

Дворников Д. С., Костионова М. А.

РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия

ВЕРИФИКАЦИЯ МЕХАНИЗМОВ УСТОЙЧИВОСТИ ДОМЕННЫХ GPO В КОРПОРАТИВНОЙ СЕТИ

Аннотация. В статье разобрано применение одного пользовательского параметра `DisableTaskMgr` в лабораторной доменной среде Windows Active Directory. Стенд включает контроллер домена Windows Server 2022 и клиентскую машину Windows 11. Цель работы состоит в сопоставлении значения реестра и поведения диспетчера задач после применения доменной GPO, локальных изменений и отключения связи с контроллером домена. Политика привязана к заданной организационной единице; проверяется конкретная учётная запись пользователя. Представлены команды обновления политики, сведения о её применении и попытки изменения контролируемого значения. Рассмотрены действия обычного пользователя и локального администратора, а также активная сессия без сети и вход с кэшированными учётными данными после перезагрузки. В показанных сценариях доменное ограничение применялось, а после локального изменения администратором восстанавливалось при штатном обновлении политики. При отсутствии сети ранее применённое значение сохранялось; попытка обычного пользователя записать другое значение завершилась отказом доступа. Дескрипторы безопасности реестра и внутренний механизм сохранения значения отдельно не исследовались. Сценарии Block Inheritance и Enforced, все этапы модели LSDOU и другие способы обхода GPO не проверялись. Результаты ограничены одним параметром, выбранной OU, привязанной политикой и указанной конфигурацией. Материал может использоваться как учебный пример применения и восстановления доменной настройки. Он показывает необходимость различать наблюдаемое поведение отдельного параметра и общую оценку устойчивости централизованного управления. Выводы не характеризуют все версии Windows, доменные архитектуры или условия физического доступа.

Ключевые слова: Windows, Active Directory, GPO, групповые политики, LSDOU, информационная безопасность, доменная инфраструктура.

Введение

В современных корпоративных сетях управление конфигурацией рабочих станций и серверов является фундаментальной задачей системных администраторов. Групповые политики Windows (Group Policy Objects, GPO) представляют собой мощный инструмент централизованного управления настройками операционной системы, приложений и параметров безопасности в среде Microsoft Active Directory. С их помощью администраторы устанавливают единые требования к парольной политике, настройкам брандмауэра, параметрам аудита и ограничениям для пользователей.

Иерархическая модель применения GPO (LSDOU: Local — Site — Domain — Organizational Unit) позволяет задавать настройки на нескольких уровнях. При совпадении параметров возможны конфликты, которые разрешаются правилами обработки политик. Механизмы Enforced и Block Inheritance дополнительно изменяют наследование и требуют проверки результирующего набора настроек; сами по себе они не являются способами обхода ограничений.

Проблематика обхода групповых политик исследуется специалистами по информационной безопасности в контексте атак на инфраструктуру Active Directory. В частности, актуальным остаётся вопрос о практической возможности локального переопределения доменных политик с использованием инструментов Windows, как со стороны обычного пользователя, так и со стороны локального администратора клиентской машины.

Объект исследования — механизм применения объектов групповой политики в инфраструктуре Windows Active Directory.

Предмет исследования — изменение одного параметра `DisableTaskMgr` при применении доменной GPO, локальном вмешательстве и отсутствии связи с контроллером домена.

Цель исследования — описать применение и восстановление `DisableTaskMgr` в одном доменном стенде Windows Server 2022 и Windows 11. Исследование не охватывает все параметры GPO или способы обхода политик.

Литературный обзор

Модель обработки и приоритизации GPO детально описана в профессиональной литературе. Krause указывает, что политики применяются в строгой последовательности LSDOU, при этом каждый последующий уровень иерархии — Domain, затем Organizational Unit — перекрывает настройки предыдущего уровня в случае конфликта параметров [1]. Данная модель предполагает, что параметры, заданные в GPO уровня домена, в случае конфликта перекрывают параметры локальной политики, а параметры GPO подразделения (OU) перекрывают доменные.

Порядок применения групповых политик и особенности диагностики описаны в специализированной литературе [2]. Для проверки того, какие объекты были применены к конкретному пользователю и компьютеру, используются gpresult и RSoP. Приоритет результирующей настройки зависит от области действия GPO, порядка обработки и параметров наследования.

Портал Инфратех в обзорном руководстве по доменным политикам отмечает, что локальные объекты групповой политики (LGPO) разделены на несколько уровней — для локального компьютера, для всех пользователей и для конкретных учётных записей, — что значительно усложняет анализ итогового результирующего набора политик [3]. На основании проведённого анализа и практического моделирования были сформулированы следующие исследовательские гипотезы:

H1: В заданной OU/GPO доменное значение DisableTaskMgr применяется к проверенной учётной записи при обновлении политики.

H2: Обычная пользовательская учётная запись не может устойчиво изменить проверенный параметр при регулярном обновлении доменной политики.

H3: Локальный администратор может временно изменить DisableTaskMgr в HKU\SID; при следующем штатном обновлении GPO доменное значение восстанавливается.

H4: В проверенной пользовательской сессии без связи с контроллером домена и после кэшированного входа сохранится ранее применённое значение DisableTaskMgr.

Внутренний механизм сохранения значения отдельно не проверяется.

Материалы и методы

Работа представляет прикладной лабораторный разбор одного параметра GPO. Описываются штатное применение доменной настройки, попытки локального изменения обычным пользователем и администратором, а также наблюдение без связи с контроллером домена.

Характеристика тестовой среды: в качестве программной платформы использовались Windows Server 2022 (в роли контроллера домена) и Windows 11 с актуальными обновлениями (в роли клиентской рабочей станции). В инфраструктуре были задействованы службы Active Directory Domain Services и DNS. Для проведения экспериментов была создана тестовая организационная единица (OU) и стандартная доменная учётная запись пользователя. Исследование проводилось в изолированной виртуальной среде.

Данные получены из показанных команд gpupdate, gpresult, обращений к реестру и поведения диспетчера задач. Отслеживается DisableTaskMgr в выбранной OU/GPO. Сценарии Block Inheritance, Enforced и полный анализ RSoP в представленных результатах не выполнены.

Описание процедуры проведения исследования: Исследование проводилось в лабораторной среде с развёрнутым доменом Active Directory и подключённой клиентской станцией. После проверки аутентификации была создана тестовая OU и доменная учётная запись пользователя, на которой оценивалось применение политик.

Затем создавался объект групповой политики с заданным пользовательским ограничением и привязывался к OU. После обновления конфигурации фиксировались групповые политики.

После локальных изменений повторно выполнялось обновление политики и проверялось значение DisableTaskMgr. Проверка ограничена выбранной учётной записью, привязанной GPO и показанными командами.

Дополнительно был проведён третий эксперимент, моделирующий сценарий атаки с использованием локальной учётной записи администратора клиентской машины. Для этого на клиентской рабочей станции была активирована встроенная локальная учётная запись администратора средствами командной строки. От её имени предпринималась попытка непосредственного изменения параметра реестра в профиле доменного пользователя через ветку HKU\SID. После внесения изменений выполнялась принудительная синхронизация политик, по результатам которой фиксировалось итоговое состояние контролируемого параметра.

В рамках четвёртого эксперимента был смоделирован сценарий потери клиентской машиной связи с контроллером домена. Сетевой адаптер клиентской рабочей станции был отключён средствами гипервизора при активной пользовательской сессии. В условиях отсутствия сетевого подключения проверялось текущее состояние контролируемого параметра, предпринималась попытка его изменения, после чего выполнялась перезагрузка машины с входом через кэшированные учётные данные. На каждом этапе фиксировалось состояние параметра реестра и фактическое поведение системы. После восстановления сетевого подключения выполнялась принудительная синхронизация политик и проводилась финальная проверка конфигурации.

Обработка данных — сопоставление показанного значения DisableTaskMgr и поведения диспетчера задач в четырёх выбранных сценариях. Таблица результатов отражает этот параметр и конфигурацию, а не полную верификацию модели LSDOU.

Ход исследования

После развертывания тестовой инфраструктуры и включения клиентской рабочей станции в домен была создана организационная единица и тестовая пользовательская учётная запись, на которой проводилась проверка настроек. На первом этапе была создана доменная групповая политика, задающая конкретное пользовательское ограничение. После её привязки к соответствующей OU на клиентской машине выполнялось принудительное обновление политик, затем фиксировались применённые GPO и фактическое состояние исследуемого параметра. Полученные результаты сопоставлялись с ожидаемой моделью приоритета в рамках LSDOU. Настройка объекта в оснастке управления показана на рис. 1.

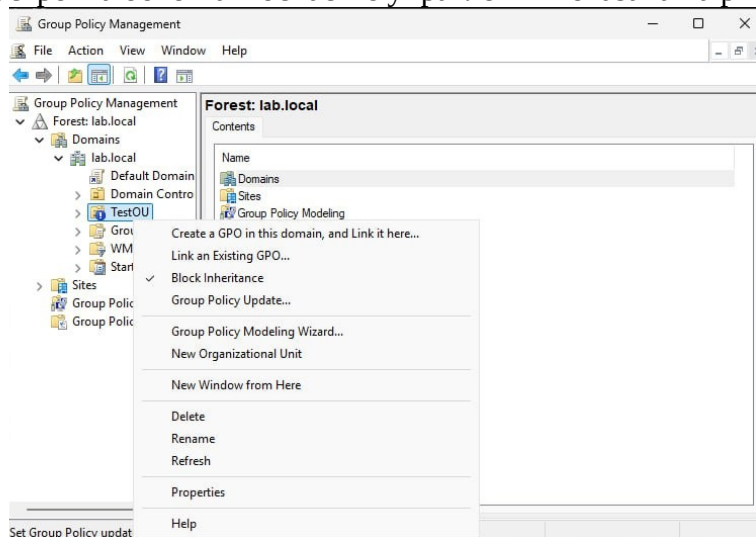


Рис. 1. Выбор команды создания и привязки GPO в оснастке Group Policy Management

После локальных изменений повторно инициировалось обновление GPO и проверялось значение DisableTaskMgr. Наблюдения позволяют сопоставить результаты конкретных попыток, но не доказывают устойчивость всех политик или невозможность других способов вмешательства. Значение параметра в редакторе реестра представлено на рис. 2.

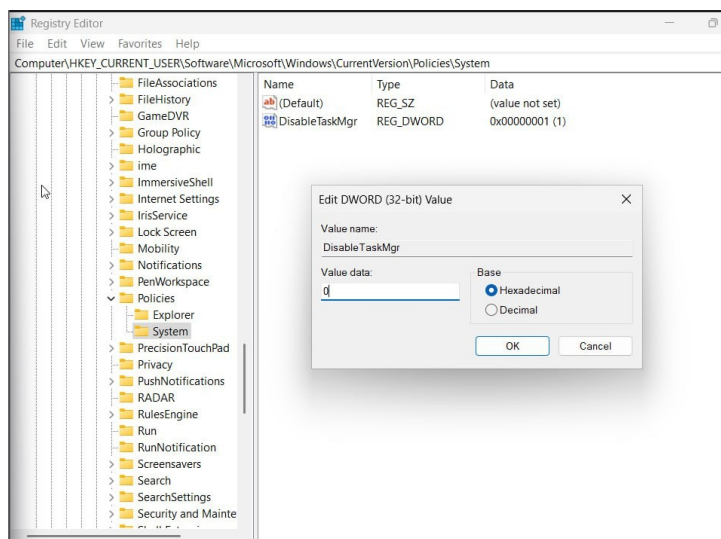


Рис. 2. Параметр DisableTaskMgr в редакторе реестра Windows

На третьем этапе был смоделирован сценарий, при котором потенциальный злоумышленник располагает правами локального администратора клиентской машины, однако не имеет привилегий в домене. Встроенная локальная учётная запись администратора была активирована штатными средствами Windows. После входа в систему под данной учётной записью был получен идентификатор безопасности (SID) доменной учётной записи testuser с помощью PowerShell, что позволило обратиться к ветке реестра HKU\SID, соответствующей профилю целевого пользователя. Попытка изменения параметра DisableTaskMgr с значения 1 на 0 завершилась успешно, и операция была выполнена без каких-либо ошибок доступа. После изменения параметра проверялся запуск диспетчера задач (рис. 3).

Листинг 1 – Получение SID и изменение параметра DisableTaskMgr в профиле пользователя

```
PS C:\WINDOWS\System32> (New-Object
System.Security.Principal.NTAccount('lab.local','testuser')).Translate([System.S
ecurity.Principal.SecurityIdentifier]).Value
S-1-5-21-2328540634-355861150-2537366535-1104
PS C:\WINDOWS\System32> reg query "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System"
DisableTaskMgr REG_DWORD 0x1
PS C:\WINDOWS\System32> reg add "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr /t REG_DWORD /d 0 /f
The operation completed successfully.
```

Листинг 2 – Проверка изменения параметра реестра

```
PS C:\WINDOWS\System32> reg query "HKU\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
HKEY_USERS\S-1-5-21-2328540634-355861150-2537366535-
1104\Software\Microsoft\Windows\CurrentVersion\Policies\System
DisableTaskMgr REG_DWORD 0x0
```

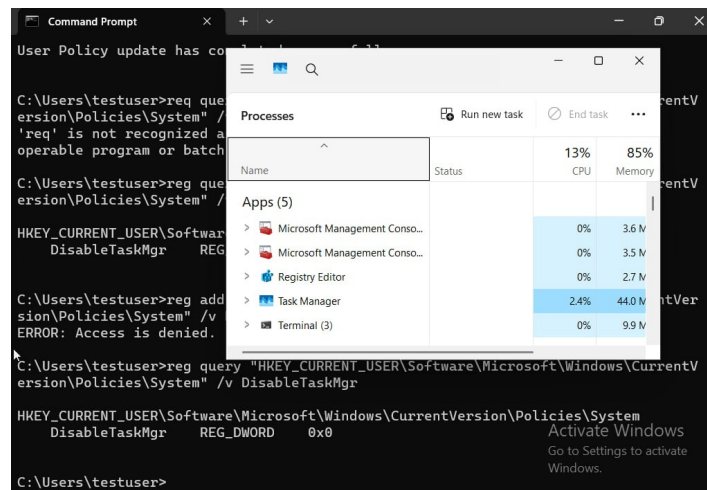


Рис. 3. Запуск диспетчера задач после локального изменения DisableTaskMgr

После этого сессия локального администратора была завершена, выполнен вход под учётной записью testuser и инициировано принудительное обновление групповых политик командой `gpupdate /force`. По результатам синхронизации значение параметра `DisableTaskMgr` вернулось к исходному значению 1, а диспетчер задач вновь оказался недоступен. Проверка через `gpresult` подтвердила, что политика `Domain-GPO-Test` присутствует в списке применённых объектов групповой политики.

Листинг 3 – Проверка восстановления параметра после `gpupdate /force`

```

C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr REG_DWORD 0x0
C:\Users\testuser> gpupdate /force
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr REG_DWORD 0x1
Task Manager has been disabled by your administrator.

```

На четвёртом этапе был смоделирован сценарий, при котором клиентская машина теряет связь с контроллером домена — например, в случае отключения от корпоративной сети. Сетевой адаптер был отключён средствами гипервизора без завершения пользовательской сессии. Попытка принудительного обновления политик командой `gpupdate /force` завершилась ошибкой — контроллер домена оказался недоступен. Тем не менее проверка параметра реестра показала сохранение значения `DisableTaskMgr = 1`, а попытка его изменения от имени testuser завершилась ошибкой доступа — аналогично поведению системы в онлайн-режиме.

Листинг 4 – Ошибка обновления групповой политики без связи с контроллером домена

```

The processing of Group Policy failed because of lack of network connectivity to
a domain controller.
User Policy could not be updated successfully.
Task Manager has been disabled by your administrator.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr REG_DWORD 0x1

```

После перезагрузки без сети выполнен вход с кэшированными учётными данными; `DisableTaskMgr` оставался равным 1 и диспетчер задач не запускался. Это наблюдение показывает сохранение ограничения в выбранном сценарии, но не устанавливает его внутреннюю причину или свойства ACL реестра. После восстановления сети `Computer Policy` и `User Policy` обновились успешно; значение подтверждено как 0x1.

Листинг 5 – Успешное обновление политик после восстановления связи

```
Ping statistics for 192.168.10.1: Packets: Sent = 3, Received = 3, Lost = 0 (0% loss).
C:\Users\testuser> gpupdate /force
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\testuser> reg query
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
DisableTaskMgr
DisableTaskMgr      REG_DWORD      0x1
```

Результаты исследования

В листинге 6 показан результат применения доменной групповой политики к пользователю testuser. В окне командной строки отображается список применённых объектов групповой политики, среди которых указана политика Domain-GPO-Test. При попытке запуска диспетчера задач появляется сообщение о том, что он отключён администратором, что подтверждает корректное применение настроек политики.

Листинг 6 – Результат gresult для пользователя testuser

```
USER SETTINGS
Applied Group Policy Objects:
    Domain-GPO-Test
    Local Group Policy
Task Manager has been disabled by your administrator.
```

На рис. 4 показана попытка изменения DisableTaskMgr в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System. Операция завершается сообщением об отказе в записи. Это подтверждает невозможность изменения значения выбранной учётной записью в показанной конфигурации; дескриптор безопасности ключа и причина отказа отдельно не исследовались.

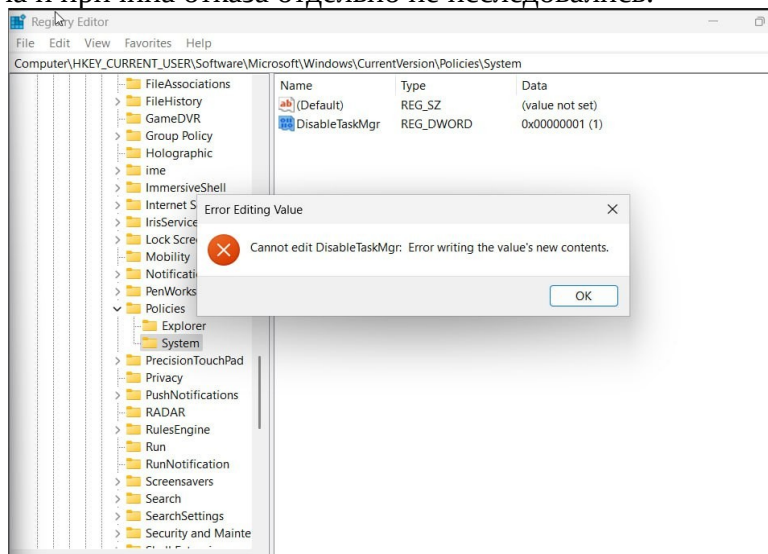


Рис. 4. Сообщение об отказе при попытке изменения DisableTaskMgr

Третий эксперимент показал, что локальная учётная запись администратора клиентской машины обладает достаточными правами для непосредственного изменения параметров реестра в профиле доменного пользователя. В отличие от попытки обычного пользователя, завершившейся ошибкой доступа, операция записи от имени локального администратора была выполнена успешно. Тем не менее данный обход носит временный характер, поскольку принудительное обновление групповой политики восстановило значение DisableTaskMgr (см. листинг 3).

В четвёртом сценарии значение DisableTaskMgr сохранялось как в активной пользовательской сессии без сети, так и после перезагрузки с кэшированным входом. Попытка записи от имени обычного пользователя завершилась отказом доступа. Это наблюдение относится к испытанной конфигурации и не подтверждает устойчивость ко всем способам локального вмешательства. Результаты четырёх экспериментов обобщены в табл. 1.

Таблица 1 – Результаты проверки доменной GPO в четырёх сценариях

№	Цель эксперимента	Действия	Наблюдаемый результат	Вывод
1	Применение доменной GPO	Привязка GPO к OU; gpupdate /force; запуск диспетчера задач	Диспетчер задач заблокирован; GPO отображается среди применённых.	В заданной OU/GPO параметр DisableTaskMgr применён к проверенной учётной записи.
2	Изменение пользователем	Попытка изменить DisableTaskMgr; повторное обновление политики	Отказ в изменении; ограничение сохраняется.	Пользователь не смог изменить значение в этой конфигурации; другие способы не проверялись.
3	Локальный администратор	Изменение реестра через HKU\SID; gpupdate /force	После обновления значение вновь равно 1.	Временное изменение было устранено штатным обновлением доменной GPO.
4	Отсутствие связи с контроллером	Отключение сети; gpupdate /force; попытка записи; кэшированный вход	Обновление GPO не выполнено; отказ в записи; ограничение сохранилось.	Сохранение DisableTaskMgr подтверждено только для данного offline-сценария.

Заключение

На стенде проверены применение доменной GPO, конфликты локальных настроек, действия локального администратора и работа без сети. Показанные наблюдения относятся к используемым Windows Server 2022 и Windows 11. Выводы по четырём гипотезам приведены ниже.

Следует также отметить, что требования к управлению конфигурацией корпоративных информационных систем и средствам защиты информации закреплены в нормативных документах ФСТЭК России [4], что дополнительно подчёркивает практическую и регуляторную значимость механизмов централизованного администрирования на основе GPO в отечественных корпоративных средах.

Результат проверки гипотез:

1. В проверенном сценарии доменная настройка DisableTaskMgr применялась к учётной записи при заданной OU и привязанной GPO. Наблюдение подтверждает гипотезу Н1 для этого параметра и конфигурации, но не проверяет все этапы и исключения модели LSDOU.
2. Гипотеза Н2 также получила подтверждение. Попытка локального изменения контролируемого параметра через реестр не привела к изменению конфигурации, а повторная синхронизация политик сохранила установленное ограничение. Это свидетельствует о приоритетности доменной GPO над локальными настройками и её устойчивости к пользовательскому вмешательству в пределах стандартных прав доступа.
3. Гипотеза Н3 подтвердилась в рамках проверенного сценария: локальный администратор изменил DisableTaskMgr в профиле доменного пользователя, после чего штатное обновление политики восстановило прежнее значение. Возможность других способов изменения или отключения механизмов обработки GPO в работе не проверялась.
4. Гипотеза Н4 подтверждается в пределах наблюдения: ранее применённое значение сохранилось в показанном offline-сценарии. Действие ACL реестра, иные способы локального вмешательства и физический доступ к машине не исследовались; результат не является общей оценкой защиты без сети.

Перспективы дальнейшего исследования связаны с проверкой нескольких GPO, порядка их обработки и механизмов Enforced и Block Inheritance, а также с оценкой различных уровней прав доступа в более сложной структуре OU.

В описанном стенде встроенные средства Windows позволили применить и восстановить доменное значение DisableTaskMgr. Это не исчерпывающая проверка контроля всех

параметров клиентских систем. Стенд может использоваться как учебный пример применения GPO и отдельных конфликтов доменного и локального значений. Для последующих проверок доступны обзор групповых политик Microsoft [5], документация LGPO.exe [6] и Get-GPResultantSetOfPolicy [7]; эти средства не применялись в описанных опытах.

Библиографический список

17. Krause, J. *Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy* / J. Krause. – Birmingham : Packt Publishing, 2018. – 390 p. – Текст : непосредственный.
18. Arya, K. *Windows Group Policy Troubleshooting: A Best Practice Guide for Managing Users and PCs Through Group Policy* / K. Arya. – Apress, 2016. – 200 p. – Текст : непосредственный.
19. Доменные политики и GPO в Active Directory: полное руководство по настройке и безопасности [Электронный ресурс] // Корпоративный блог Инфратех. – URL: <https://blog.infra-tech.ru/domennye-politiki/> (дата обращения: 20.02.2026). – Текст : электронный.
20. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 № 17 [Электронный ресурс]. – URL: https://rppa.pro/npa/fstek17_11.02.2013 (дата обращения: 21.02.2026). – Текст : электронный.
21. Group Policy Overview [Электронный ресурс] // Microsoft Learn. – URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview> (дата обращения: 21.02.2026). – Текст : электронный.
22. LGPO.exe — Local Group Policy Object Utility [Электронный ресурс] // Microsoft Security. – URL: <https://www.microsoft.com/en-us/download/details.aspx?id=55319> (дата обращения: 17.02.2026). – Текст : электронный.
23. Get-GPResultantSetOfPolicy [Электронный ресурс] // Microsoft Learn. – URL: <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpresultantsetofpolicy> (дата обращения: 17.02.2026). – Текст : электронный.

References

24. Krause, J. (2018). *Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy*. Packt Publishing.
25. Arya, K. (2016). *Windows Group Policy troubleshooting: A best practice guide for managing users and PCs through Group Policy*. Apress.
26. Infratech Corporate Blog. (n.d.). *Domennye politiki i GPO v Active Directory: Polnoe rukovodstvo po nastroyke i bezopasnosti* [Domain policies and GPO in Active Directory: A complete guide to configuration and security]. <https://blog.infra-tech.ru/domennye-politiki/>
27. Federal Service for Technical and Export Control of Russia. (2013). *Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, sodержashchey v gosudarstvennykh informatsionnykh sistemakh* [On approval of requirements for the protection of information in state information systems] (Order No. 17). https://rppa.pro/npa/fstek17_11.02.2013
28. Microsoft. (n.d.). *Group Policy overview*. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>
29. Microsoft. (n.d.). *LGPO.exe: Local Group Policy Object utility*. Microsoft Security. <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
30. Microsoft. (n.d.). *Get-GPResultantSetOfPolicy*. Microsoft Learn. <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpresultantsetofpolicy>

Информация об авторах

Дворников Дмитрий Сергеевич — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва; e-mail: dmitriidvo@gmail.com

Костионова Мария Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва; e-mail: maria.kowela@gmail.com

VERIFICATION OF DOMAIN GPO STABILITY MECHANISMS IN A CORPORATE NETWORK

Dvornikov D. S., Kostionova M. A.

Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. *This paper examines one user setting, DisableTaskMgr, on a Windows Active Directory laboratory testbed. The testbed includes a Windows Server 2022 domain controller and a Windows 11 client. The aim is to compare the registry value and Task Manager behavior after applying a domain GPO, attempting local changes, and disconnecting the client from the domain controller. The policy is linked to a specified organizational unit and tested with one user account. The article presents policy-update commands, reported policy application, and attempts to modify the controlled value. It considers an ordinary user, a local administrator, an active session without network connectivity, and a cached sign-in after reboot. In the displayed scenarios, the domain restriction was applied and restored by a normal policy update after an administrator changed the local value. Without connectivity, the previously applied value persisted; the ordinary user could not write a different value. Registry security descriptors and the internal persistence mechanism were not separately examined. Block Inheritance, Enforced, the complete LSDOU model, and other bypass methods were not tested. Results concern one setting, organizational unit, policy, and configuration. The material is a teaching example of applying and restoring a domain setting. It distinguishes observed parameter behavior from a general assessment of centralized-management security and does not characterize all Windows versions or physical-access scenarios.*

Keywords: *Windows, Active Directory, GPO, Group Policy, LSDOU, information security, domain infrastructure.*

Information about the authors

Dvornikov Dmitriy Sergeevich — third-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow; e-mail: dmitriidvo@gmail.com

Kostionova Maria Aleksandrovna — third-year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow; e-mail: maria.kowela@gmail.com