Оглавление

[Документ 1](#_Toc191968787)

[Список 10-и критичных проверок 2](#_Toc191968788)

[Почему именно эти проверки 3](#_Toc191968789)

[Команды для проверки (PowerShell) 5](#_Toc191968790)

# Документ

**CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0** — это набор рекомендаций по безопасности, разработанный **Center for Internet Security (CIS)** для операционной системы **Windows 11 Enterprise**. Документ содержит подробные инструкции по настройке системы для повышения её защищённости от киберугроз.

Оно включает рекомендации по:

* **Настройке групповых политик** (GPO)
* **Ограничению прав пользователей**
* **Конфигурации брандмауэра и антивируса**
* **Шифрованию и управлению учетными записями**
* **Аудиту и журналированию событий**

Каждая рекомендация включает:

* **Описание**: что именно настраивается.
* **Рекомендуемое значение**: какое значение параметра считается безопасным.
* **Обоснование**: почему это важно.
* **Процедура аудита**: как проверить текущее состояние.
* **Процедура исправления**: как применить рекомендуемые настройки.
* **Возможное влияние**: какие последствия могут быть от изменения настроек.

**Профили безопасности**:

**Level 1 (L1)**: базовые настройки.

**Level 2 (L2)**: повышенная безопасность для организаций с высокими требованиями.

# Список 10-и критичных проверок

Выбранные проверки связаны со следующими направлениями:

* **защита учетных данных**
* **контроль доступа**
* **сетевая безопасность**
* **защита от вредоносного ПО**

**При выборе опирался на наиболее очевидные ситуации и случаи угроз (о чем слышал, с чем сталкивался, про что приходилось читать). Ознакомился со структурой документа и выбрал некоторые проверки из различных разделов. Цветом выделил ключевые слова, за которые «зацепился» при поиске и подборе проверок (использовал интернет для подбора направлений поиска, а также нейронки для подробного описания каждой проверки и помощи в составлении команд для автоматизации проверок, за основу брал указанные в тексте документа поля Audit и Remediation)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Проверка** | **Раздел** | **Уровень** | **Страница** |
| 1 | LSA Protection  Защита учетных данных | Account Policies | Level 1 | 748-749 |
| 2 | Порог блокировки учётной записи | Account Policies | Level 1 | 55-56 |
| 3 | Включение контроля учетных записей (UAC) | User Account Control | Level 1 | 279-280 |
| 4 | Доступ к Credential Manager | User Rights Assigment | Level 1 | 63-64 |
| 5 | Ограничение анонимного доступа к Named Pipes и Shares | Network Security | Level 1 | 234-236 |
| 6 | Включение Windows Defender SmartScreen | Malware Defenses | Level 1 | 1183-1185 |
| 7 | Включение аудита входа в систему | Audit Policy | Level 1 | 455-456 |
| 8 | Ограничение RDP-доступа (Network Level Authentication) | Remote Access | Level 1 | 1126-1127 |
| 9 | Отключение SMBv1 | Network Security | Level 1 | 516-517 |
| 10 | Отключение гостевой учётной записи | Security Options | Level 1 | 146-147 |

# **Почему именно эти проверки**

**1. LSA Protection – Защита учетных данных**

*18.9.26.2 (L1) Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock'*

Защищает процесс **LSASS**, который управляет паролями и учетными данными.  
**-** Без защиты злоумышленники могут украсть пароли с помощью атак.

**2. Порог блокировки учетной записи – Защита от подбора паролей**

*1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer*

*invalid logon attempt(s), but not 0'*

Автоматически блокирует учетную запись после **5 неудачных попыток входа**.  
**-** Предотвращает **брутфорс-атаки.**

**3. Включение контроля учетных записей (UAC) – Предотвращение запуска вредоносных программ**

*2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)*

Требует подтверждения перед выполнением действий с правами администратора.  
**-** Предотвращает запуск программ с правами администратора.

**4. Доступ к Credential Manager – Защита хранилища паролей**

*2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'*

Запрещает программам обращаться к хранилищу учетных данных.  
**-** Credential Manager может использоваться для **кражи паролей, сохраненных в системе.**

**5. Ограничение анонимного доступа к Named Pipes и Shares – Защита от сетевых атак**

*2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'*

Запрещает анонимным пользователям получать доступ к общим папкам и Named Pipes, также о**граничивает возможность злоумышленников получать информацию о системе (например, список пользователей, групп, общих ресурсов).**

**6. Включение Windows Defender SmartScreen – Защита от вредоносных сайтов и файлов**

*18.10.75.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'*

Проверяет загружаемые файлы и предупреждает о подозрительных сайтах.  
**-** Блокирует **фишинговые атаки** и загрузку вредоносного ПО.

**7. Включение аудита входа в систему – Мониторинг попыток входа**

*17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)*

Записывает в журнал успешные и неудачные попытки входа.  
**-** Позволяет выявить **взлом учетных записей или подозрительную активность.**

**8. Ограничение RDP-доступа (Network Level Authentication) – Защита удаленного доступа**

*18.10.56.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)*

Требует предварительной аутентификации перед установкой RDP-сессии.

**9. Отключение SMBv1 – Предотвращение атак через устаревший протокол**

*18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)*

Отключает старый протокол SMBv1, который использовался в атаках **WannaCry**.  
**-** SMBv1 **имеет критические уязвимости**.

**10. Отключение гостевой учётной записи (2.3.1.2)**

*2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (Automated)*

**Отключает гостевую учётную запись.**

**- Гостевые учётные записи часто используются злоумышленниками для получения доступа.**

# Команды для проверки (**PowerShell)**

**1. LSA Protection (Configures LSASS to run as a protected process)**

(Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa").RunAsPPL

**Ожидаемое значение:** 1 (Включено)

**2. 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'**

Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "LockoutThreshold" | Select-Object -ExpandProperty LockoutThreshold

**Ожидаемое значение**: 5 или меньше.

**3. User Account Control (UAC): Admin Approval Mode**

(Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System").EnableLUA

**Ожидаемое значение:** 1 (Включено)

**4. 2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'**

secedit /export /cfg C:\secpol.cfg

Select-String -Path C:\secpol.cfg -Pattern "SeTrustedCredManAccessPrivilege"

**Ожидаемое значение**: Пустая строка или отсутствие значений.

**5. Ограничение анонимного доступа к Named Pipes и Shares**

(Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa").RestrictAnonymous

**Ожидаемое значение:** 1 или 2 (Ограничено)

**6. Windows Defender SmartScreen**

(Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer").SmartScreenEnabled

**Ожидаемое значение:** RequireAdmin или Warn (Включено)

**7. Аудит входа в систему (Audit logon events)**

auditpol /get /category:"Logon/Logoff"

**Ожидаемое значение:** Success and Failure (Включен для обоих)

**8. Network Level Authentication (NLA) для RDP**

(Get-WmiObject -Class "Win32\_TerminalServiceSetting" -Namespace "root\CIMV2\TerminalServices").UserAuthenticationRequired

**Ожидаемое значение:** 1 (Включено)

**9. Отключение SMBv1 (Configure SMB v1 server)**

Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol

**Ожидаемое значение:** False (Отключено)

**10. 2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'**

Get-LocalUser -Name "Guest" | Select-Object -ExpandProperty Enabled

**Ожидаемое значение**: False (учётная запись отключена).