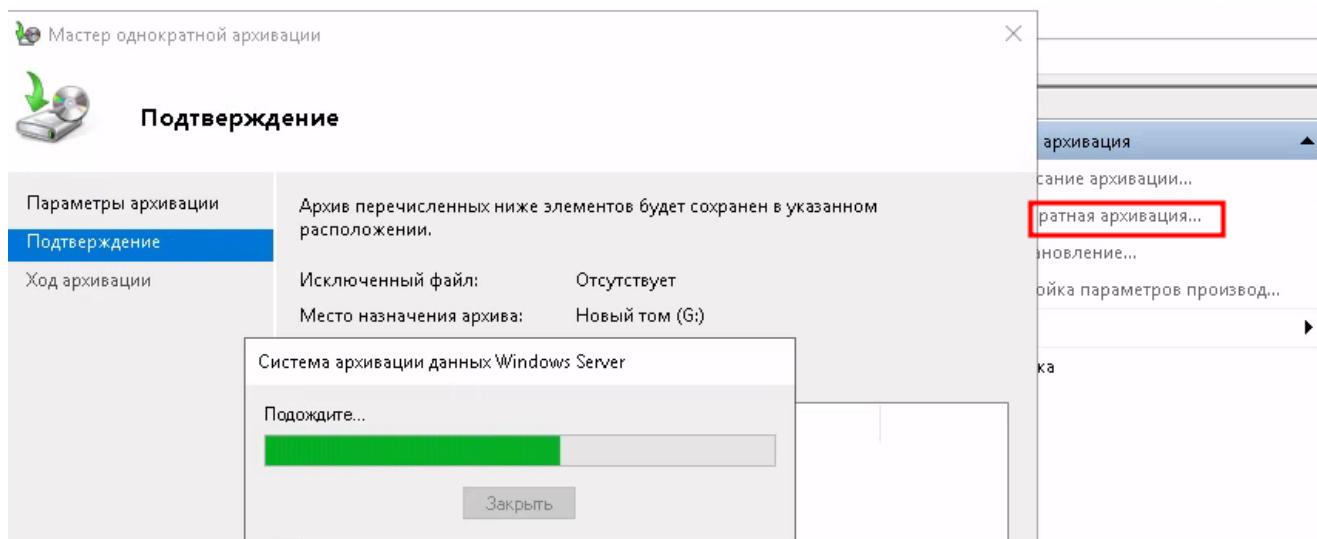
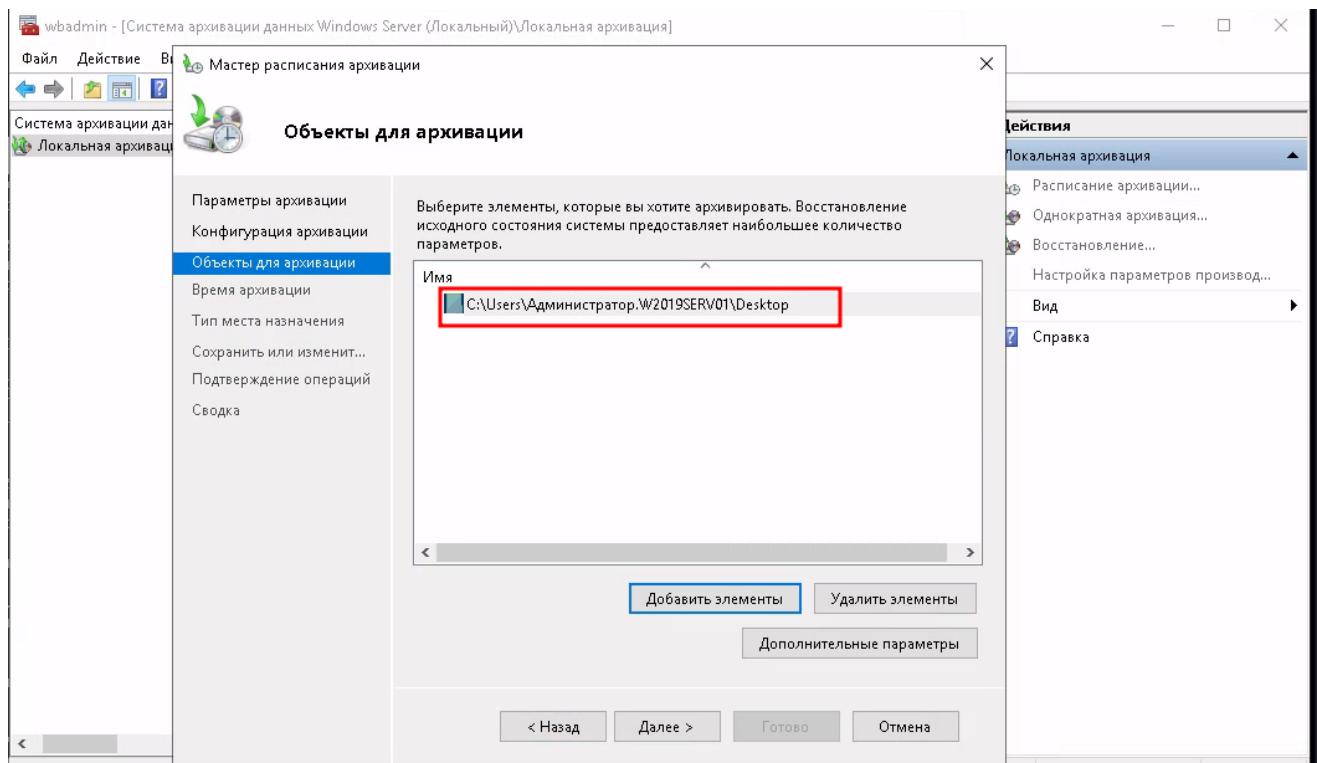


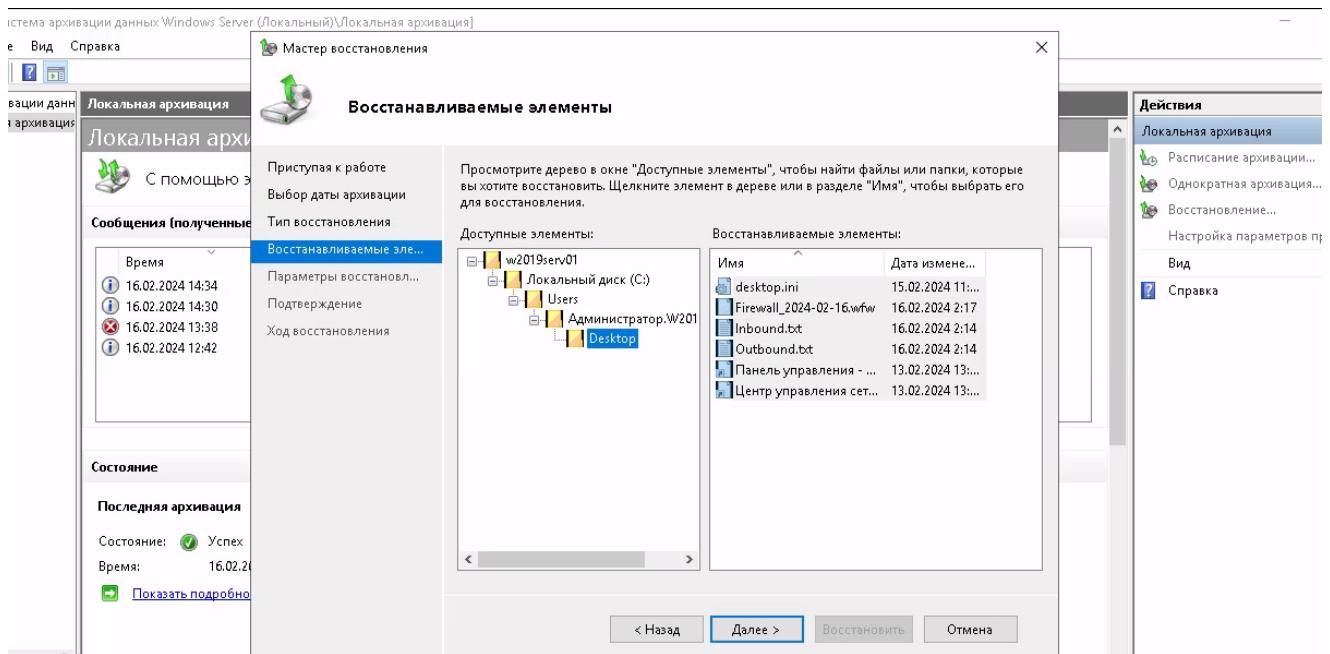
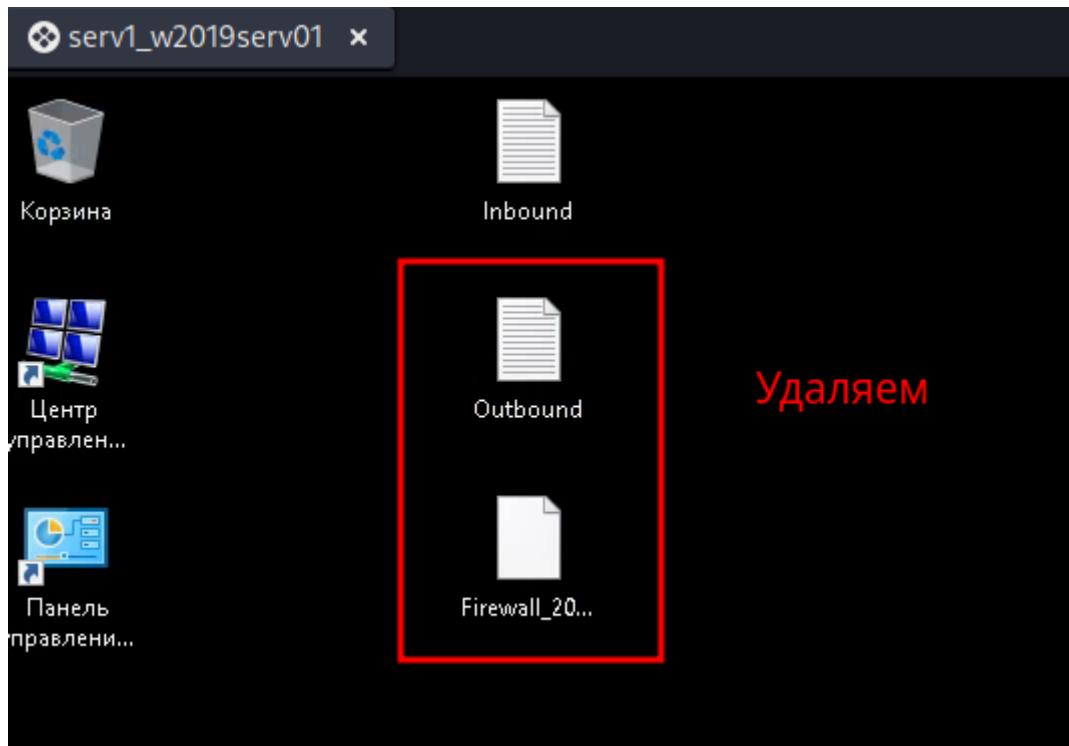


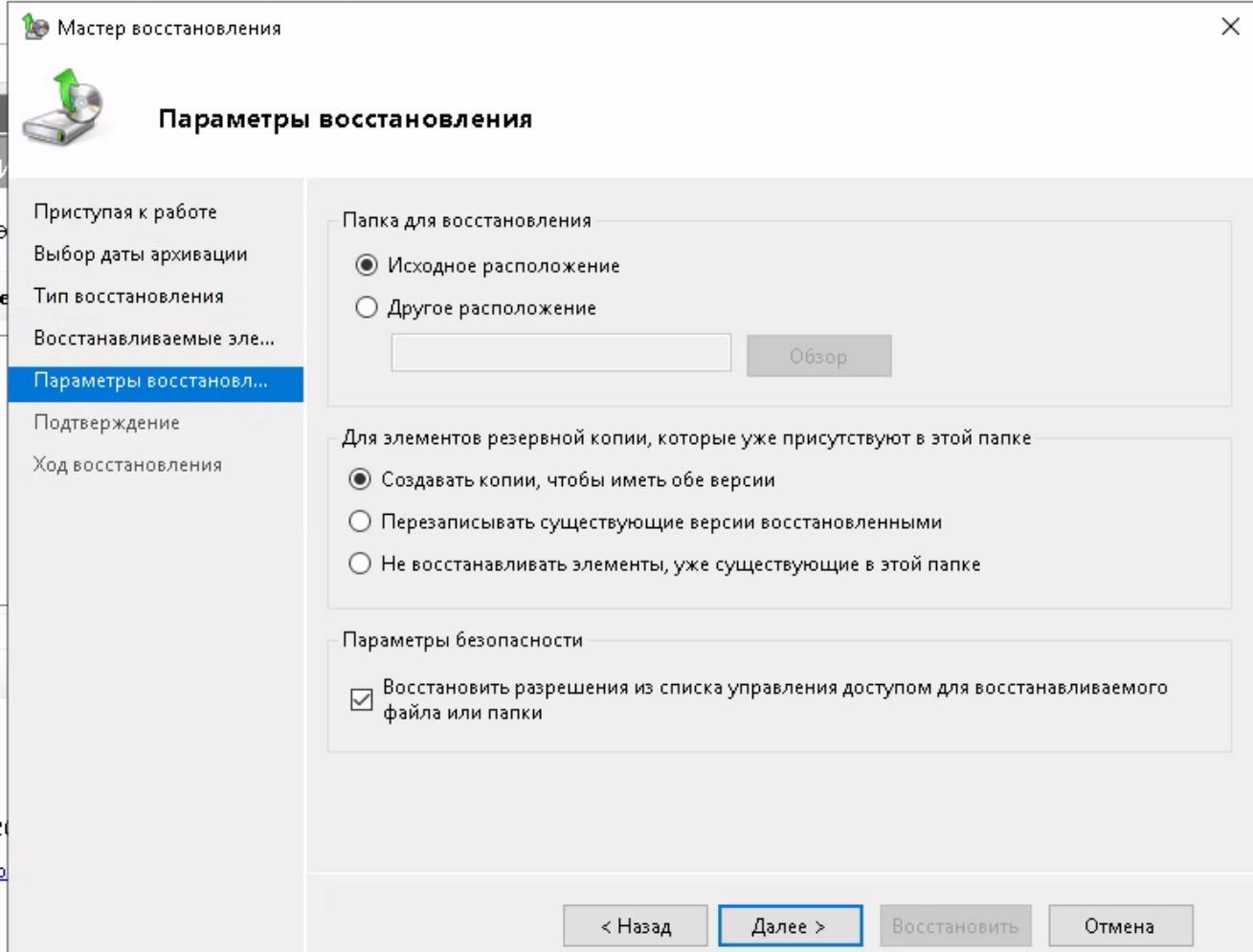
Если архив слишком старый и не подлежит восстановлению, меняем текущую дату.

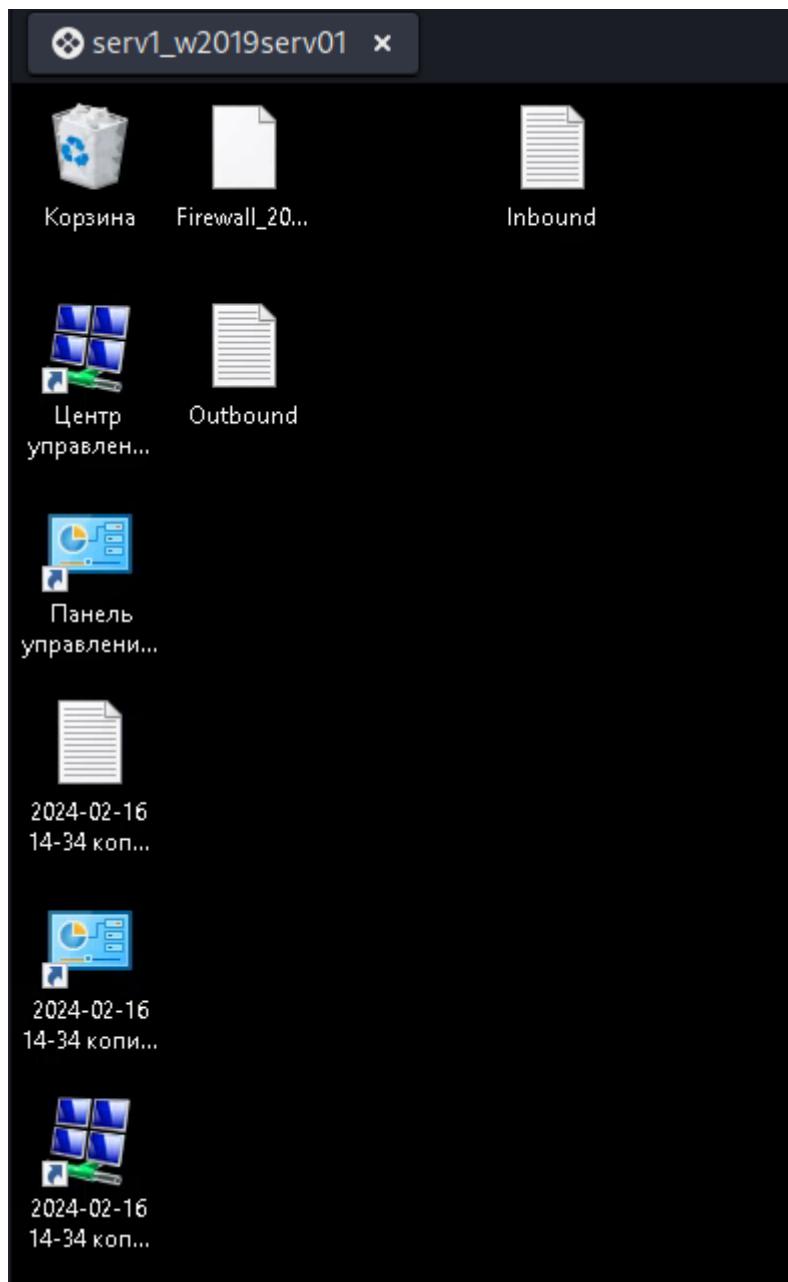
Удалите файлы с рабочего стола, затем восстановите их из резервной копии



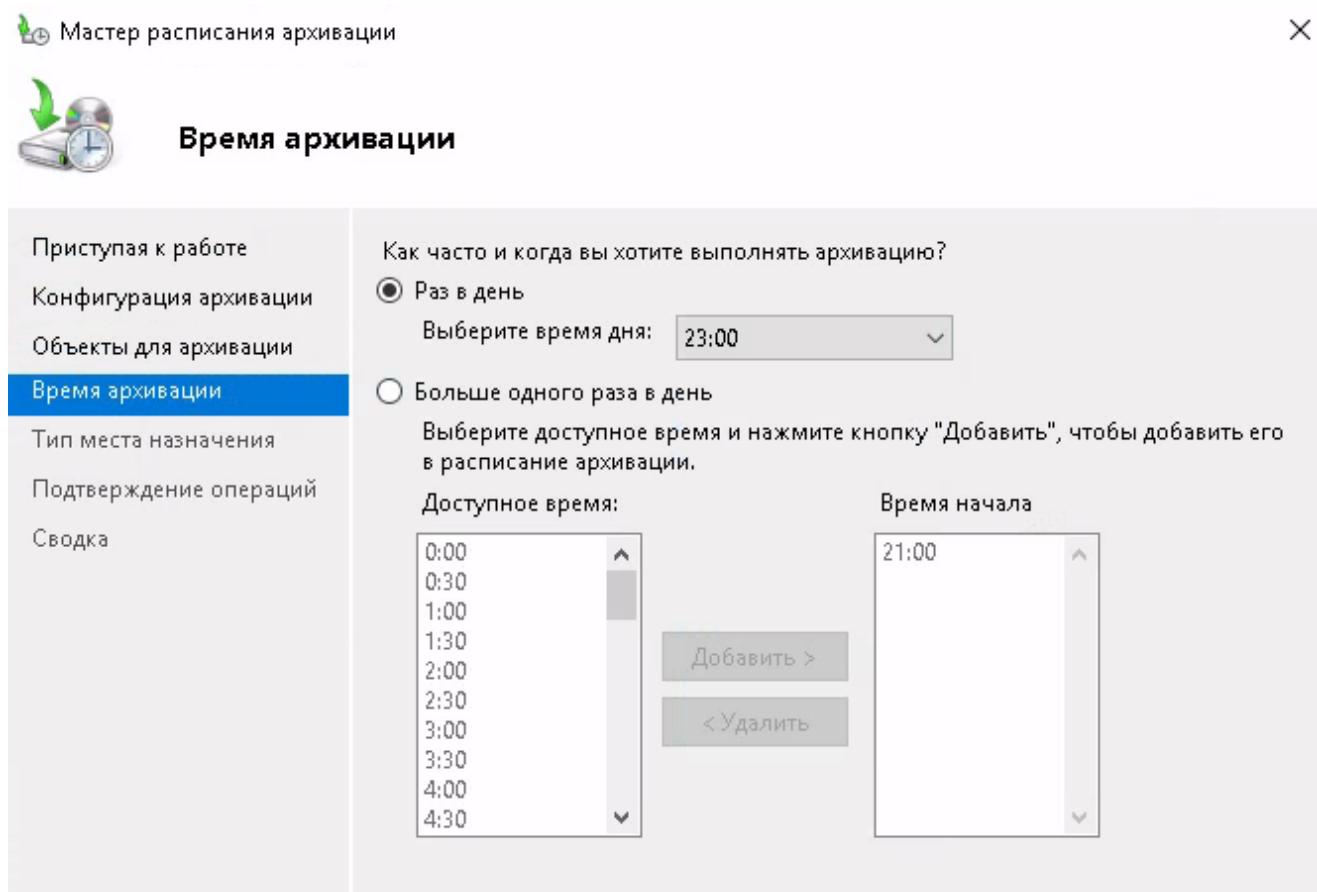
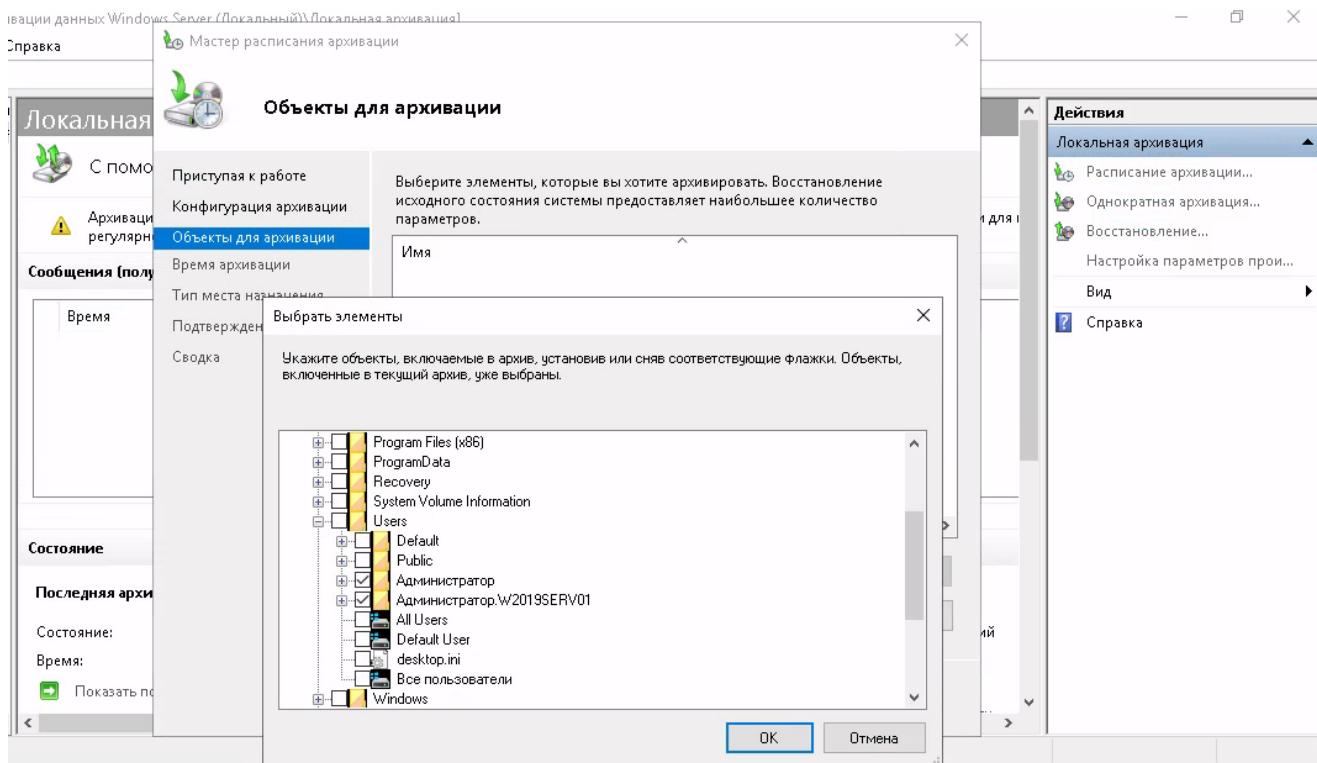


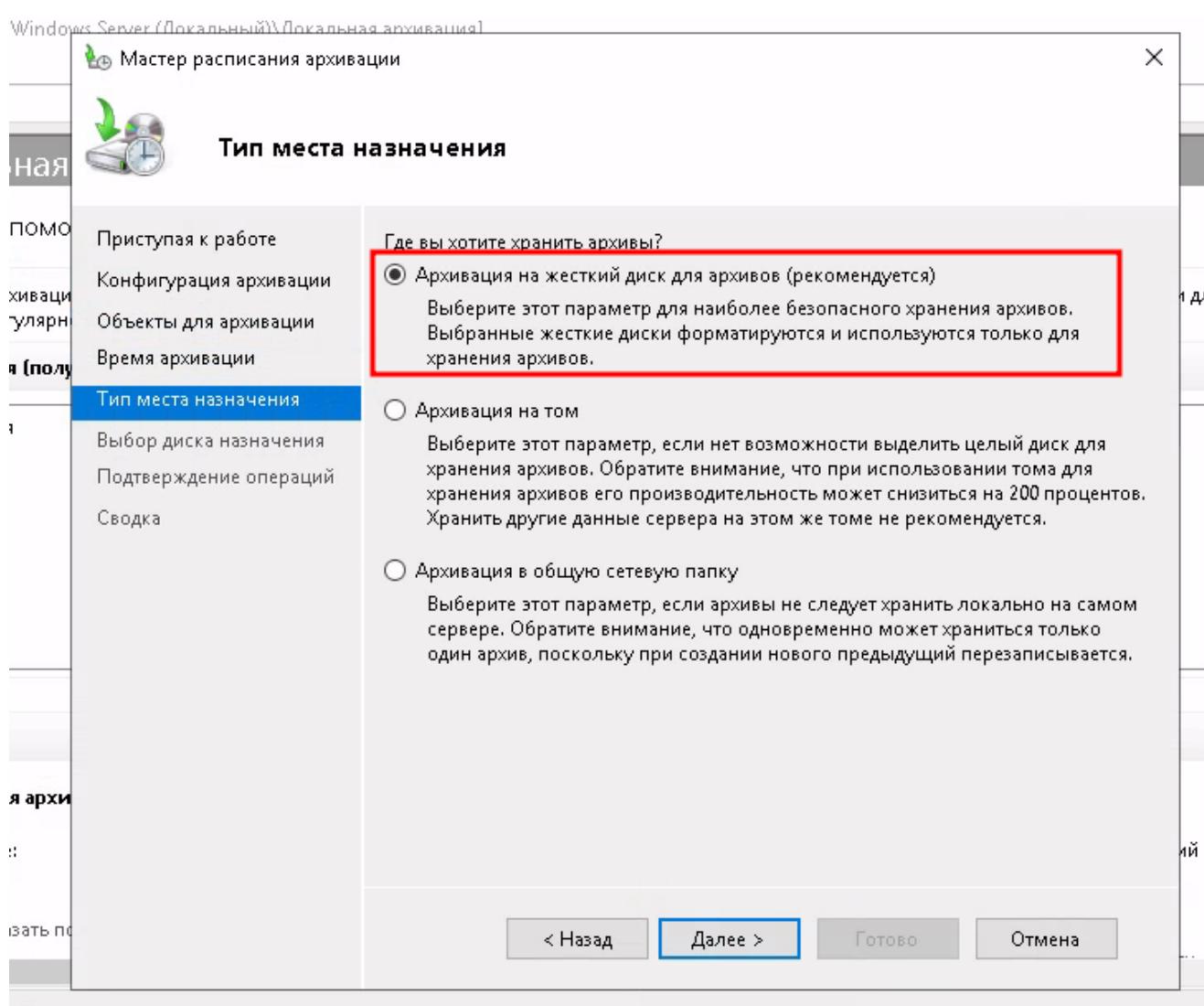
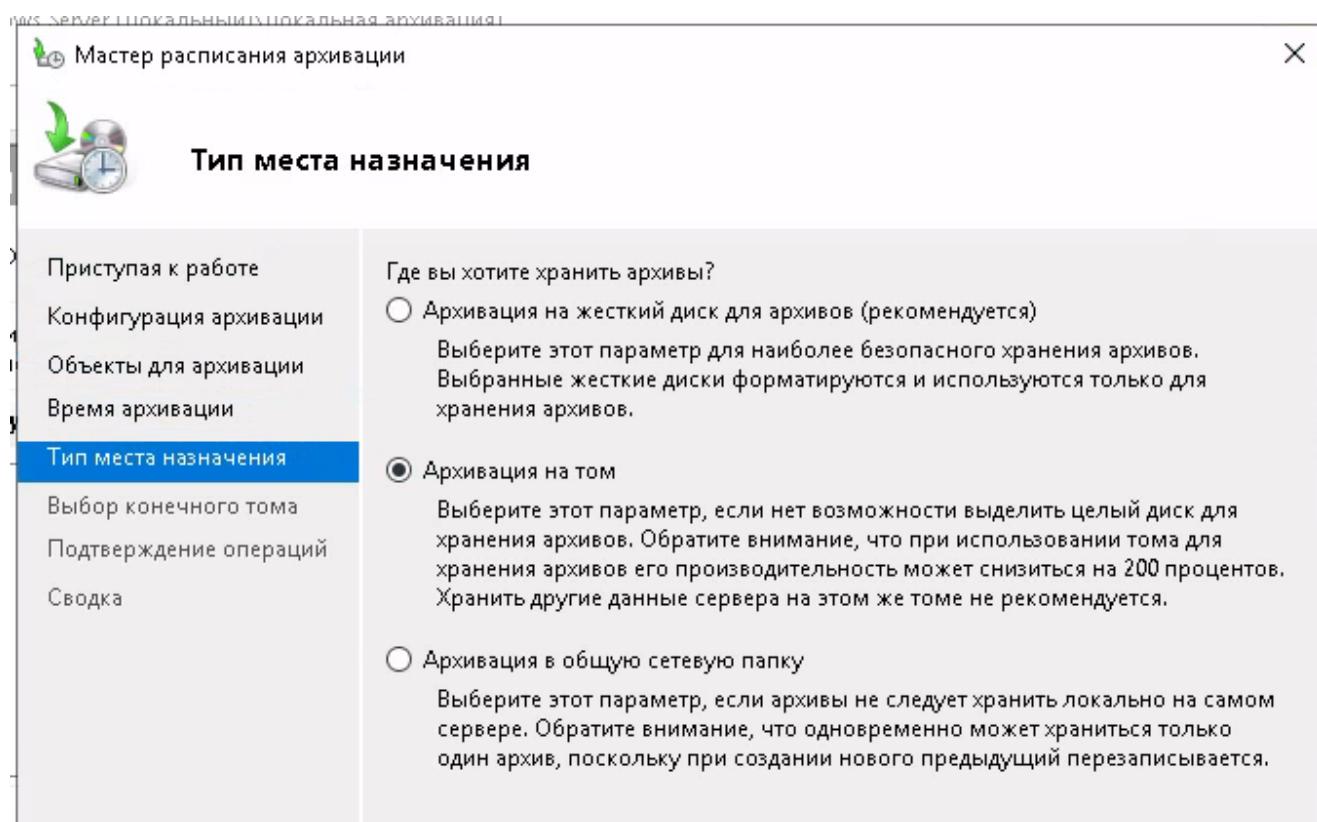






Используя утилиту WAdmin создайте
резервную копию системы







Выбор диска назначения

Все доступные диски

На странице мастера (по умолчанию) отображается только диск, использование которого вами наиболее вероятно.

В списке ниже показаны все внутренние и внешние диски, подключенные к этому серверу. В список не включены критически важные диски, содержащие системные файлы, и диски общих томов кластера.

Установите флажок для диска, чтобы он отображался в списке доступных дисков на странице мастера.

Доступные диски:

Диск	Имя	Размер	Занято	Тома
<input checked="" type="checkbox"/> 1	Microsoft Virtual Disk	10,00 ГБ	56,71 МБ	E:\;F:\



, Несколько
са.

- Приступая к работе
- Конфигурация архивации
- Объекты для архивации
- Время архивации
- Тип места назначения
- Выбор диска назначения**
- Подтверждение операций
- Сводка



Выбор диска назначения

Приступая к работе

Конфигурация архивации

Объекты для архивации

Время архивации

Тип места назначения

Выбор диска назначения

Подтверждение операций

Сводка

Выберите один или несколько дисков для хранения резервных копий. Несколько дисков можно использовать, если вы планируете хранить их вне офиса.

Доступные диски:

Диск	Имя	Размер	Занято	Тома на диске
<input checked="" type="checkbox"/> 1	Microsoft ...	10,00 ГБ	56,71 МБ	E:\;F:\

[Показать все доступные диски...](#)



Подтверждение операций

Приступая к работе

Будет создано следующее расписание архивации.

Конфигурация архивации

Время архивации: 23:00

Объекты для архивации

Исключенные файлы: Отсутствует

Время архивации

Дополнительные параметры: Копировать архив VSS

Тип места назначения

Места назначения архива

Выбор диска назначения

Имя	Только заголовок	Размер	Занято
Microsoft Virt... w2019se 2024_...	10,00 ГБ	56,71 МБ	

Подтверждение операций

Сводка

Архивные элементы

Имя

C:\Users\Администратор

ⓘ При создании архива томов, на которых размещены файлы виртуальных жестких дисков, VHD-файлы автоматически исключаются из архива, если они подключены во время создания архива. Для архивации содержимого VHD-файлов необходимо архивировать виртуальные тома отдельно или отключать VHD-файлы перед всеми операциями архивации.

< Назад

Далее >

Готово

Отмена

wbadmin - [Система архивации данных Windows Server (Локальный)\Локальная архивация]

Файл Действие Вид Справка

Система архивации данных
Локальная архивация

Локальная архивация

С помощью этого приложения вы можете выполнять операции с архивами.

Сообщения (полученные за последнюю неделю; для просмотра сведений)

Время	Сообщение	Описание
16.02.2024 12:42	Архив	Успех

Состояние

Последняя архивация

Состояние: Успех
Время: 16.02.2024 12:42
[Показать подробности](#)

Архив

Описание: Архив
Расположение архива: w2019se 2024_02_16 12:40 DISK_01
Параметры VSS: Копировать архив VSS
Состояние: Успех

Сведения о состоянии

Время начала: 16.02.2024 12:42
Время окончания: 16.02.2024 12:43
Переданные данные: 334,53 МБ

Элементы

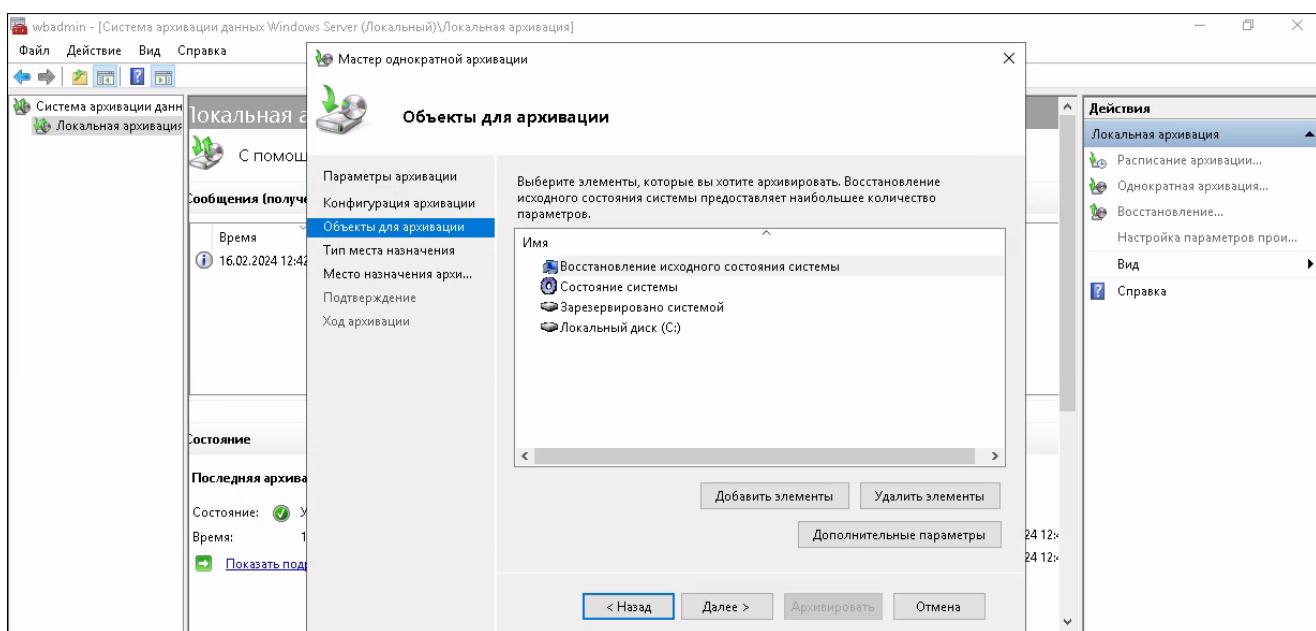
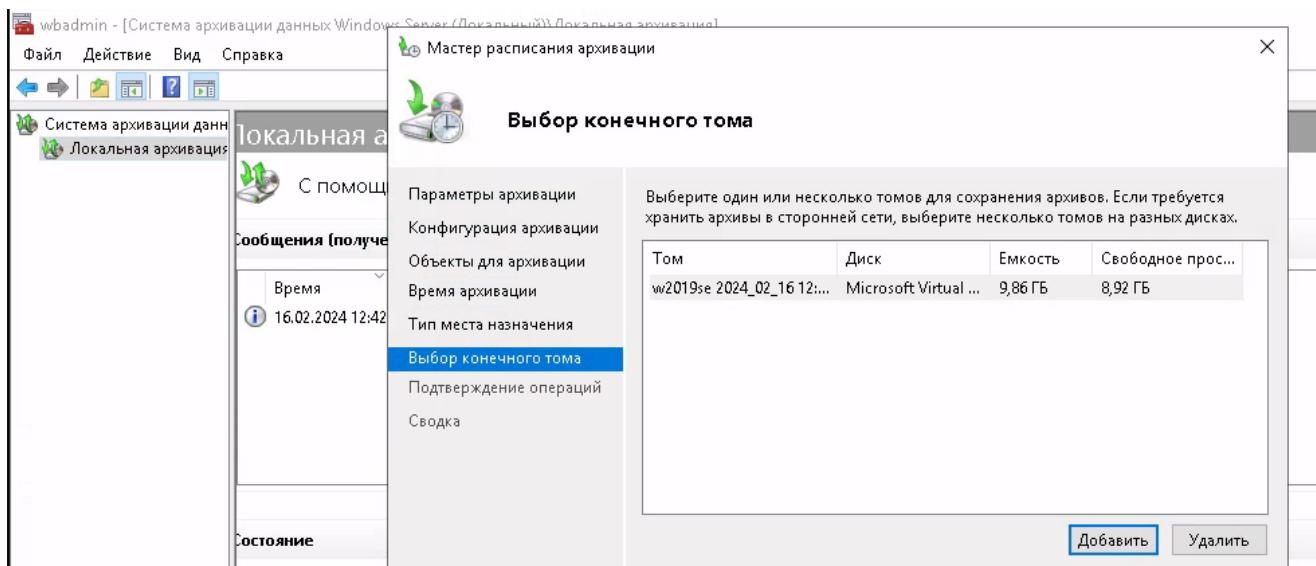
Имя	Состояние	Переданны...	Тип архива
C:	Завершено.	334,53 МБ	Полный

Backup-16-02-2024_09-42-10 — Блокнот

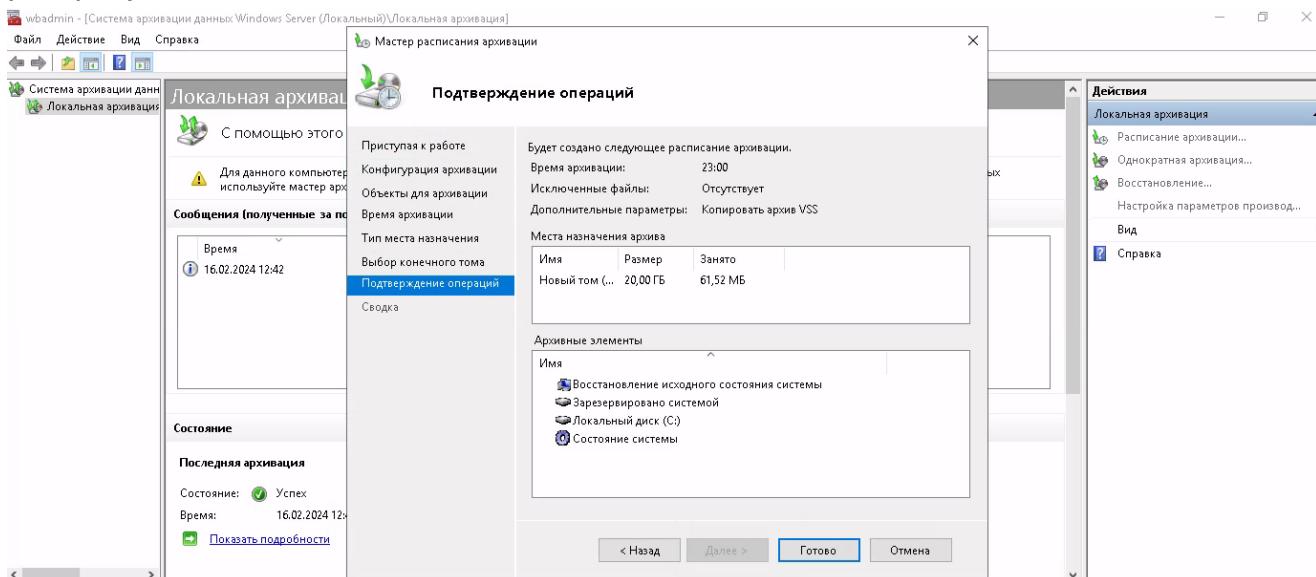
Файл Правка Формат Вид Справка

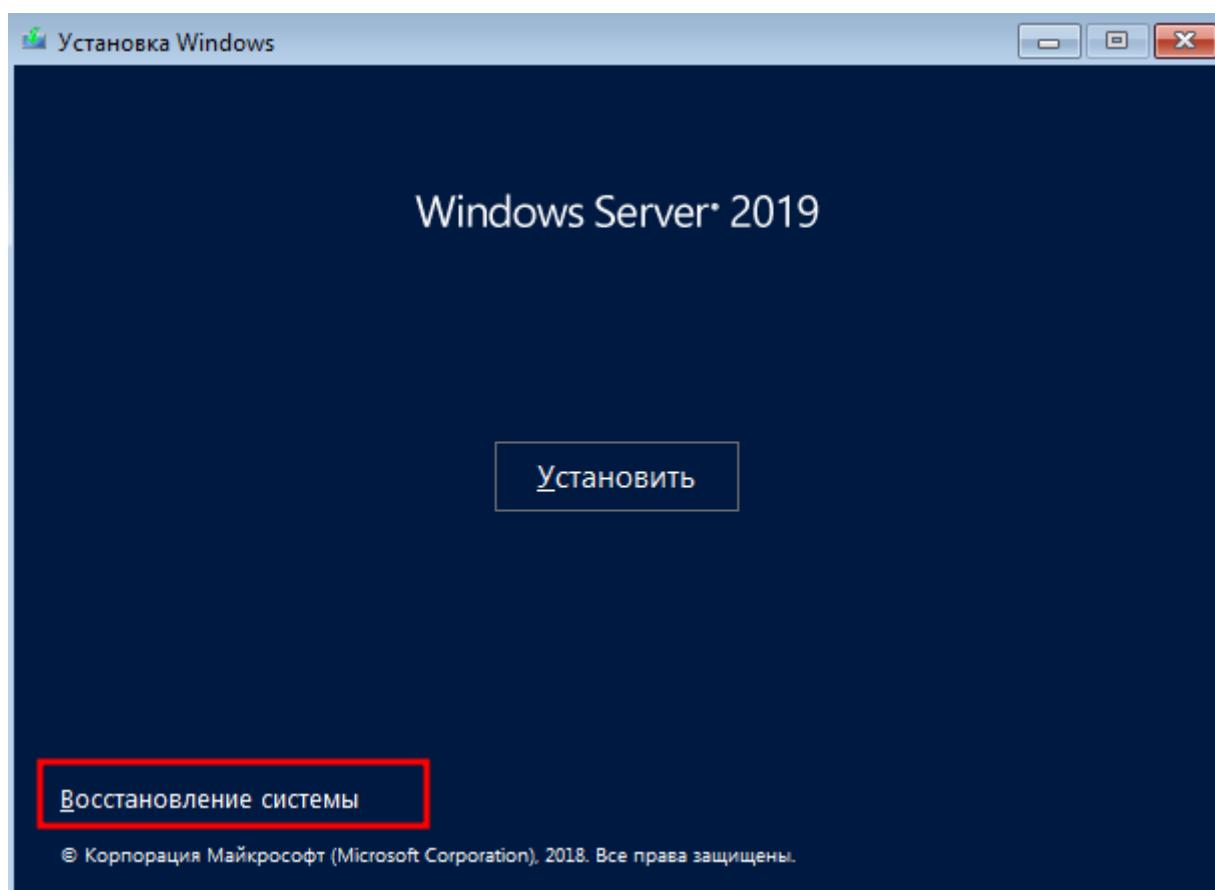
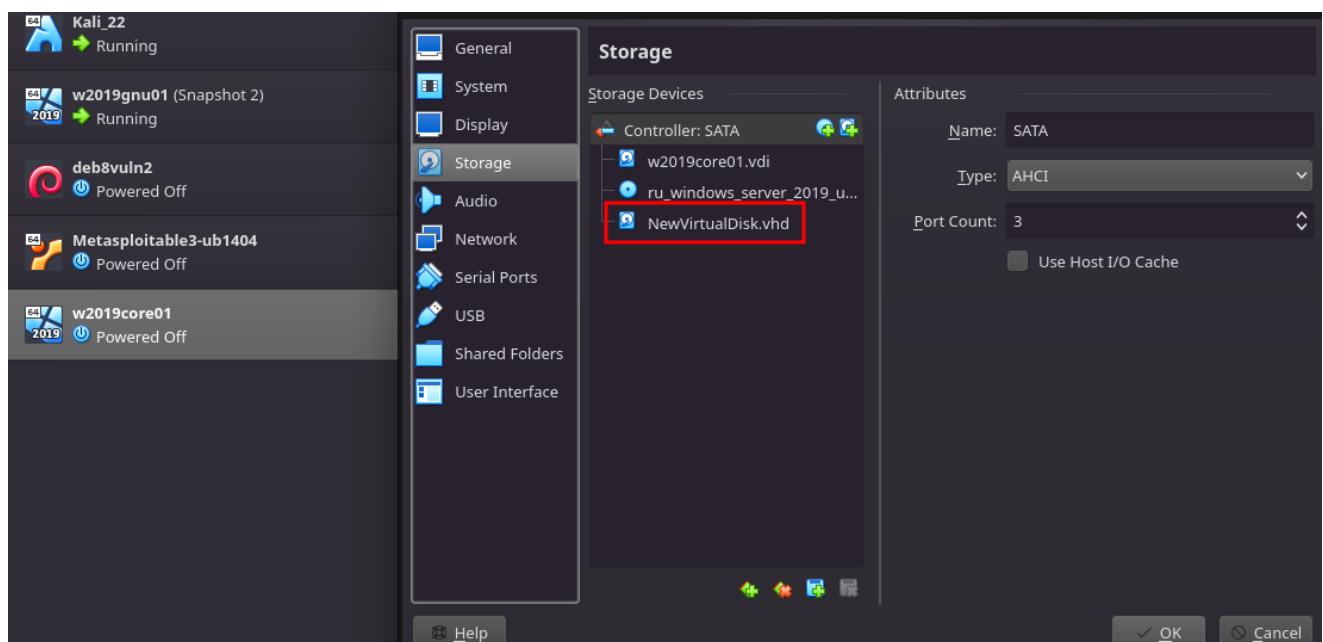
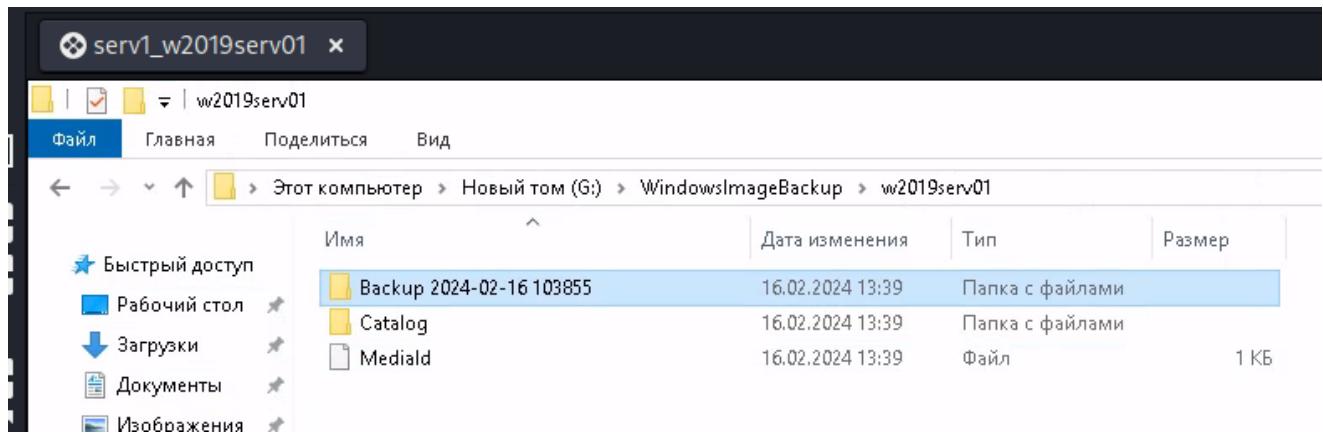
- Заархивировано C:\
- Заархивировано C:\Users\
- Заархивировано C:\Users\Администратор\
- Заархивировано C:\Users\Администратор\log.txt
- Заархивировано C:\Users\Администратор\NTUSER.DAT

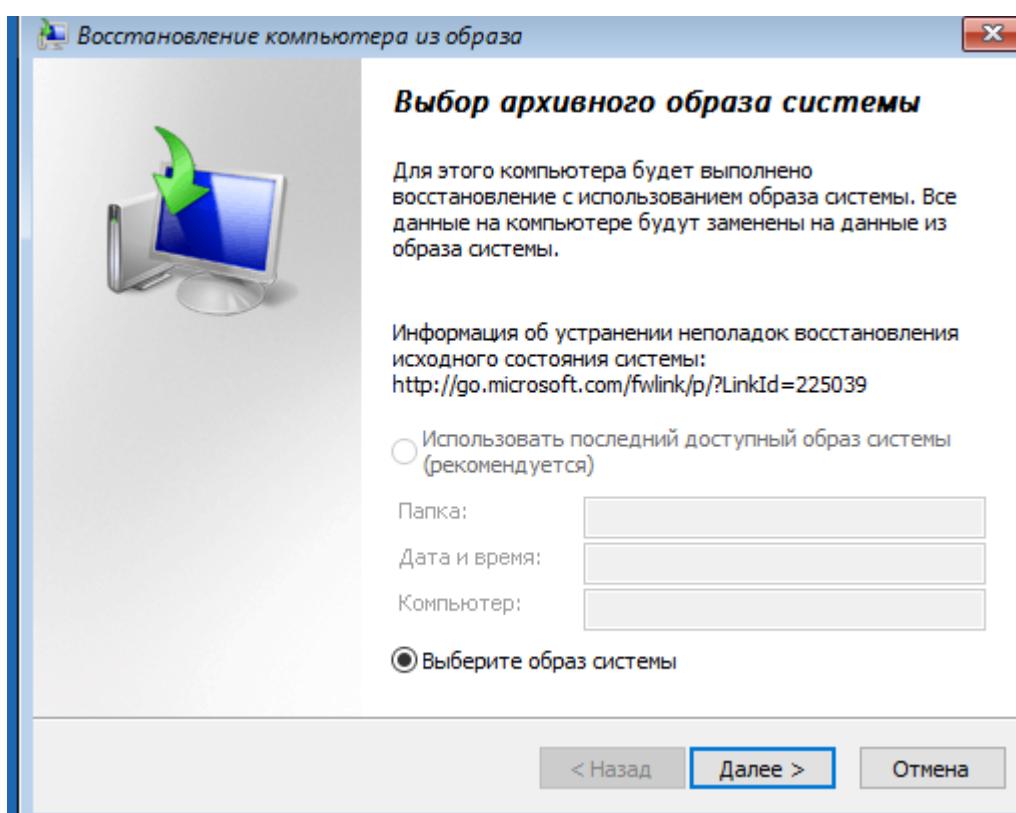
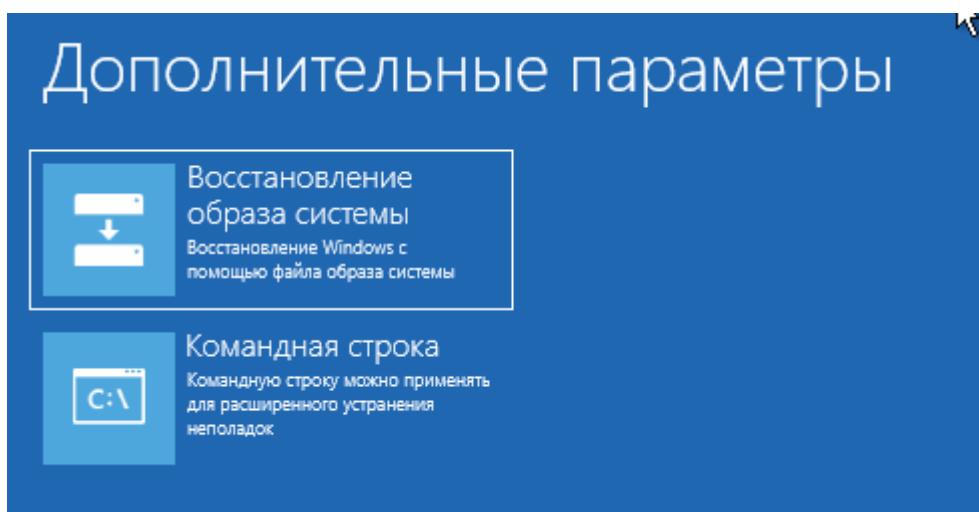
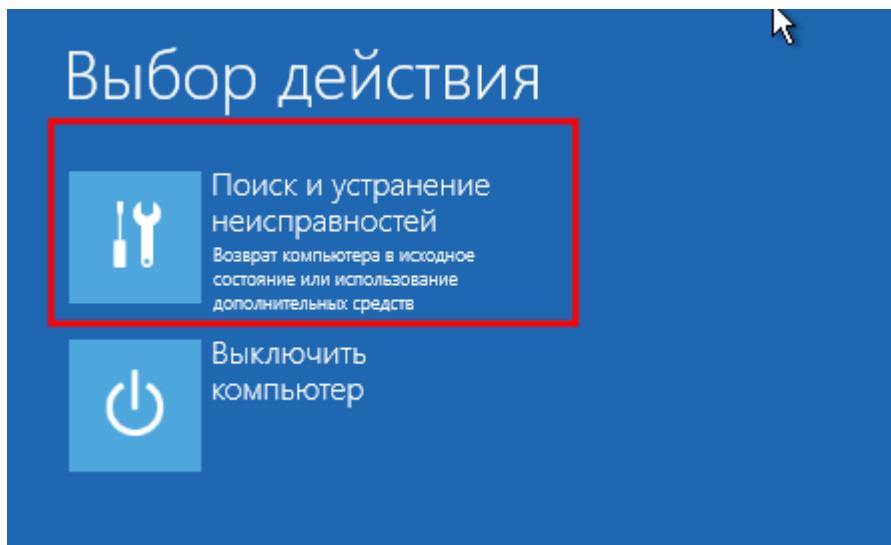
Windows (CRLF) Стр 1, столб 1 100%

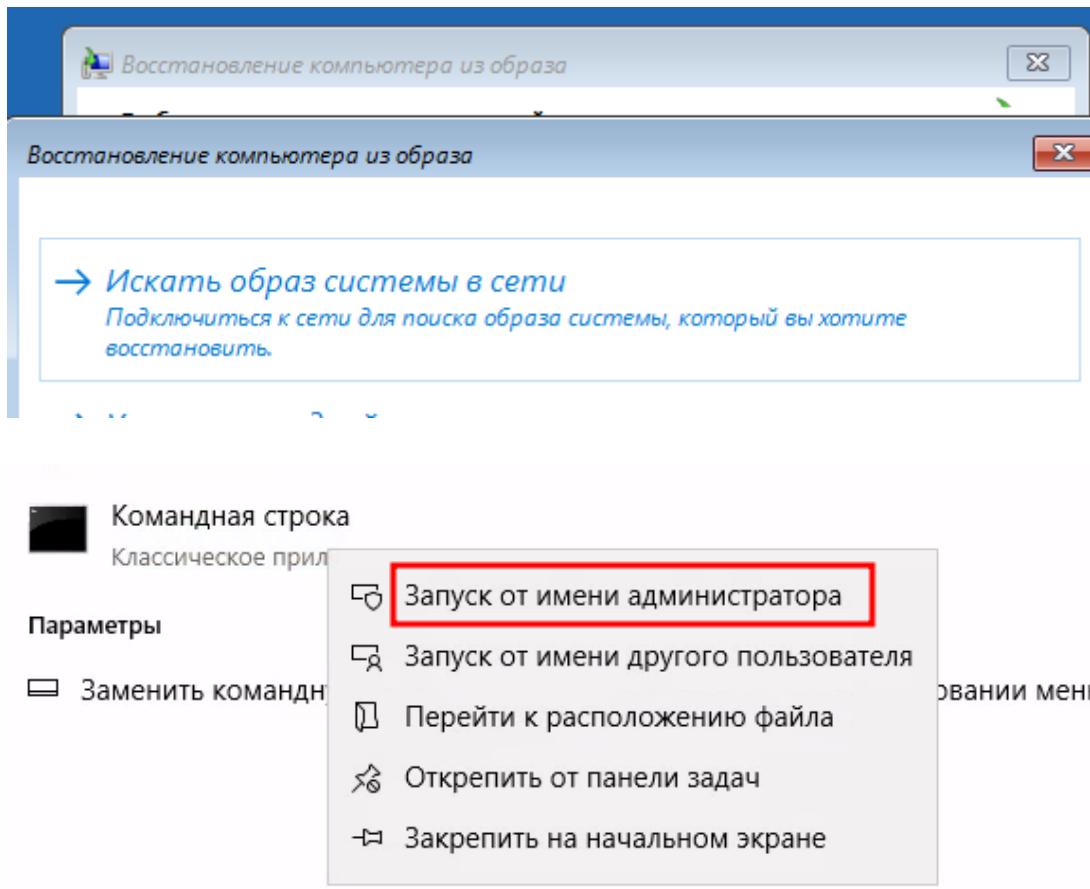


Восстановите состояние сервера используя загрузочный диск и ранее созданную резервную копию









```
C:\Users\Администратор.W2019SERV01>wbadmin
wbadmin 1.0 - программа командной строки для резервного копирования
(С) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

ОШИБКА: команда введена не полностью. См. приведенный ниже список.
Чтобы получить справку по этой команде, введите "WBADMIN <команда> /?".
```

---- 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.

```
wbadmin get version
wbadmin start backup /?
wbadmin start backup -backupTarget:g: -include:c:\backup -vsscopy
```

#удаление :0 все удаляет

```
wbadmin delete systemstatebackup -backupTarget:g: -deleteOldest -quiet  
wbadmin get versions  
wbadmin delete backup -keepversions:0
```

```
C:\Users\Администратор.W2019SERV01>wbadmin get versions  
wbadmin 1.0 - программа командной строки для резервного копирования  
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.  
  
Время архивации: 16.02.2024 12:42  
Конечный объект архивации: 1394/USB-диск с именем w2019se 2024_02_16 12:40 DISK_01(\?\Volume{2756fe76-752c-4bf3-ae3a-1ba506cbc451})  
Идентификатор версии: 02/16/2024-09:42  
Возможность восстановления: Тома, Файл(ы)  
Ид снимка: {e2074adf-c5c0-4ef8-8f9e-3f8f116f1746}
```

```
C:\Users\Администратор.W2019SERV01>wbadmin start backup /?  
wbadmin 1.0 - программа командной строки для резервного копирования  
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.  
  
ОШИБКА: синтаксическая ошибка в команде. Ошибка: /?. См. приведенный ниже  
синтаксис команды.
```

```
Синтаксис: WBADMIN START BACKUP  
[-backupTarget:{<целевой_том_архивации> | <целевая_сетевая_папка>}]  
[-include:<включаемые_элементы>  
[-nonRecurseInclude:<включаемые_элементы>]  
[-exclude:<исключаемые_элементы>]  
[-nonRecurseExclude:<исключаемые_элементы>]  
[-hyperv:<включаемые_компоненты_Hyper-V>]  
[-allCritical]  
[-systemState]  
[-noVerify]  
[-user:<имя_пользователя>]  
[-password:<пароль>]  
[-noInheritAcl]  
[-vssFull | -vssCopy]
```

```
Примеры:  
WBADMIN START BACKUP -backupTarget:f: -include:e:,  
d:\mountpoint,\?\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\  
-hyperv:vm1,{627cf8de-2967-4c39-852c-655a691d245f}
```

```
WBADMIN START BACKUP -backupTarget:f: -include:e:\*,  
d:\mountpoint\*,\?\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\  
-exclude:e:\folder\*
```

```
WBADMIN START BACKUP -backupTarget:\server\share  
-hyperv:vm1,{627cf8de-2967-4c39-852c-655a691d245f}
```

Примечания. Если требуется архивация приложений для восстановления,
то нужно архивировать весь том, содержащий приложение и данные приложения.

Создадим папку

	Имя	Дата изменения	Тип	Размер
оступ	mib.bin	15.09.2018 10:12	Файл "BIN"	43 КБ
стол	notepad	09.02.2024 16:13	Приложение	249 КБ
ы	out_process1.csv	10.02.2024 4:33	Файл "CSV"	3 КБ
зния	out_process2	10.02.2024 4:33	HTML-документ	1 КБ
й диск (C:	PFRO	10.02.2024 3:36	Текстовый докум...	4 КБ
ютер	regedit	09.02.2024 16:13	Приложение	350 КБ
	ServerStandard	15.09.2018 10:13	Документ XML	31 КБ
	splwow64	09.02.2024 16:14	Приложение	131 КБ
	system	15.09.2018 10:16	Параметры конф...	1 КБ
	test	10.02.2024 3:57	Текстовый докум...	1 КБ
	test2	10.02.2024 4:28	Текстовый докум...	1 КБ
	twain_32.dll	15.09.2018 10:13	Расширение при...	63 КБ
	win	15.09.2018 10:16	Параметры конф...	1 КБ
	WindowsUpdate	16.02.2024 11:13	Текстовый докум...	1 КБ

```
C:\Users\Администратор.W2019SERV01>wbadmin start backup -backupTarget:g: -include:c:\backup -vsscopy
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Получения сведений о томе...
Будет выполнена архивация (C:) (выбранные файлы) на g:.
Вы хотите начать операцию архивации?
[Y] – да; [N] – нет _
```

```
C:\Users\Администратор.W2019SERV01>wbadmin delete systemstatebackup -backupTarget:g: -deleteOldest -quiet
wbadmin 1.0 - программа командной строки для резервного копирования
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Перечисление архивов состояния системы...
```

```
C:\Users\Администратор.W2019SERV01>wbadmin get versions
wbadmin 1.0 - программа командной строки для резервного копирования
(С) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Время архивации: 16.02.2024 12:42
Конечный объект архивации: 1394/USB-диск с именем w2019se 2024_02_16 12:40 DISK_01(\?\Volume{2756fe76-752c-4bf3-ae3a-1ba506cbc451})
Идентификатор версии: 02/16/2024-09:42
Возможность восстановления: Тома, Файл(ы)
Ид снимка: {e2074adf-c5c0-4ef8-8f9e-3f8f116f1746}
```

```
C:\Users\Администратор.W2019SERV01>wbadmin delete backup -keepversions:0
wbadmin 1.0 - программа командной строки для резервного копирования
(С) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
```

Идет перечисление резервных копий...
Обнаружено резервных копий: 1,
останется после операции удаления: 0.
Будут удалены все резервные копии сервера в указанном
расположении.

Вы хотите удалить резервные копии?
[Y] – да; [N] – нет у

Удаление версии 02/16/2024-09:42 резервной копии (1 из 1)...
Сбой удаления версии 02/16/2024-09:42 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 у

Удаление резервных копий завершено.
Удалено резервных копий: 1

Команды:

Резервное копирование Windows с помощью Wbadmin

Утилита wbadmin.exe – это средство командной строки, которое позволяет создавать резервную копию состояния системы или создавать резервные копии отдельных дисков, каталогов (и файлов) и восстанавливать данные из такой резервной копии.

- ENABLE BACKUP – создать или изменить запланированное задание резервного копирования;
- DISABLE BACKUP – отключить автоматическое задание резервного копирования;
- START BACKUP – одноразовое задание резервного копирования;
- STOP JOB – остановить задачу резервного копирования или восстановления;
- GET VERSIONS – перечислить доступные резервные копии в указанном хранилище;
- GET ITEMS – перечислить элементы, хранящиеся в резервной копии;
- GET STATUS – отображать состояние запущенной задачи резервного копирования или восстановления;
- DELETE BACKUP – удалить резервную копию.

Дополнительно поддерживаются подкоманды wbadmin на Windows Server:

- GET DISKS
- GET VIRTUALMACHINES
- START SYSTEMSTATERECOVERY

- START SYSTEMSTATEBACKUP
- DELETE SYSTEMSTATEBACKUP

Например, вы можете создать резервную копию образа операционной системы, добавить диск F: в резервную копию и записать его на диск E:

```
wbadmin start backup -backupTarget:E: -include:F: -allCritical -quiet
```

При создании резервной копии на диске, указанном в параметре backupTarget, создается каталог WindowsImageBackup, в котором сохраняется образ резервной копии системы;

- Параметр include позволяет указать диски, которые будут включены в резервную копию образа;
- Параметр allCritical используется для того, чтобы все резервные копии, необходимые для восстановления системы (включая разделы с загрузчиком конфигурации BCD), были добавлены в резервную копию образа.

Так же можно создать архив состояния системы с помощью команды

Wbadmin start systemstatebackup

Чтобы открыть командную строку с более высоким уровнем привилегий, нажмите кнопку **Пуск**, щелкните правой кнопкой мыши **Командная строка**, а затем выберите **От имени администратора**.

В командной строке введите:

```
wbadmin start systemstatebackup -backupTarget:<имя_тома> [-quiet]
```

Например, чтобы создать архив состояния системы без вывода сообщений для пользователя и сохранить его на том F, введите:

```
wbadmin start systemstatebackup -backupTarget:F: -quiet
```

Чтобы просмотреть полный синтаксис этой команды, введите в командной строке:

```
Wbadmin start systemstatebackup /?
```

Обратите внимание, что система резервного копирования Windows основана на службе теневого копирования томов (VSS).

Утилита wbadmin создает теневую копию (снимок) указанного тома и создает резервную копию образа системы на основе этого снимка (производительность компьютера может уменьшиться во время резервного копирования).

Вы можете создать резервную копию нескольких папок и сохранить их на отдельном диске:

```
wbadmin start backup -backupTarget:e: -include:c:\docs\,c:\backup -vsscopy
```

Вы также можете сохранить резервную копию в общей сетевой папке:

```
wbadmin start backup -backupTarget:\\srv1\backup -  
include:c:\docs\,c:\backup
```

Вы можете создать задачу автоматического резервного копирования, которая будет резервировать системный образ и указанную папку или диски один раз в день:

```
wbadmin enable backup -include:c:\docs\* -addtarget:e: -allCritical -  
schedule:00:00
```

Список доступных резервных копий можно отобразить с помощью команды:
wbadmin get versions

Удалить все копии, кроме двух последних (0 – удалить все резервные копии):
wbadmin delete systemstatebackup -keepversions:2

Вы можете удалить только самую старую резервную копию:

```
wbadmin delete systemstatebackup -backupTarget:e: -deleteOldest -quiet
```

Восстановление (восстановление папки folder на диске D со всеми вложенными папками)

```
wbadmin start recovery -version:03/31/2020-09:00 -itemType:File -  
items:d:\folder -recursive
```

Дополнительно:

Глоссарий

Дополнительные материалы

Используемые источники

*Выполнил: AndreiM