министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

*факультет Программной инженерии и компьютерной техники*

*Дисциплина «Информационная безопасность»*

**Лабораторная работа №3**

Вариант 7

Группа: P3417

Выполнил: Ореховский А.

Проверила: Маркина Т. А.

Санкт-Петербург,

2021г

# Часть 1

Какие конкретно ветки и ключи доступны (в отчёте: перечислите их названия):

* Пользователю хотя бы на чтение

По умолчанию, пользователь имеет доступ к веткам HKCU и HKU, а также доступ на чтение ко всем остальным веткам

* только Администратору

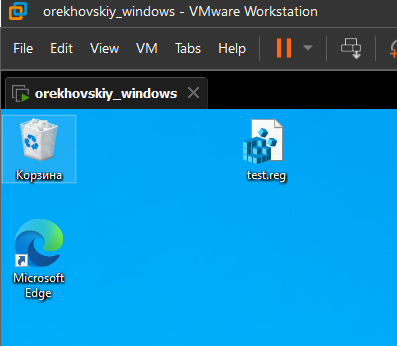
Отсутствуют

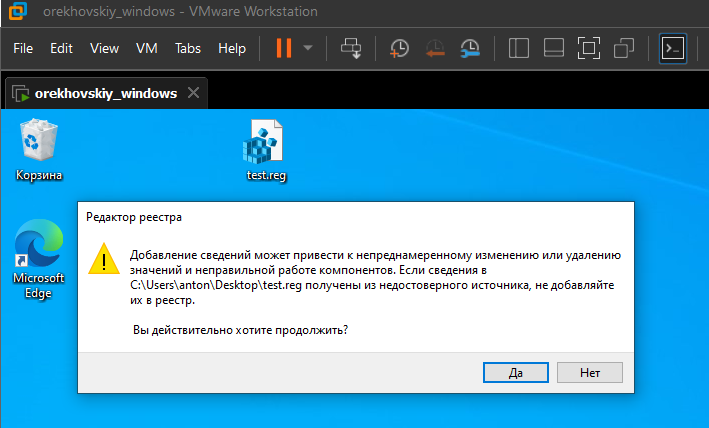
* только System

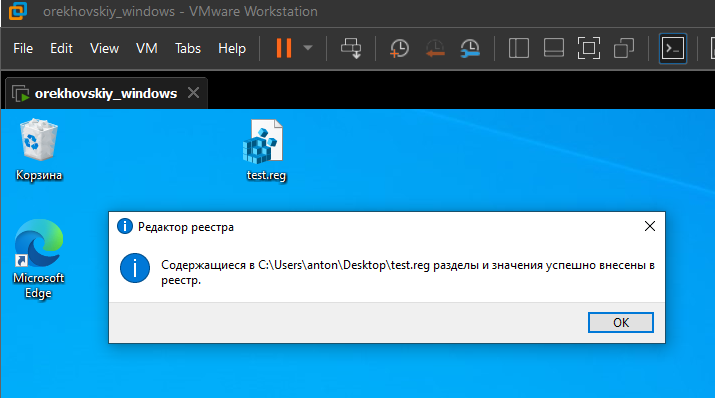
HKLM (SAM, SECURITY)

# Часть 2. Опишите в отчете способы восстановления реестра

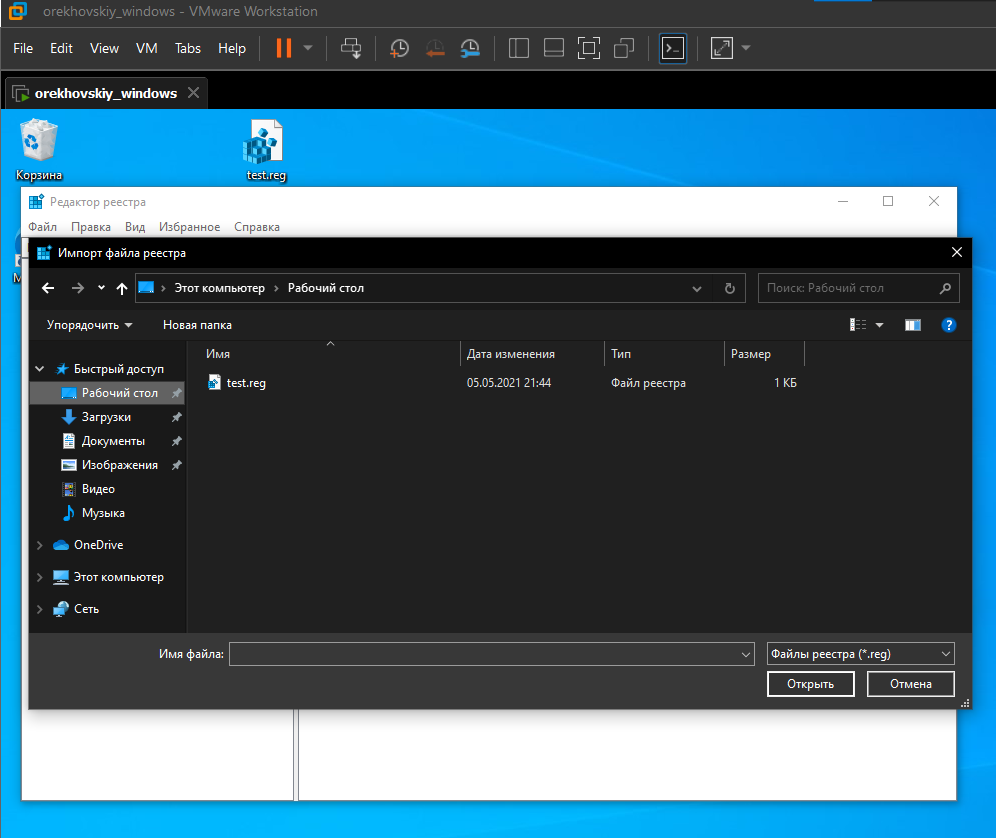
Имея файл, который является экспортом реестра, можно запустить его как обычный либо из контекстного меню выбрать опцию слияние.

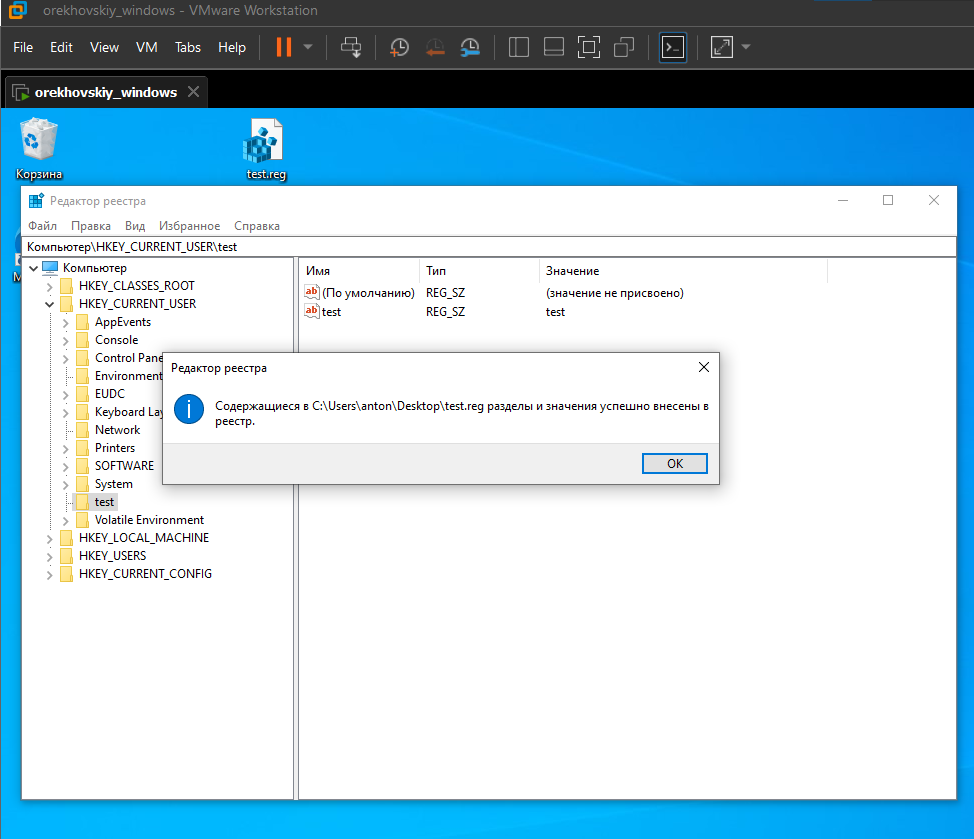






Либо же импортировать в самом редакторе реестра.

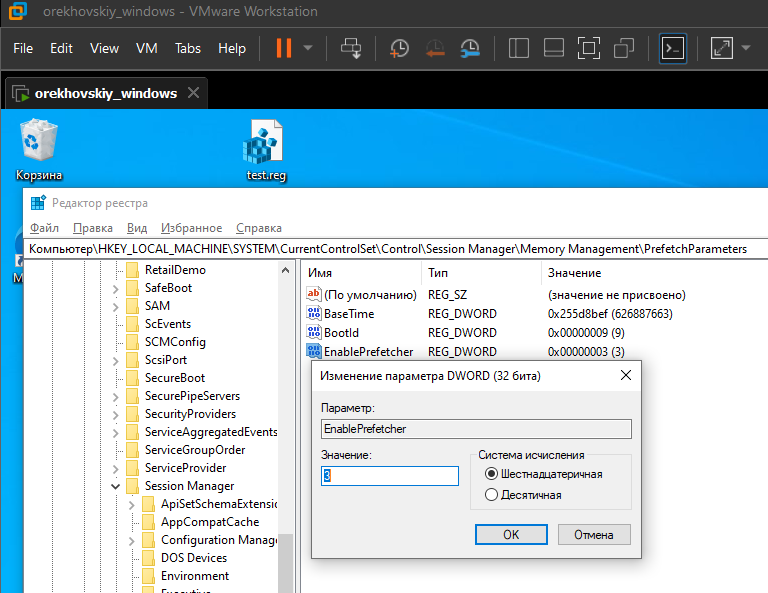




Также возможен вариант использования восстановления системы, так как точка восстановления хранит в себе параметры реестра. Таким образом, нужно лишь откатиться к созданной точке восстановления либо импортировать значение файла точки восстановления используя диск восстановления и командную строку запущенную из оного средства.

# Часть 3

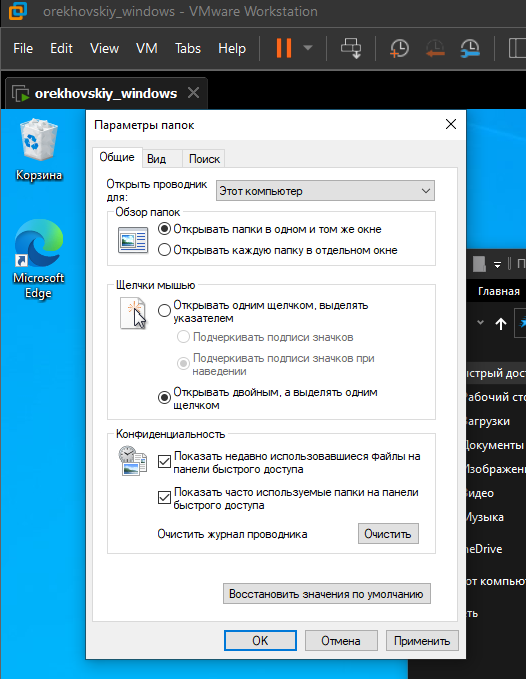
## Настройка службы Superfetch: включение службы Superfetch.

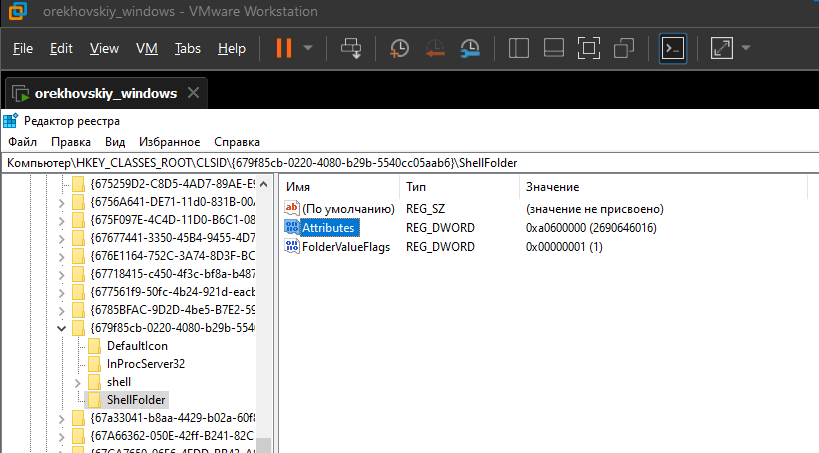


Значение 3 говорит о включении префектуры всего и используется по умолчанию. 0 – отключение.

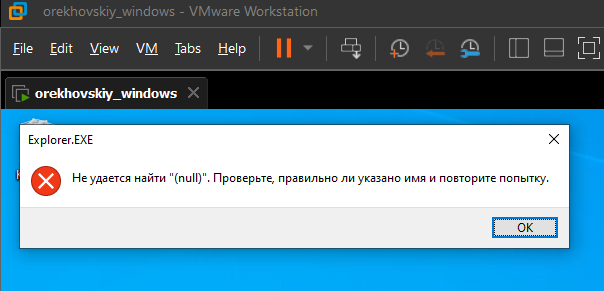
## Отключение истории списка последних и часто используемых файлов.

Для корректного изменения соответствующего значения в редакторе реестра, для начала необходимо изменить то, что проводник открывает по умолчанию, а именно с быстрого доступа на этот компьютер. Далее необходимо найти соответствующий ключ в редакторе реестра и настроить права доступа для него. Таким образом необходимо поменять владельца данного ключа и добавить разрешение на полный доступ группе администраторов. Затем необходимо поменять значение параметра Attributes на a0600000.



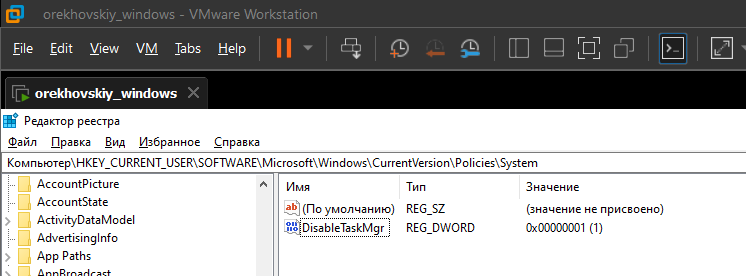


После выполнения всех действий и поменяв начально окно в проводнике обратно на быстрый доступ, имеем следующую ошибку.

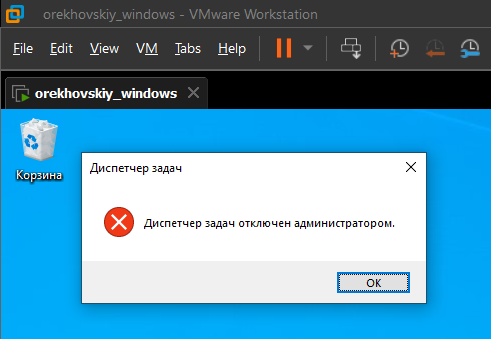


## Отключение вызова диспетчера задач.

Необходимо в редакторе реестра создать параметр DisableTaskMger в указанном ключе со значением 1.

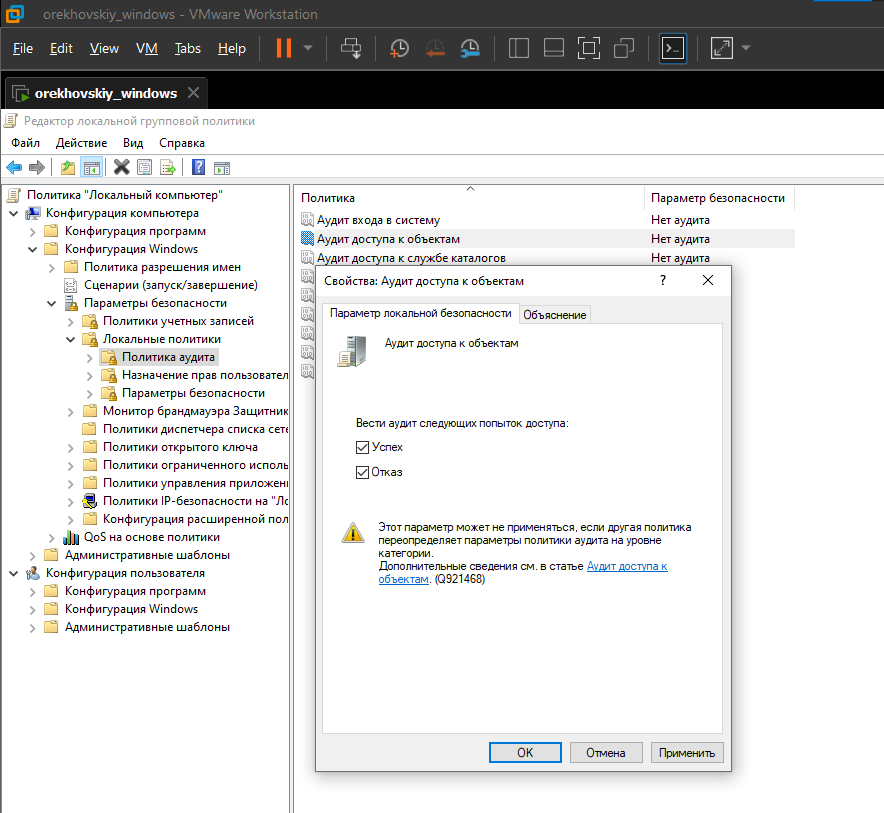


Пытаемся вызвать диспетчер задач.

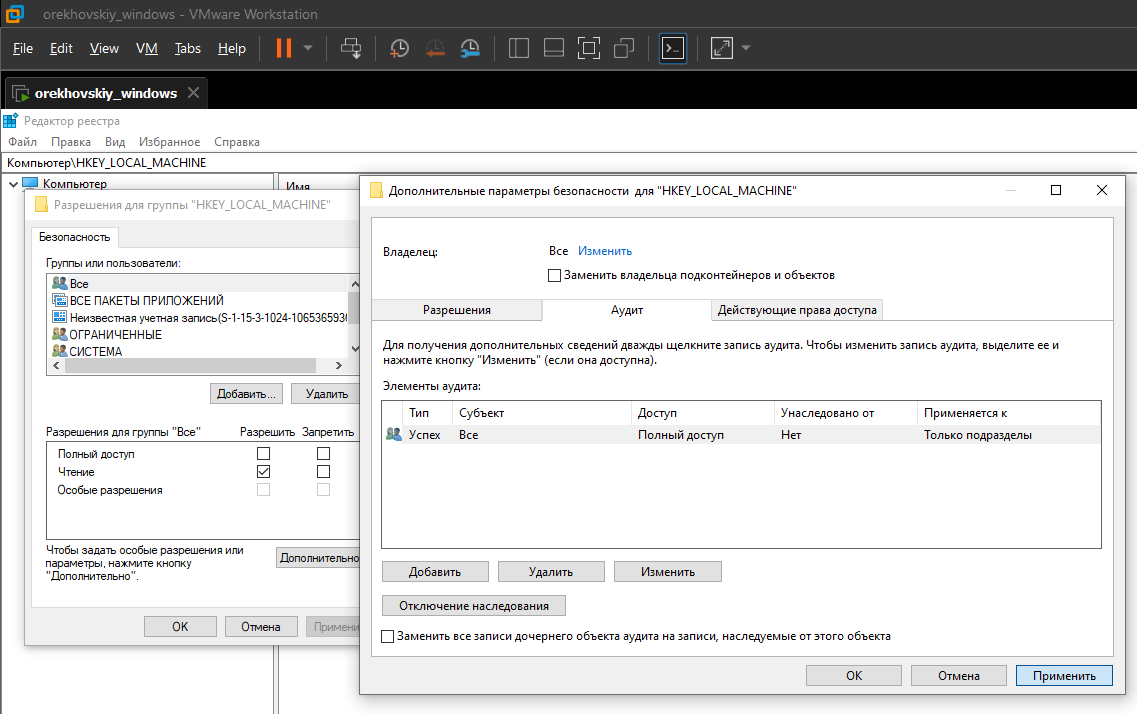


# Часть 4.

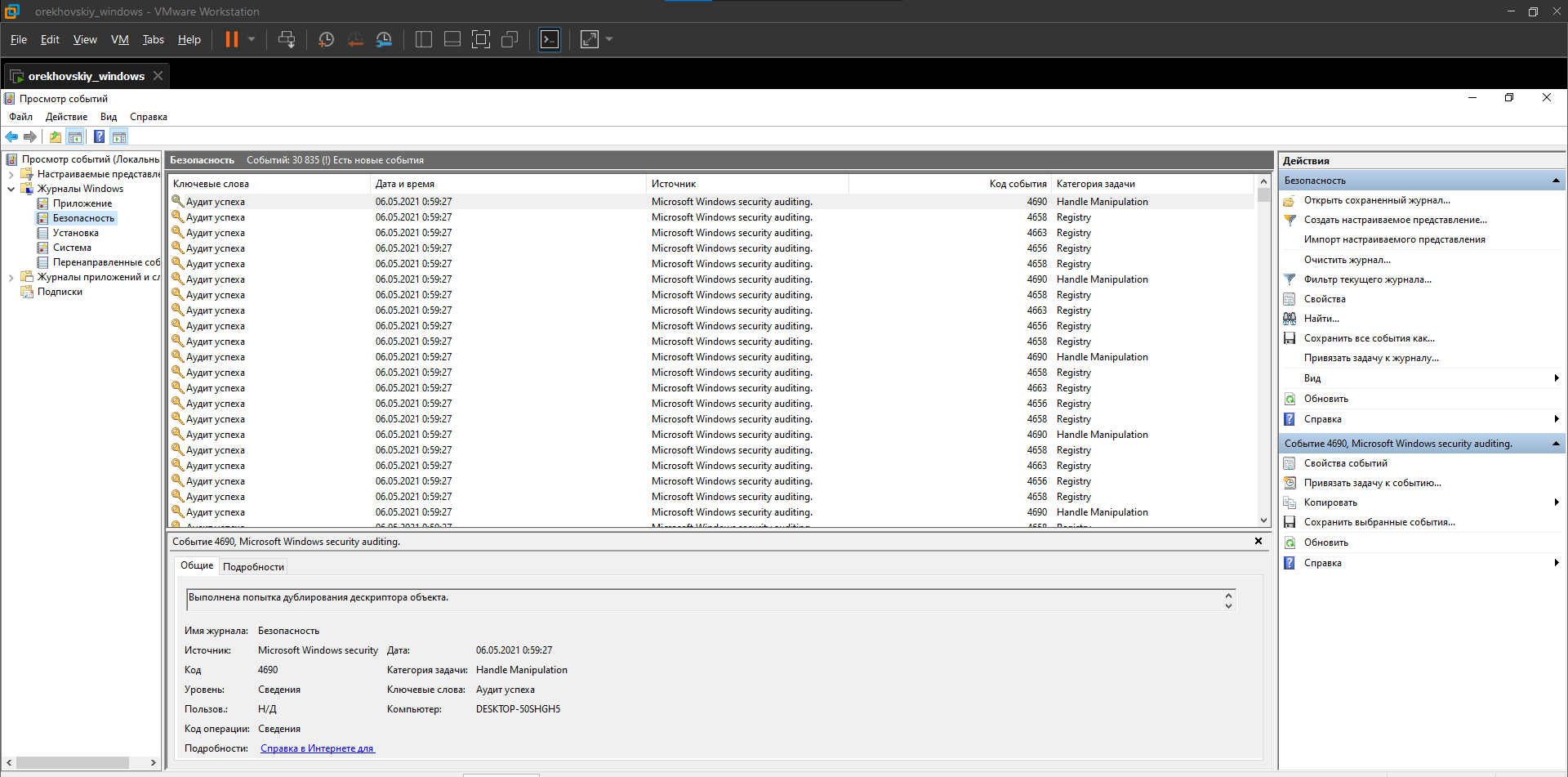
Так как по умолчанию аудит не включен, его необходимо включить ручками при помощи редактора локальной групповой политики.



Далее добавляем аудит на ветку HKLM, а именно на ее подразделы (сразу на все, что вроде как больше 5)

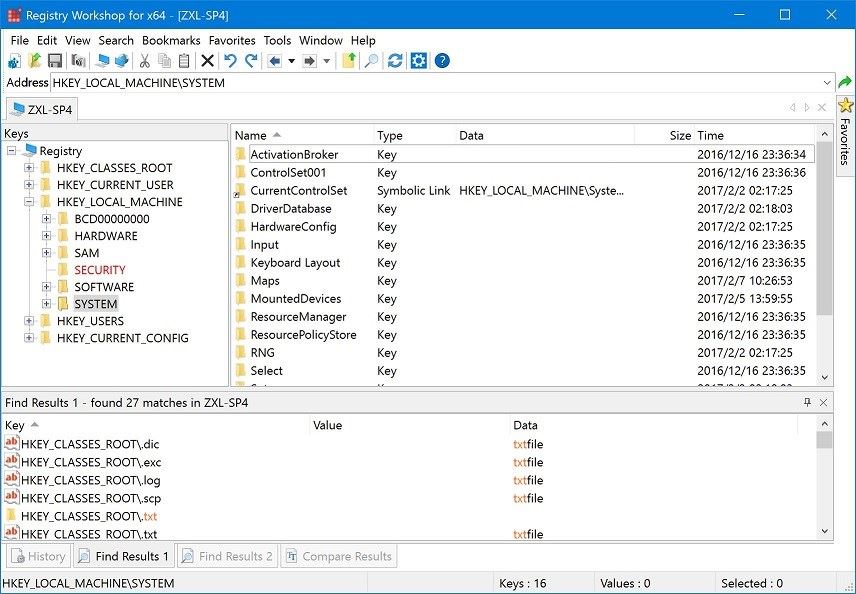


Просматриваем журнал аудита в приложении «Просмотр событий»



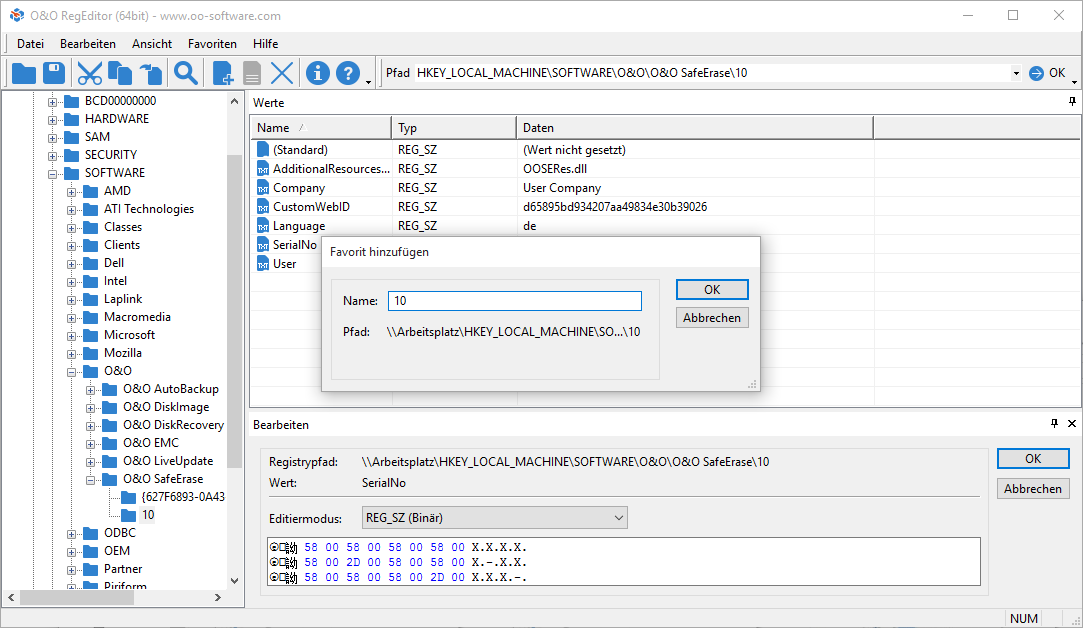
# Часть 5. Аналоги Regedit

## Registry Workshop



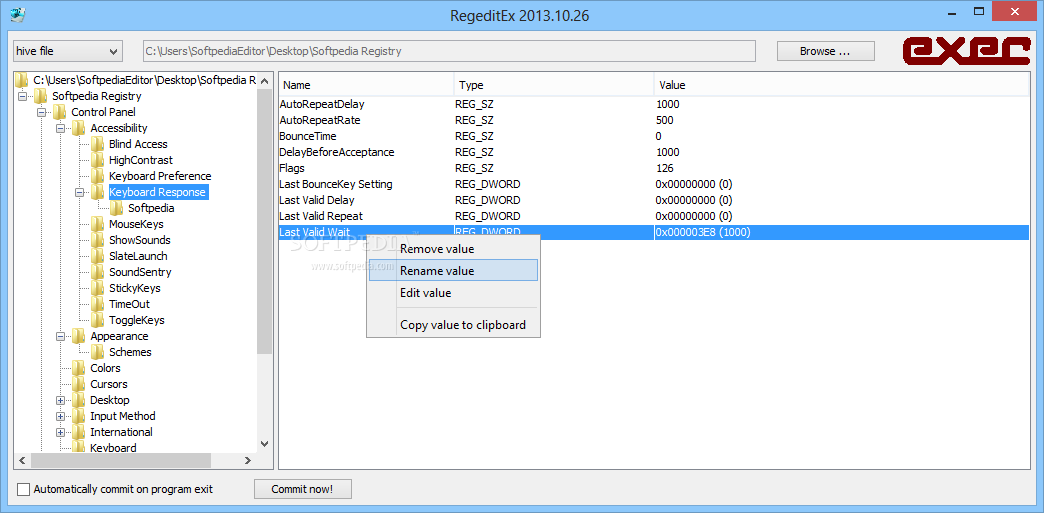
Registry Workshop - продвинутый редактор реестра. Это идеальная замена для RegEdit и RegEdt32, которые поставляются с Windows. В дополнение ко всем стандартным функциям Registry Workshop добавляет множество мощных функций, которые позволяют вам быстрее и эффективнее работать с задачами, связанными с реестром. С Registry Workshop, редактирование реестра становится более безопасным, чем когда-либо прежде. Все изменения, кроме изменения прав доступа к ключам, можно безопасно отменить (даже заменить и импортировать реестр), используя несколько уровней отмены. Из недостатков можно выделить отсутствие бесплатной версии, достаточной для решения общих проблем и чересчур большое количество возможностей, кторые структурированы не лучшим образом, что может сбивать с толку.

## O&O RegEditor



Изменение или создание настроек системы и программы принадлежит повседневной работе каждого администратора. O & O RegEditor значительно облегчает работу с регистрационной базой данных. Он поставляется с чрезвычайно удобным для пользователя приложением, но благодаря своей мобильности он действительно значительно облегчает жизнь администратора. Минусом является плохо продуманная система экспорта настроек, так например нет возможности выбора папки для экспорта.

## RegeditEx



RegeditEx написан на Java без использования Windows API. Он похож на инструмент Windows Regedit. Но в отличие от Regedit, он может работать и в средах, отличных от Windows, таких как Linux. RegeditEx может обрабатывать кусты стандартных реестров и реестров PE (включая PE1 setupreg.hiv). Не рекомендуется обрабатывать живой реестр хоста. Это может сработать, но в настоящее время неизвестно, что может произойти.