?????????? ?? ????????? ???????????????? « ?????????? ??????? ? ???????» (KICS for Nodes 4.0) ? «???????? ??????????? ???????» (KICS for Nodes 4.5)

В данной статье рассмотрены возможности решения KICS for Nodes по отслеживанию и блокированию изменений, вносимых в системный реестр операционных систем семейства Windows (на примере ОС Windows 7 и Windows 10).

В ходе развития атаки на уровне рабочей станции нарушителю приходится изменять отдельные настройки действующей системы, что влечёт за собой изменение отдельных ключей системного реестра. Поэтому важной составляющей процесса организации защиты конечных узлов под управлением ОС Windows является отслеживание (а в отдельных случаях — блокирование) таких изменений.

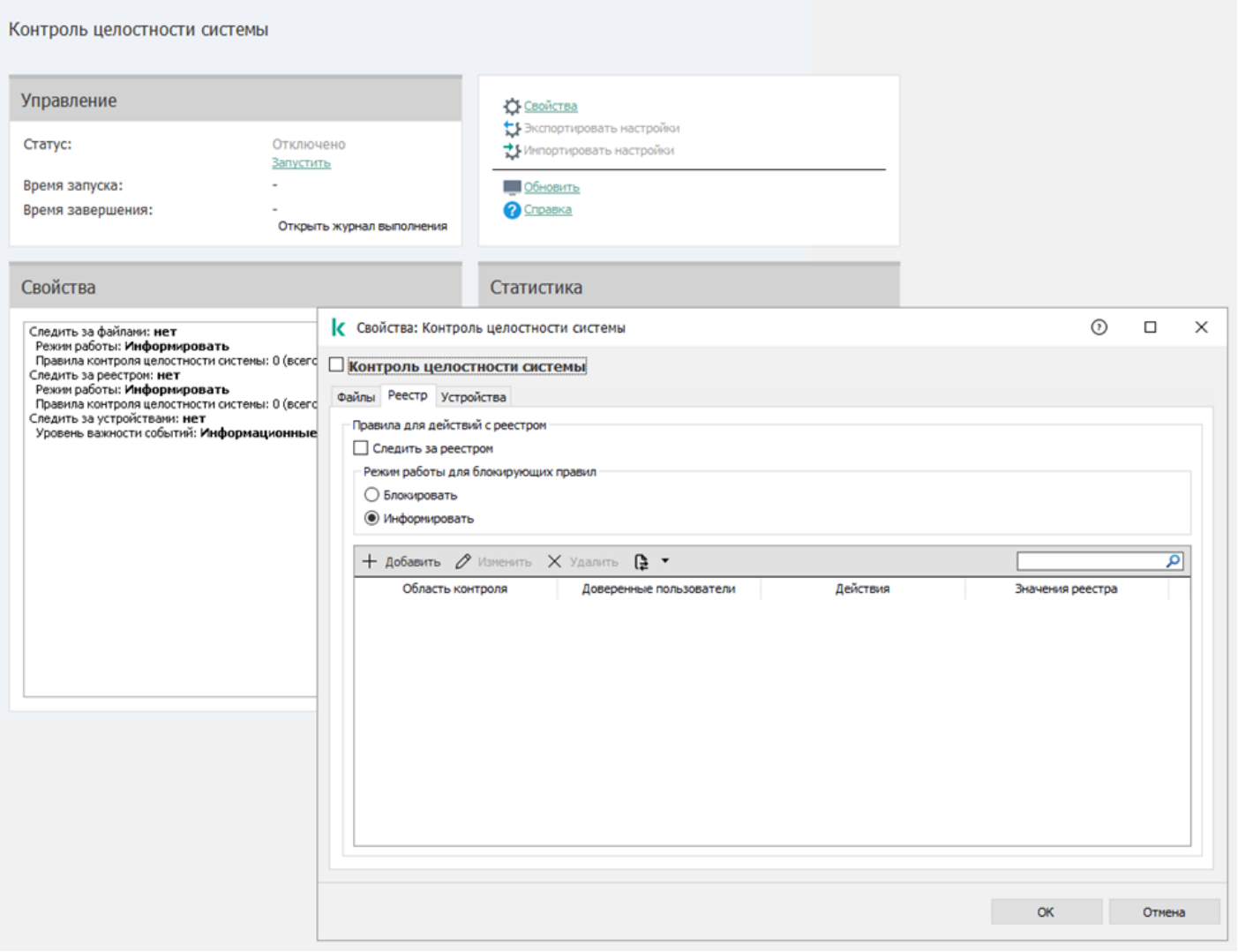
Решение KICS for Nodes позволяет контролировать выбранные значения ключей системного реестра ОС Windows и мгновенно информировать администратора информационной безопасности о внесении изменений в соответствующие настройки. Данный инструмент позволяет выявить на ранней стадии следующие нарушения в системе:

- действия нарушителя в рамках развития атаки на систему;
- попытки системного администратора внести в систему «более удобные» настройки, тем самым снизив её защищённость;
- ошибки в конфигурации операционной системы.

Результат фиксации попытки нарушения может выражаться как в уведомлении администратора ИБ о нарушении, так и в блокировке попытки внесения изменений по выбранным ключам реестра — в зависимости от выбранного режима реагирования («Информировать» / «Блокировать»).

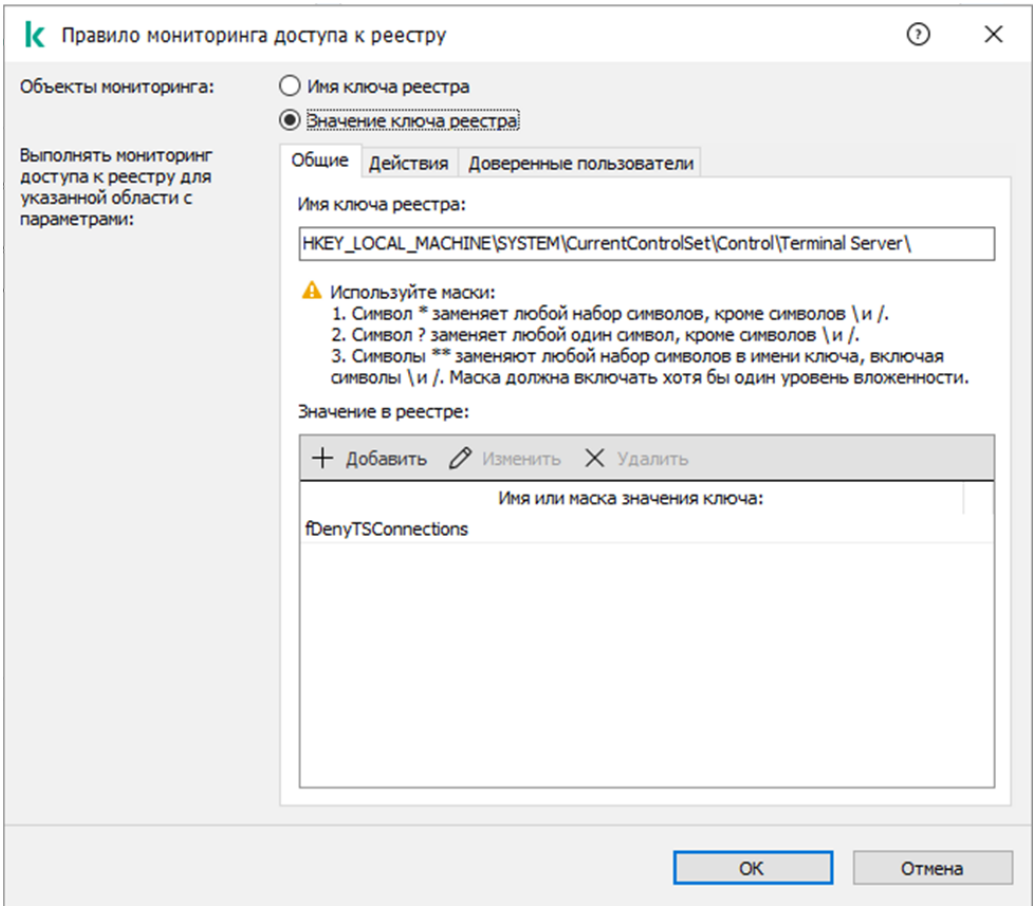
Рассмотрим работу инструмента «Контроль целостности системы» (KICS for Nodes 4.5) на примере контроля состояния функции «Удалённый рабочий стол».

Для настройки соответствующей задачи перейдём в окно свойств функциональности «Контроль целостности системы».

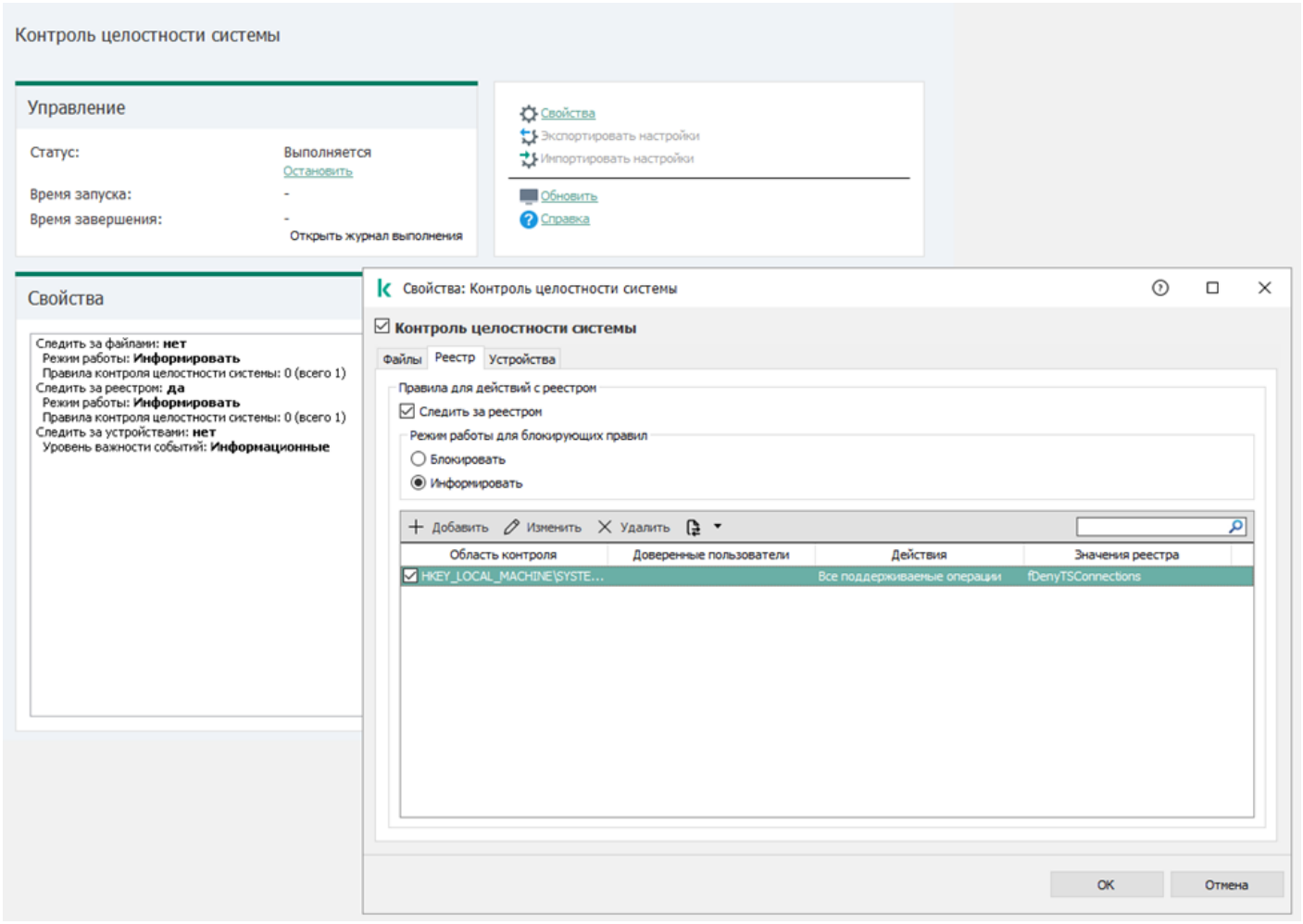


В окне свойств нажмём кнопку «Добавить» и настроим объект мониторинга, соответствующий ключу системного реестра, отвечающему за состояние функции удалённого рабочего стола операционной системы:

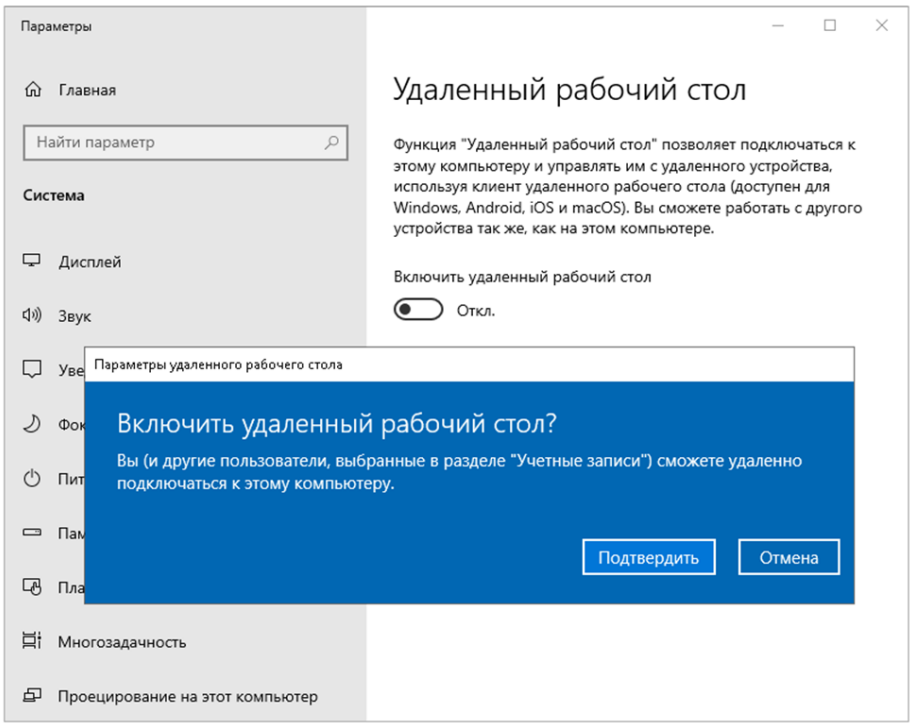
- Ветка: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`
- Параметр: `fDenyTSConnections`



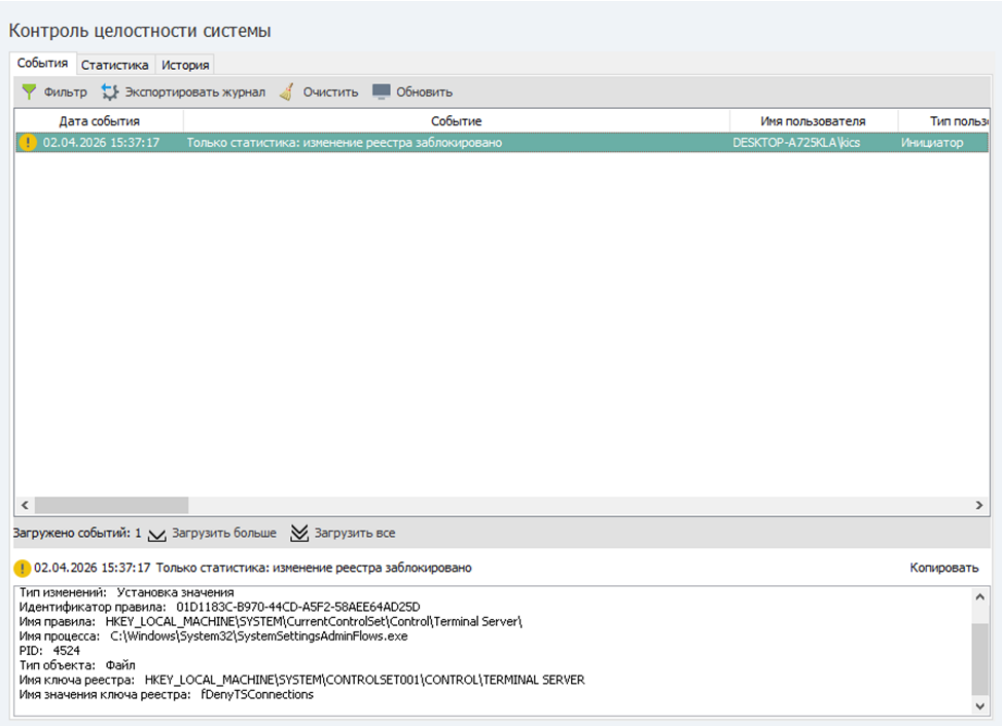
После настройки ключа активируем правило, включим функцию «Следить за реестром» в режиме «Информировать» и запустим «Контроль целостности системы».



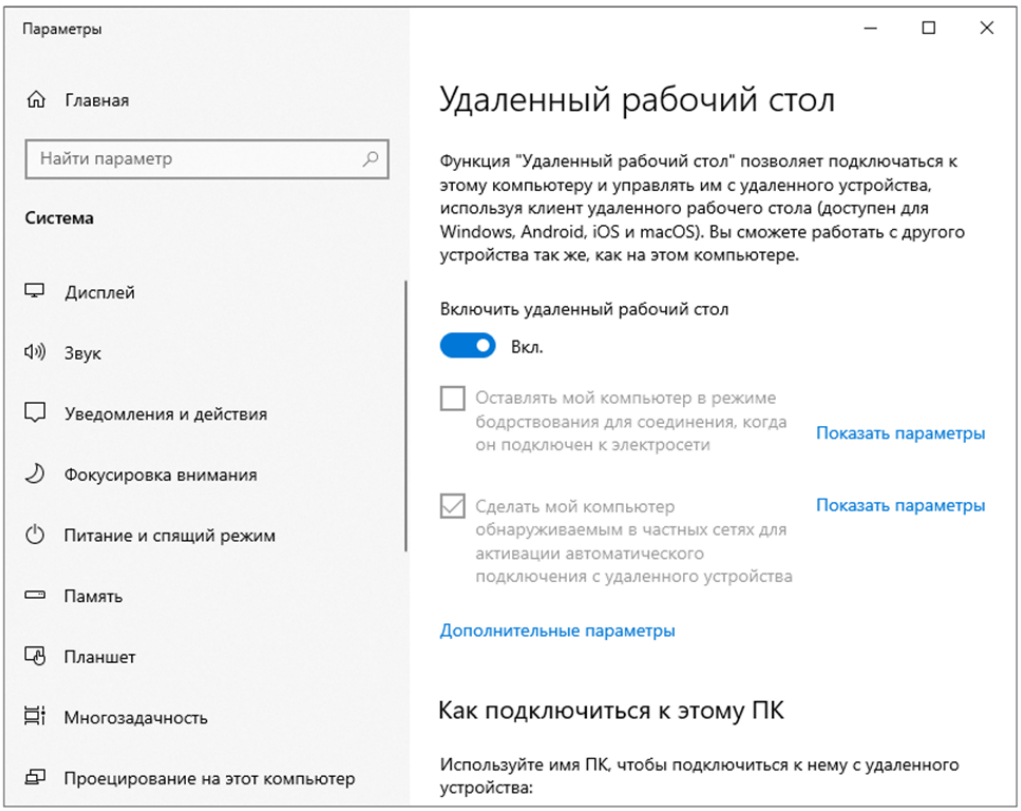
Перейдём в утилиту администрирования ОС и включим удалённый рабочий стол.



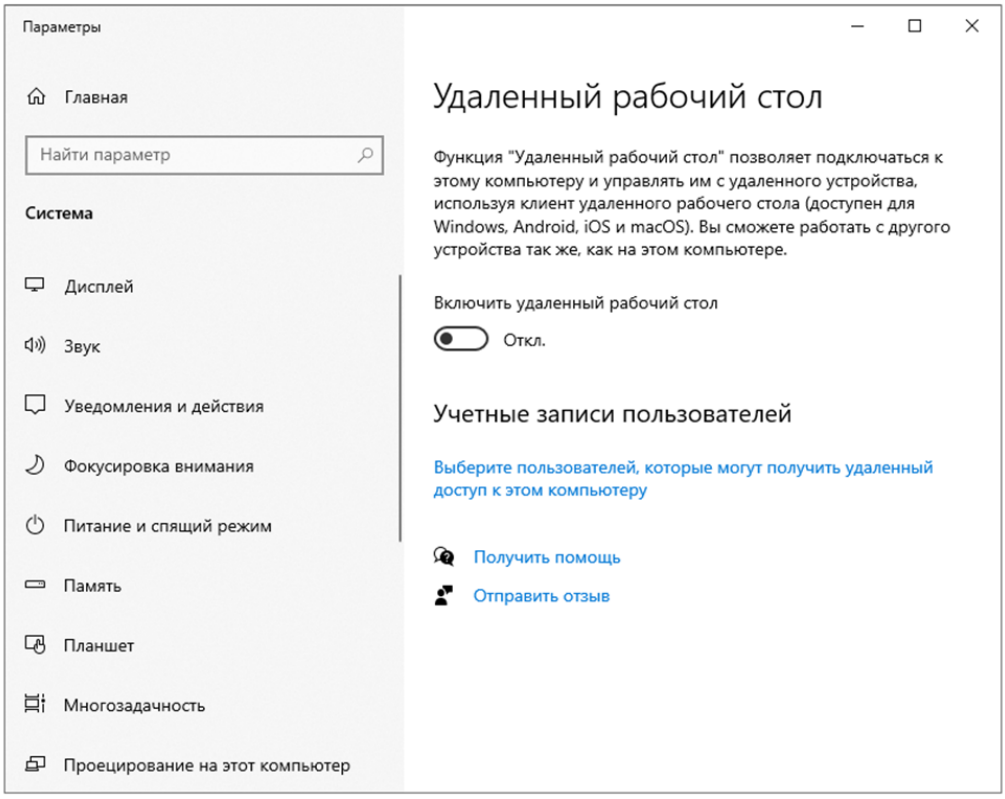
Проверим, что в журнале функциональности «Контроль целостности системы» появилось сообщение об изменении системного реестра с пометкой «Только статистика».



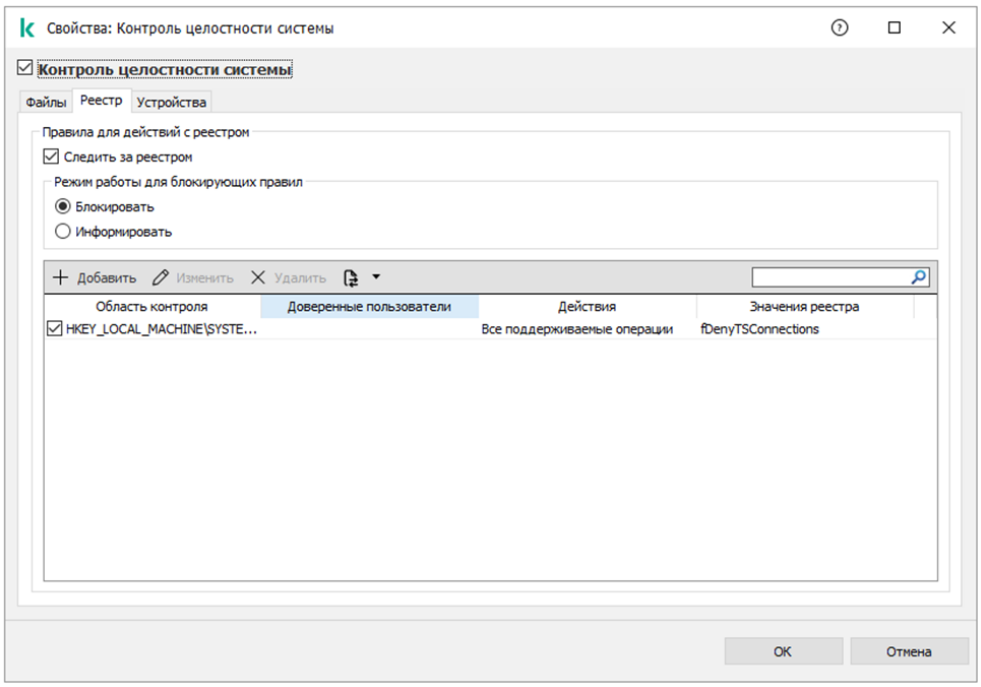
Убедимся, что изменение настройки системы прошло успешно — удалённый рабочий стол включён.



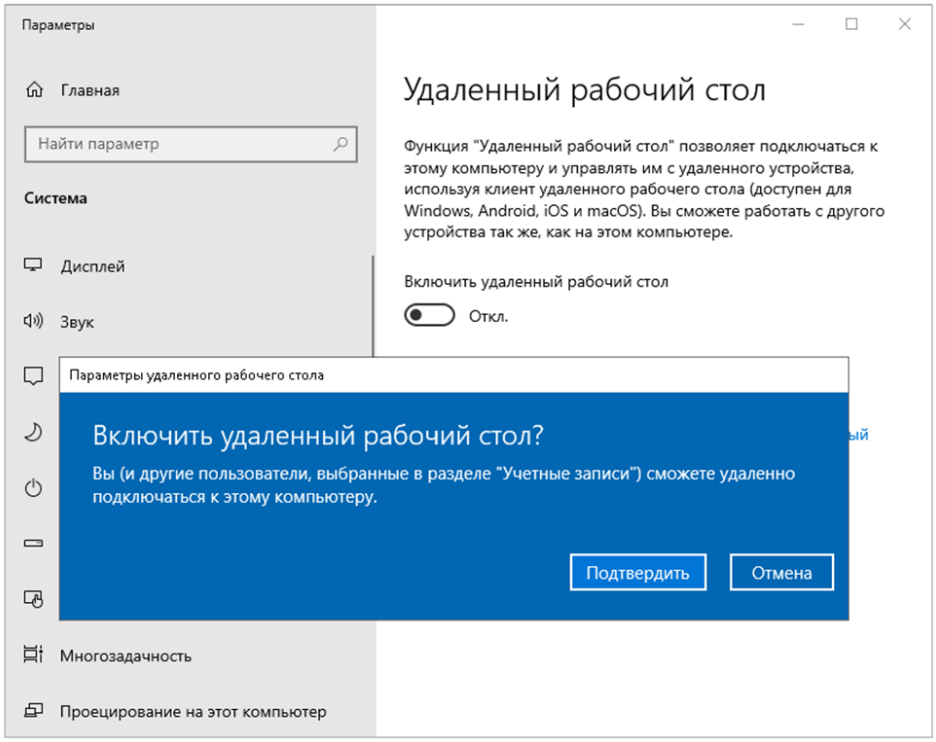
Переведём удалённый рабочий стол в выключенное состояние (целевое для защищаемой системы).



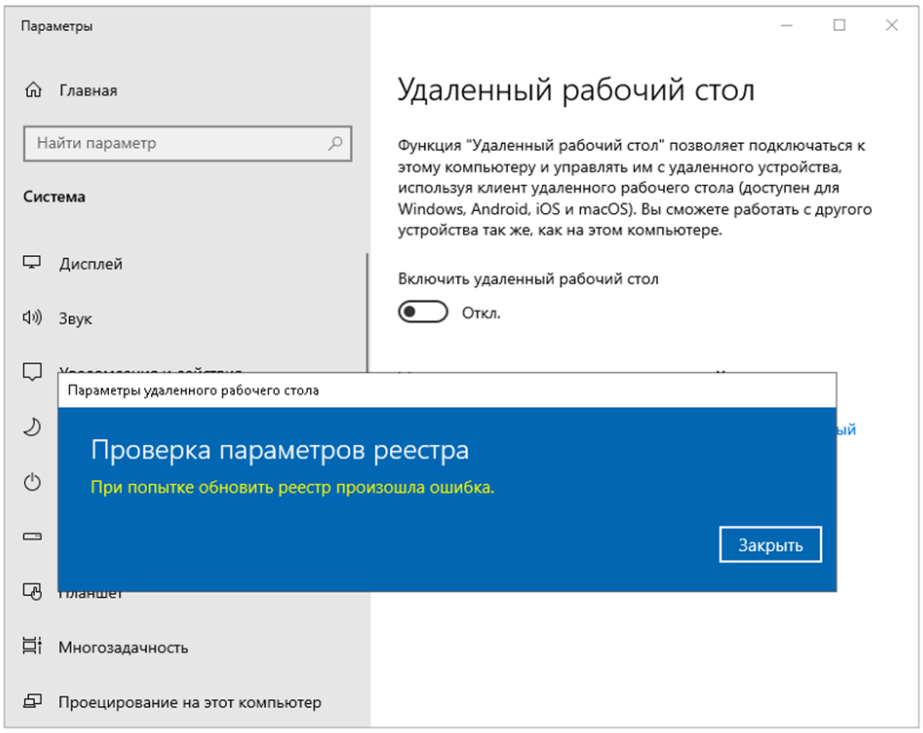
Изменим настройку режима функции «Следить за реестром» на «Блокировать» и применим изменения, нажав кнопку «OK».



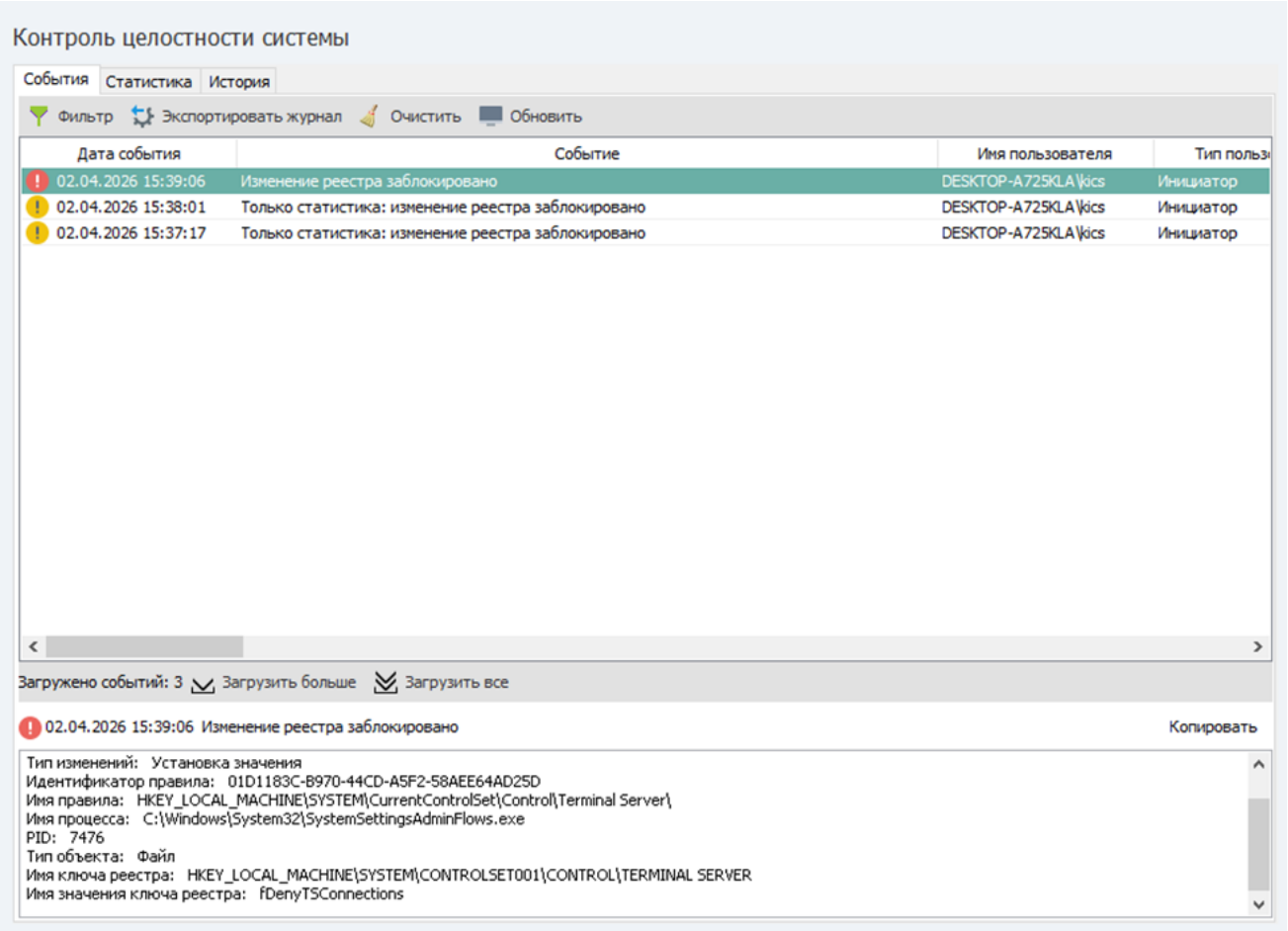
Перейдём в утилиту администрирования ОС и попытаемся включить удалённый рабочий стол.



Убедимся, что блокирующая технология KICS for Nodes отработала и операционная система ответила ошибкой на попытку изменения настроек.



Проверим, что в журнале функциональности «Контроль целостности системы» появилось сообщение о заблокированной попытке изменения системного реестра.



Аналогичным образом может быть реализовано реагирование на изменение других настроек операционных систем Windows. Ниже справочно приведены наборы ключей реестра операционных систем Windows 7 и Windows 10 для функций, изменение состояния которых можно контролировать или блокировать в целях обеспечения защищённости системы.

ВАЖНО! Отдельные ключи могут различаться в зависимости от выпуска операционной системы. Данный материал предоставляется в ознакомительных целях и не может быть использован для настройки действующих систем. Настройка действующих систем осуществляется исключительно на основании наименований фактических ключей, используемых в защищаемой системе, с обязательной проверкой работоспособности системы в соответствии с установленными требованиями.

Набор ключей для ОС Windows 7

Функция	Путь в реестре (Registry Path)	Имя параметра	Значение
ПОЛИТИКА ПАРОЛЕЙ			
Максимальный срок действия пароля	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters	MaximumPasswordAge	Число в днях (например, 30, 90)
УДАЛЕННЫЙ ПОМОЩНИК (Remote Assistance)			

Включение/Отключение помощника	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance	fAllowToGetHelp	1 = Включен, 0 = Отключен
Разрешение полного управления	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance	fAllowFullControl	1 = Разрешено, 0 = Только просмотр
Предложение помощи (несанкционированное)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services	fAllowUnsolicited	1 = Разрешено, 0 = Запрещено
Управление чатом	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Remote Assistance	fEnableChatControl	1 = Чат включен, 0 = Чат отключен
УДАЛЕННЫЙ РАБОЧИЙ СТОЛ (Remote Desktop / RDP)			
Включение/Отключение RDP	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server	fDenyTSConnections	0 = Включен, 1 = Отключен
Альтернативный путь (Политики)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services	fDenyTSConnections	0 = Включен, 1 = Отключен
Количество одновременных сессий	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server	fSingleSessionPerUser	0 = Несколько сессий, 1 = Одна сессия
Запрет пустых паролей	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	1 = Запретить, 0 = Разрешить
Перенаправление USB (RemoteFX)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client	fUsbRedirectionEnableMode	0 = Выкл, 1 = Только админы, 2 = Все
Remote Registry (служба)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry	Start	4 = Отключено
СЕТЕВОЕ ОБНАРУЖЕНИЕ И ОБЩИЙ ДОСТУП			
Сетевое обнаружение	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNSCache\Parameters	EnableNetbiosDetection	Управляет обнаружением сетей
Общий доступ к файлам и принтерам	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print	DisableServerThread	1 = Отключить общий доступ к принтерам
Общий доступ к папкам (админ. ресурсы)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	AutoShareServer	0 = Отключить C$, ADMIN$

Общий доступ к папкам (рабочая станция)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	AutoShareWks	0 = Отключить общие ресурсы
АУДИТ И СОБЫТИЯ			
Аудит (глобальное состояние)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	auditbaseobjects	0 = Отключить аудит базовых объектов
Размер журнала безопасности	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security	MaxSize	Максимальный размер в байтах
Размер журнала приложений	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application	MaxSize	Максимальный размер в байтах
Очистка журнала (запрет перезаписи)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security	Retention	Управляет перезаписью и очисткой
КОНТРОЛЬ УЧЕТНЫХ ЗАПИСЕЙ (UAC)			
Главный выключатель UAC	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableLUA	1 = UAC включен, 0 = UAC отключен
Поведение запроса для администраторов	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	0 = Без запроса, 1 = Запрос данных, 2 = Запрос согласия, 5 = Затемнение экрана
Поведение запроса для обычных пользователей	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	1 = Запрос данных, 3 = Затемнение экрана
Переключение на безопасный рабочий стол	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	PromptOnSecureDesktop	1 = Запрос на безопасном столе, 0 = На обычном
Режим одобрения администратором	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableVirtualization	Управляет виртуализацией
Обнаружение установки приложений	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableInstallerDetection	1 = Запрос повышения прав при установке
Только подписанные исполняемые файлы	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ValidateAdminCodeSignatures	1 = Только для подписанных файлов

Режим одобрения для встроенного администратора	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	FilterAdministratorToken	1 = Режим одобрения для Administrator
UIAccess без безопасного стола	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableUIADesktopToggle	1 = Разрешено, 0 = Запрещено
Виртуализация файлов и реестра	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableVirtualization	1 = Включена, 0 = Отключена
ВОССТАНОВЛЕНИЕ СИСТЕМЫ			
Восстановление системы	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore	DisableSR	1 = Отключено, 0 = Включено
БРАНДМАУЭР			
Включение брандмауэра (стандартный профиль)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	EnableFirewall	1 = Включен, 0 = Отключен
Включение брандмауэра (доменный профиль)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile	EnableFirewall	1 = Включен, 0 = Отключен
БЕЗОПАСНОСТЬ ПОДКЛЮЧЕНИЙ			
Подписывание пакетов SMB (клиент)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters	RequireSecuritySignature	1 = Подписывание обязательно
Подписывание пакетов SMB (сервер)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	RequireSecuritySignature	1 = Подписывание обязательно
КОНТРОЛЬ ПРОЦЕССОВ И ОБЪЕКТОВ			
Квоты памяти для процессов	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	PagedPoolQuota	Управляет квотой страничного пула
Отладка программ	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	Debugger	Управляет отладчиками по умолчанию

Профилирование процессов	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment	PROFILER	Настройки профилирования
СЛУЖБА ЖУРНАЛА СОБЫТИЙ			
Административные шаблоны Event Log	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application	MaxSize, Retention	Параметры размера и хранения
ОТЧЕТЫ ОБ ОШИБКАХ			
Отключить отчеты об ошибках Windows	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting	Disabled	1 = Отключить, 0 = Включить
АВТОЗАПУСК (AUTOPLAY / AUTORUN)			
Вариант работы автозапуска	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoDriveTypeAutoRun	Битовая маска (255 = отключить все)
Флажок "Всегда выполнять"	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers	DisableAlwaysShowCheckBox	1 = Не показывать флажок
Отключить автозапуск (полностью)	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutorun	1 = Отключить автозапуск
Отключить автозапуск для устройств, не являющихся томами	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutoplayfornonVolume	1 = Отключить для MTP устройств

Набор ключей для Windows 10

Функция	Путь в реестре (Registry Path)	Имя параметра	Значение
ПОЛИТИКА ПАРОЛЕЙ			
Максимальный срок действия пароля	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters	MaximumPasswordAge	Число в днях (например, 30, 90)
УДАЛЕННЫЙ ПОМОЩНИК (Remote Assistance)			
Включение/Отключение помощника	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance	fAllowToGetHelp	1 = Включен, 0 = Отключен
Разрешение полного управления	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance	fAllowFullControl	1 = Разрешено, 0 = Только просмотр

Предложение помощи (несанкционированное)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services	fAllowUnsolicited	1 = Разрешено, 0 = Запрещено
Управление чатом	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Remote Assistance	fEnableChatControl	1 = Чат включен, 0 = Чат отключен
УДАЛЕННЫЙ РАБОЧИЙ СТОЛ (Remote Desktop / RDP)			
Включение/Отключение RDP	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server	fDenyTSConnections	0 = Включен, 1 = Отключен
Альтернативный путь (Политики)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services	fDenyTSConnections	0 = Включен, 1 = Отключен
Аутентификация на уровне сети (NLA)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp	UserAuthentication	1 = NLA обязательна
Запрет пустых паролей	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	1 = Запретить, 0 = Разрешить
Remote Registry (служба)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry	Start	4 = Отключено
СЕТЕВОЕ ОБНАРУЖЕНИЕ И ОБЩИЙ ДОСТУП			
Общий доступ к папкам (админ. ресурсы)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	AutoShareServer	0 = Отключить C$, ADMIN$
Общий доступ к папкам (рабочая станция)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	AutoShareWks	0 = Отключить общие ресурсы
Отключение SMBv1 (небезопасный протокол)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	SMB1	0 = Отключен
АУДИТ И СОБЫТИЯ			
Размер журнала безопасности	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security	MaxSize	Максимальный размер в байтах
Размер журнала приложений	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application	MaxSize	Максимальный размер в байтах
Размер журнала системы	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System	MaxSize	Максимальный размер в байтах

КОНТРОЛЬ УЧЕТНЫХ ЗАПИСЕЙ (UAC)			
Главный выключатель UAC	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableLUA	1 = UAC включен, 0 = UAC отключен
Поведение запроса для администраторов	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	0 = Без запроса, 1 = Запрос данных, 2 = Запрос согласия, 5 = Затемнение экрана
Поведение запроса для обычных пользователей	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	1 = Запрос данных, 3 = Затемнение экрана
Переключение на безопасный рабочий стол	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	PromptOnSecureDesktop	1 = Запрос на безопасном столе, 0 = На обычном
Режим одобрения для встроенного администратора	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	FilterAdministratorToken	1 = Режим одобрения для Administrator
Обнаружение установки приложений	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableInstallerDetection	1 = Запрос повышения прав при установке
Только подписанные исполняемые файлы	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	ValidateAdminCodeSignatures	1 = Только для подписанных файлов
Виртуализация файлов и реестра	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableVirtualization	1 = Включена, 0 = Отключена
SmartScreen (Защита от фишинга и вредоносных сайтов)			
Включение SmartScreen для Edge/Chrome	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter	EnabledV9	1 = Включен
SmartScreen для приложений из Store	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System	EnableSmartScreen	1 = Включен
ВОССТАНОВЛЕНИЕ СИСТЕМЫ			
Восстановление системы	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore	DisableSR	1 = Отключено, 0 = Включено
БЕЗОПАСНОСТЬ ПОДКЛЮЧЕНИЙ			

Подписывание пакетов SMB (клиент)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters	RequireSecuritySignature	1 = Подписывание обязательно
Подписывание пакетов SMB (сервер)	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	RequireSecuritySignature	1 = Подписывание обязательно
ОТЧЕТЫ ОБ ОШИБКАХ			
Отключить отчеты об ошибках Windows	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting	Disabled	1 = Отключить, 0 = Включить
АВТОЗАПУСК (AUTOPLAY / AUTORUN)			
Вариант работы автозапуска	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoDriveTypeAutoRun	Битовая маска (255 = отключить все)
Отключить автозапуск (полностью)	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutorun	1 = Отключить автозапуск
Отключить автозапуск для устройств, не являющихся томами	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutoplayfornonVolume	1 = Отключить для MTP устройств
BitLocker (шифрование диска)			
Включение BitLocker	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE	EnableBDEWithNoTPM	1 = Разрешить без TPM
Тип шифрования	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE	EncryptionMethod	4 = XTS-AES 128, 6 = XTS-AES 256
Windows Update (безопасность обновлений)			
Автоматическая установка обновлений	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	4 = Автоустановка
Отключение обновлений	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoUpdate	1 = Отключено, 0 = Включено

Данные наборы не являются исчерпывающими. Выбор функций, подлежащих мониторингу, зависит от конфигурации конкретной защищаемой системы.

Revision #8
Created 2 April 2026 13:38:36 by Alexey Panyukhin
Updated 2 April 2026 14:34:59 by Alexey Panyukhin