Настройка антивирусов для работы LanAgent

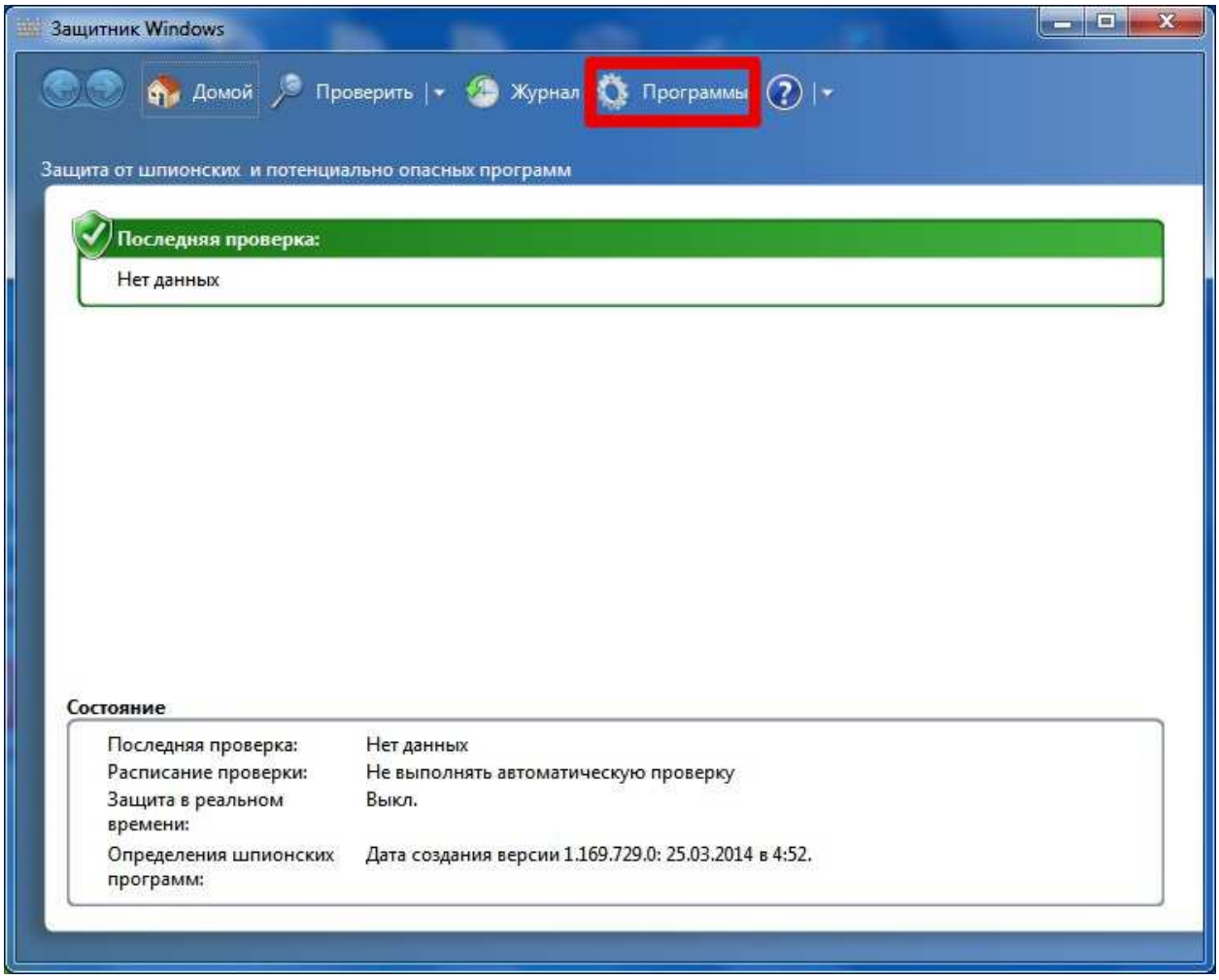
Оглавление

1 Защитник Windows

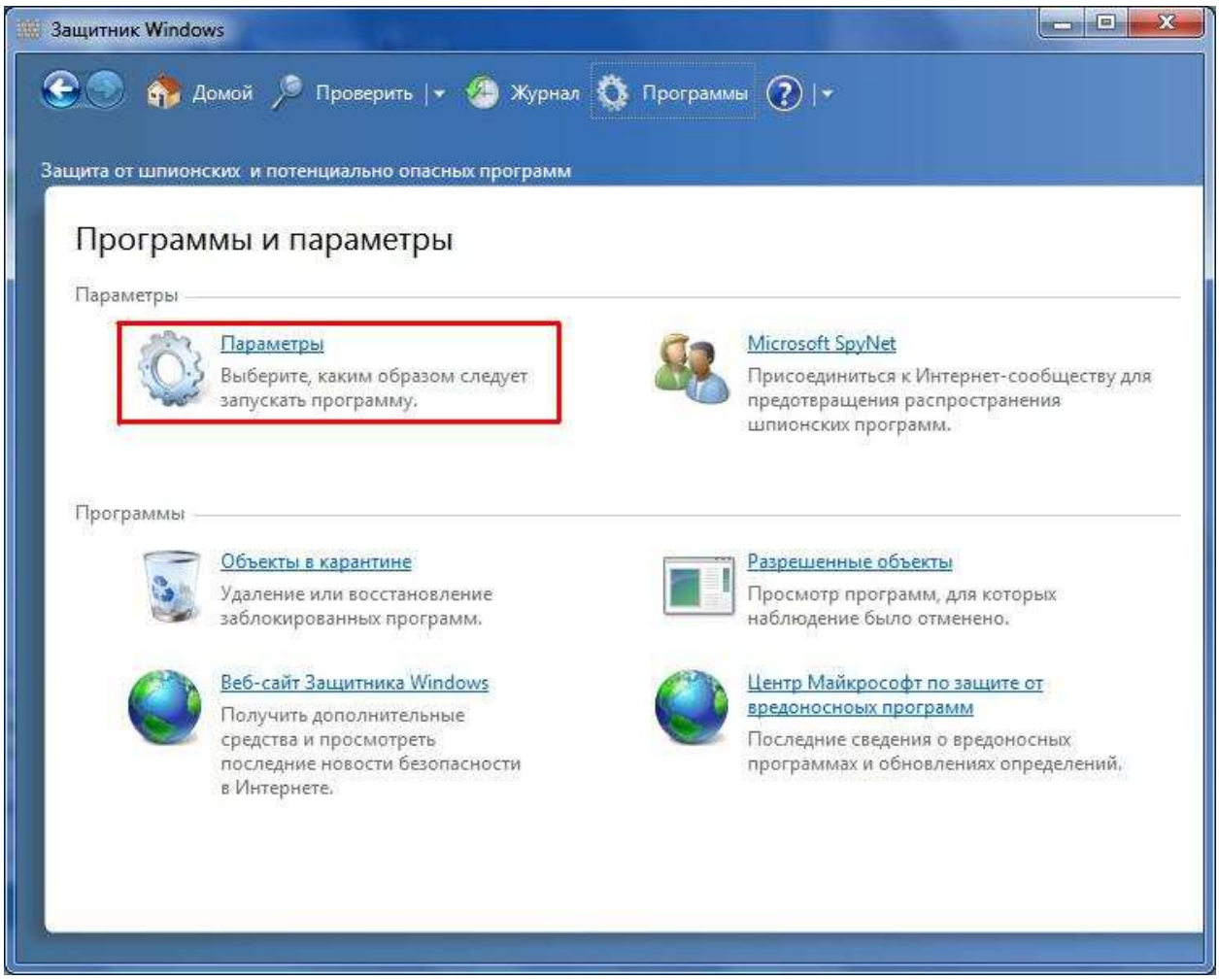
На компьютерах с операционной системой Windows 7/8 по умолчанию включен Защитник windows, это встроенный антивирус от Майкрософт. Не путайте его, пожалуйста, с брандмауером, это разные программы. Желательно внести в настройках «Защитника» исключение на каталог установки агента. Это можно сделать как локально (непосредственно на контролируемом компьютере), так и через групповые политики.

1.1 Локальная настройка

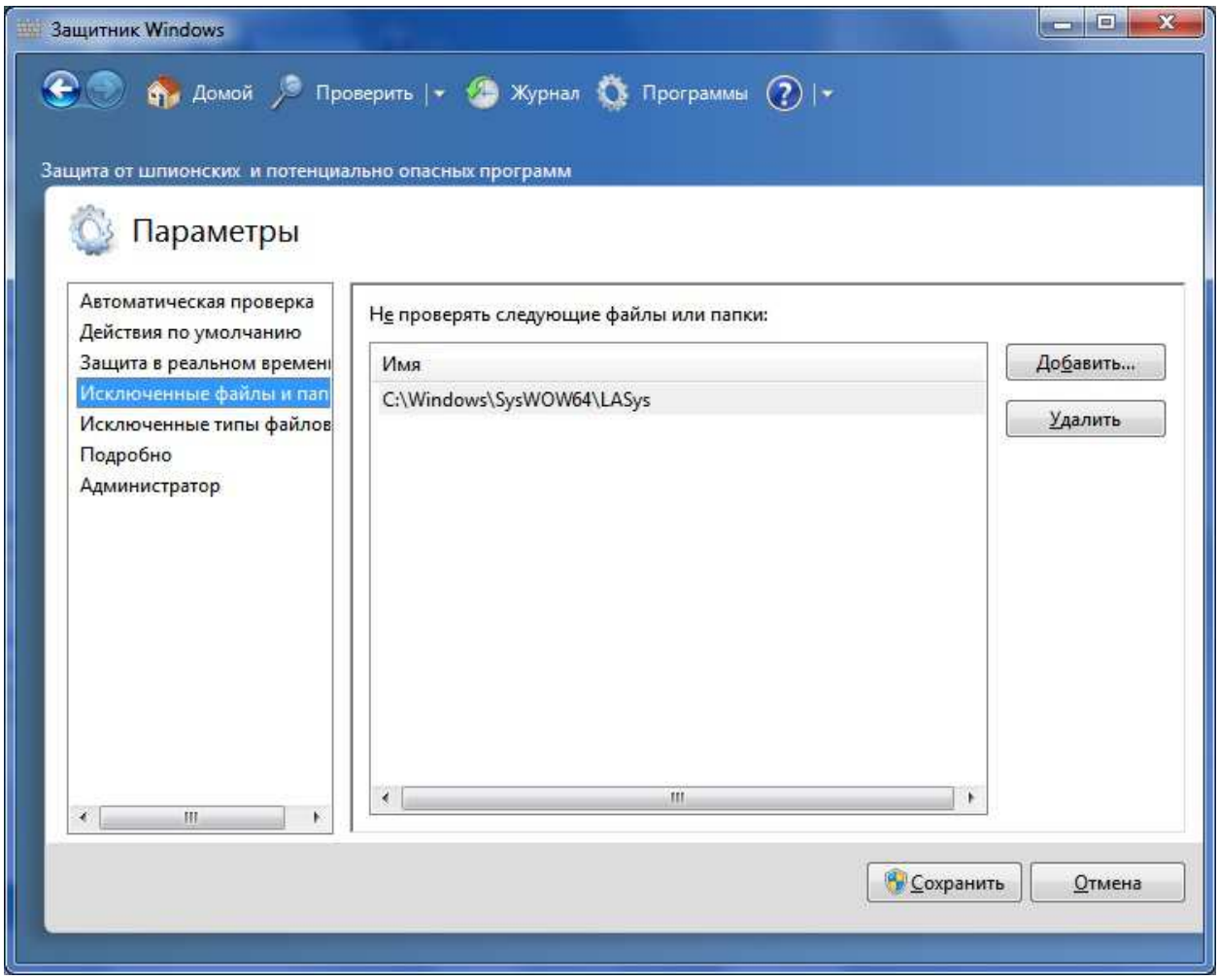
Для локальной настройки, выполните Пуск – в строке поиска программ наберите Защитник – выберите программу «Защитник Windows» из предложенного списка.



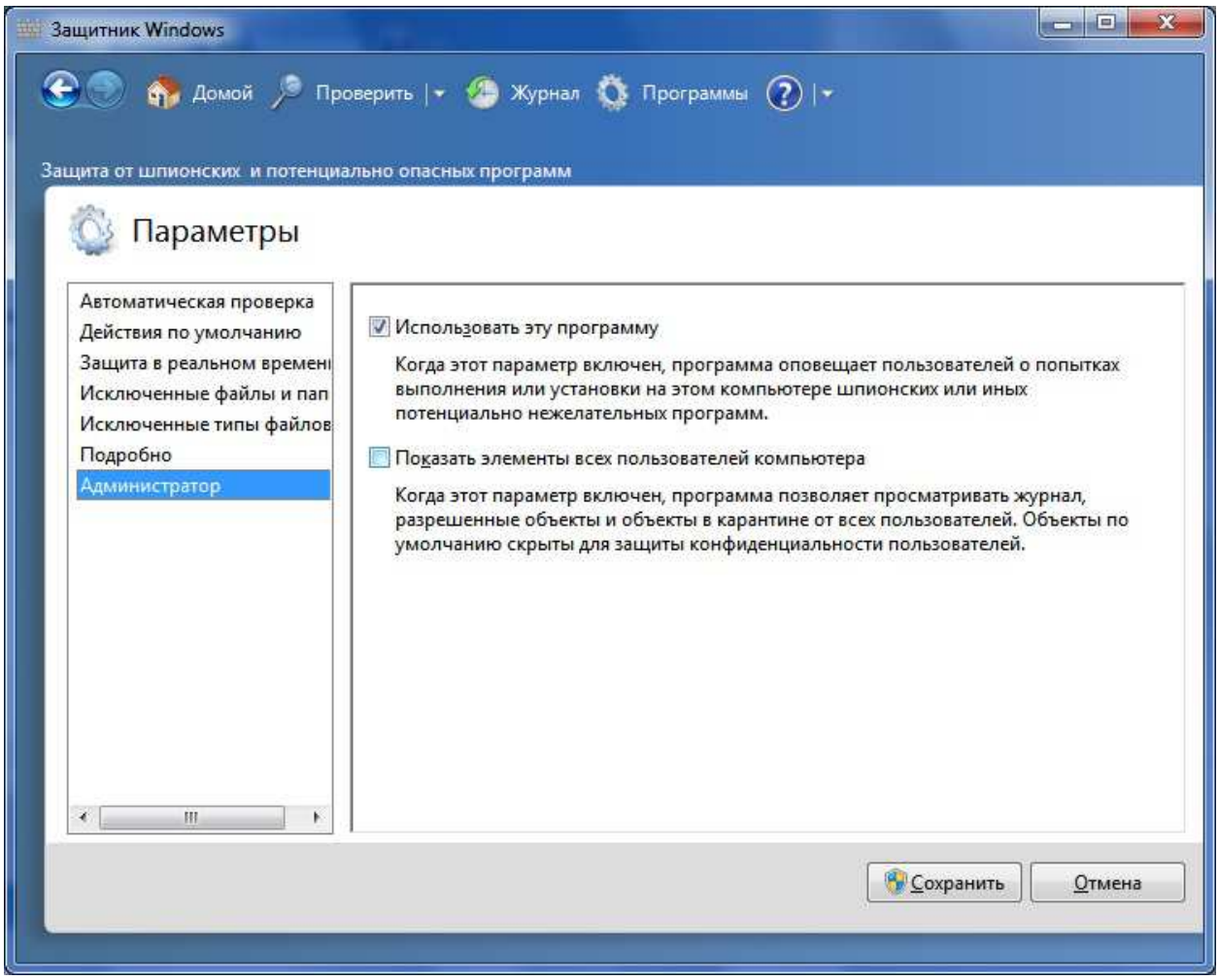
В открывшемся приложении нажмите кнопку «Программы» в верхнем меню. Далее, нажмите кнопку Параметры.



Перейдите на пункт «Исключенные файлы и папки». Надо добавить в исключение каталог установки агента. Для 32 битных систем это system32\lasys, для 64 битных систем – syswow64\lasys. Каталог скрытый и системный. Для того, чтобы Защитник Windows смог его увидеть, надо в проводнике нажать Alt, в появившемся меню выбрать Сервис – Параметры папок… В открывшемся окне перейти на пункт Вид и там поставить галочку на пункте «Показывать скрытые файлы, папки и диски» и убрать галочку с пункта «Скрывать защищенные системные файлы». После этого в перечне папок для исключений появится папка LASys. После ее добавления указанные опции можно вернуть к исходному состоянию.



Если на компьютере установлен качественный антивирус, то Защитник windows можно и совсем отключить. Для этого надо убрать галочку «Использовать эту программу» на пункте «Администратор».



1.2 Настройка Защитника через групповые политики.

Дистанционная настройка защитника заключается в добавлении на нужные компьютеры ключей реестра. Ниже указаны конкретные ветки:

Ключ реестра для отключения Защитника:

```
;Использовать эту программу
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000000
```

Исключение каталога

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"ИМЯ_ПАПКИ"=dword:00000000
```

Где в названии параметра «ИМЯ_ПАПКИ» нужно ввести полный путь к папке или файлу, который будет исключен из сканирования.

Пример:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"C:\windows\system32\lasys"=dword:00000000
```

Для 64 битных систем ключ будет:
"C:\windows\syswow64\lasys"=dword:00000000

1.3 Настройка MS Essentials через групповые политики.

Дистанционная настройка также как и для Защитника заключается в добавлении на нужные компьютеры ключей реестра. Ниже указаны конкретные ветки:

Исключение каталога
```
[SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Paths]
ИМЯ_ПАПКИ=dword:00000000
```

Где в названии параметра ИМЯ_ПАПКИ нужно ввести полный путь к папке или файлу, который будет исключен из сканирования.

Пример:
```
[SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Paths]
```
C:\windows\system32\lasys =dword:00000000

Для 64 битных систем ключ будет:
C:\windows\syswow64\lasys =dword:00000000

Путь указывается без кавычек.

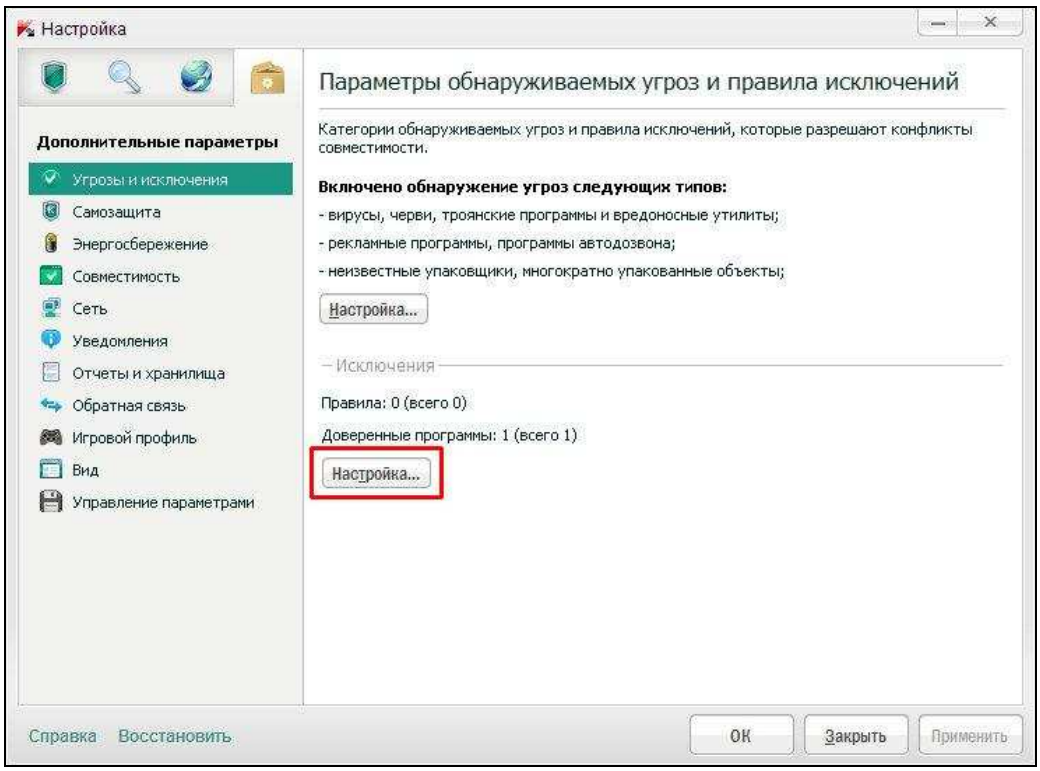
2 Антивирус Касперского

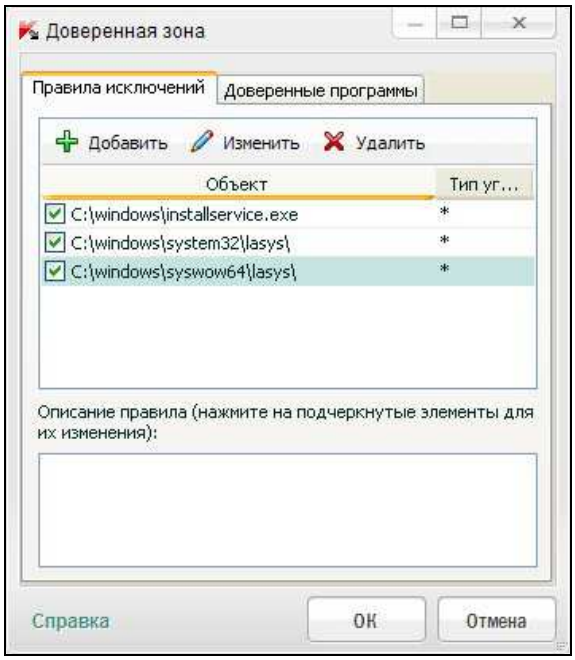
Для успешной дистанционной установки агента средствами программы LA Admin, желательно на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe и Admin$\installservice.exe Это один и тот же путь.

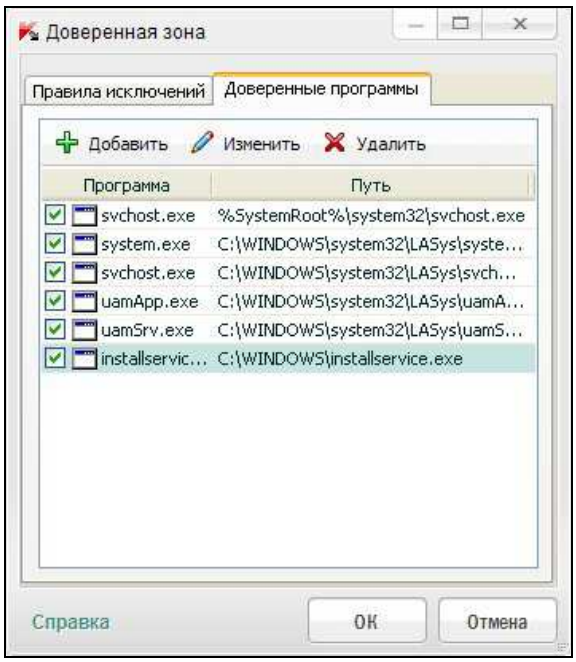
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, желательно внести в исключение антивируса либо сам каталог установки агента C:\windows\system32\lasys для 32 битных систем и syswow64\lasys для 64 битных, либо конкретные файлы system.exe, svchost.exe, uamApp.exe, uamSrv.exe, sys.dll, sysl.dll, laNetwork.exe из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

Особенность антивируса Касперского заключается в том, что в нем есть два места для внесения исключения: «Правила исключений» и «Доверенные программы». Вносить исключение надо в оба эти места.


Настройка
Параметры обнаруживаемых угроз и правила исключений
Дополнительные параметры
Угрозы и исключения
Самозащита
Энергосбережение
Совместимость
Сеть
Уведомления
Отчеты и хранилища
Обратная связь
Игровой профиль
Вид
Управление параметрами
Категории обнаруживаемых угроз и правила исключений, которые разрешают конфликты совместимости.
Включено обнаружение угроз следующих типов:
- вирусы, черви, троянские программы и вредоносные утилиты;
- рекламные программы, программы автодозвона;
- неизвестные упаковщики, многократно упакованные объекты;
Настройка...
Исключения
Правила: 0 (всего 0)
Доверенные программы: 1 (всего 1)
Настройка...
Справка
Восстановить
ОК
Закрыть
Применить


Доверенная зона
Правила исключений
Доверенные программы
Добавить
Изменить
Удалить
Объект
Тип уг...
C:\windows\installservice.exe
C:\windows\system32\lasys\
C:\windows\syswow64\lasys\
Описание правила (нажмите на подчеркнутые элементы для их изменения):
Справка
ОК
Отмена



Эта часть общая для всех версий Касперского. Ее будет достаточно для большинства версий этого антивируса.

3 Антивирус НОД32

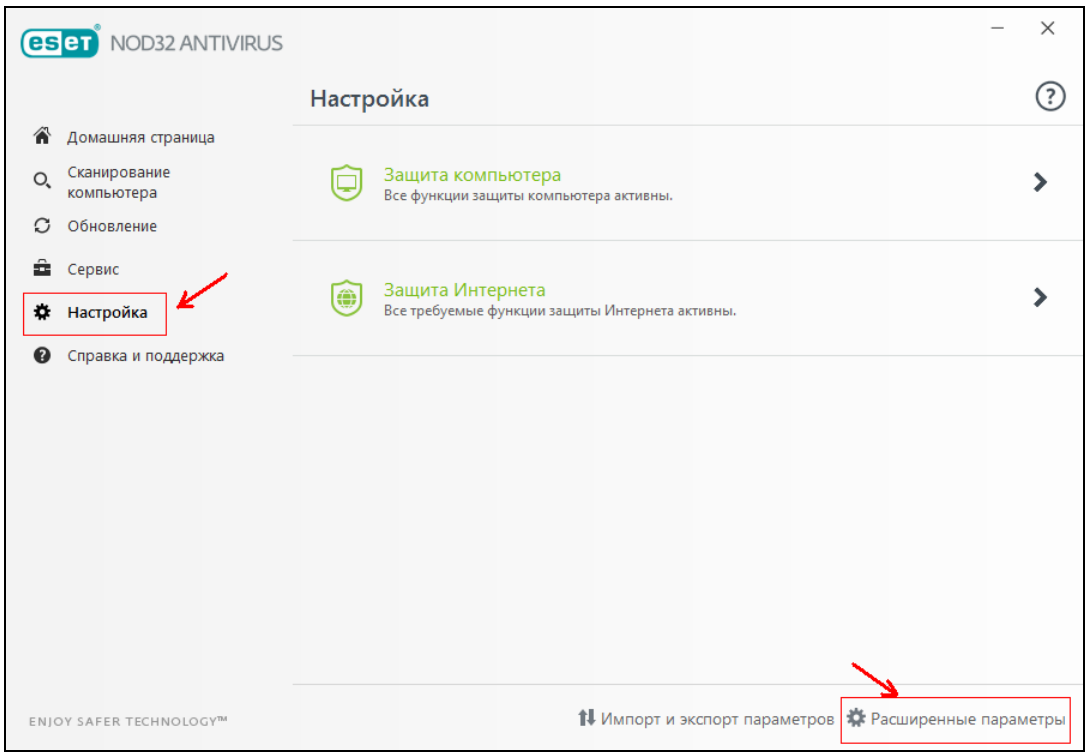
Принцип внесения исключений в НОД32 тот же, что и во все остальные антивирусы: для успешной дистанционной установки агента средствами программы LA Admin, надо на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe .

При инсталляции агента через msi файл, происходит распаковка файлов из пакета во временный каталог, поэтому, при возникновении сложностей с антивирусом, надо на время установки или приостановить антивирус или опять же временно внести темповый каталог в исключение.

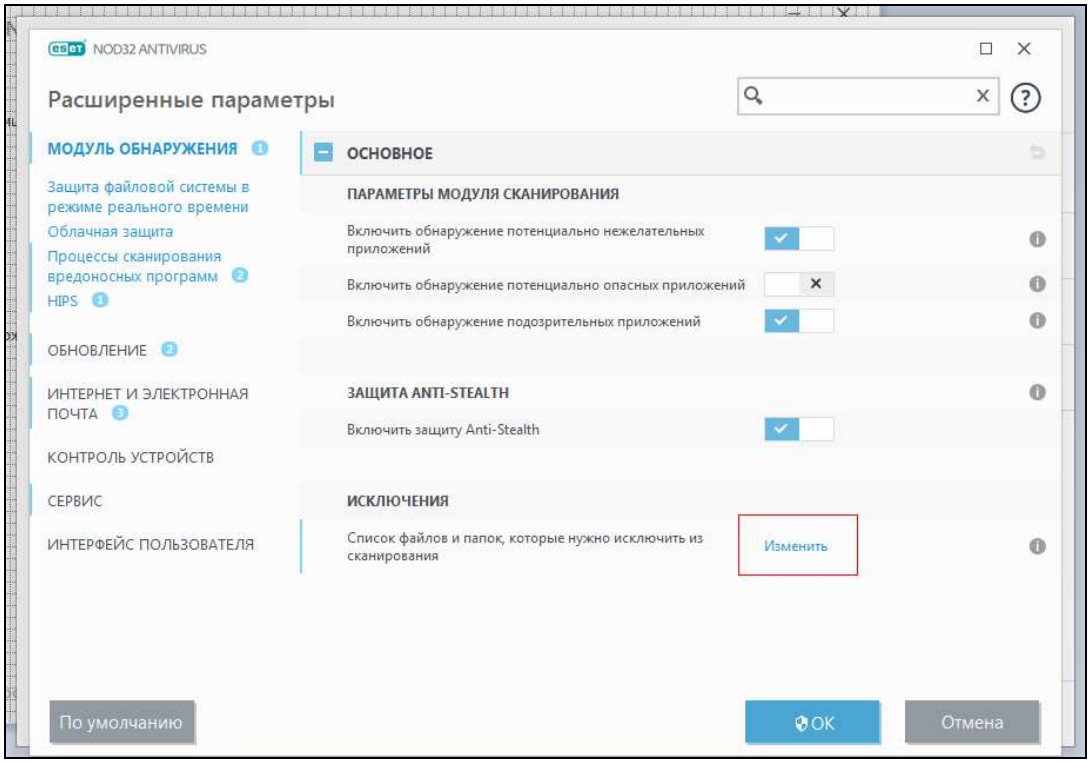
Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, для последующей работы агента на компьютере, желательно внести в исключение либо сам каталог установки агента с файлами по маске: C:\windows\system32\lasys*.* для 32 битных систем и syswow64\lasys*.* для 64 битных, либо конкретные файлы из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.

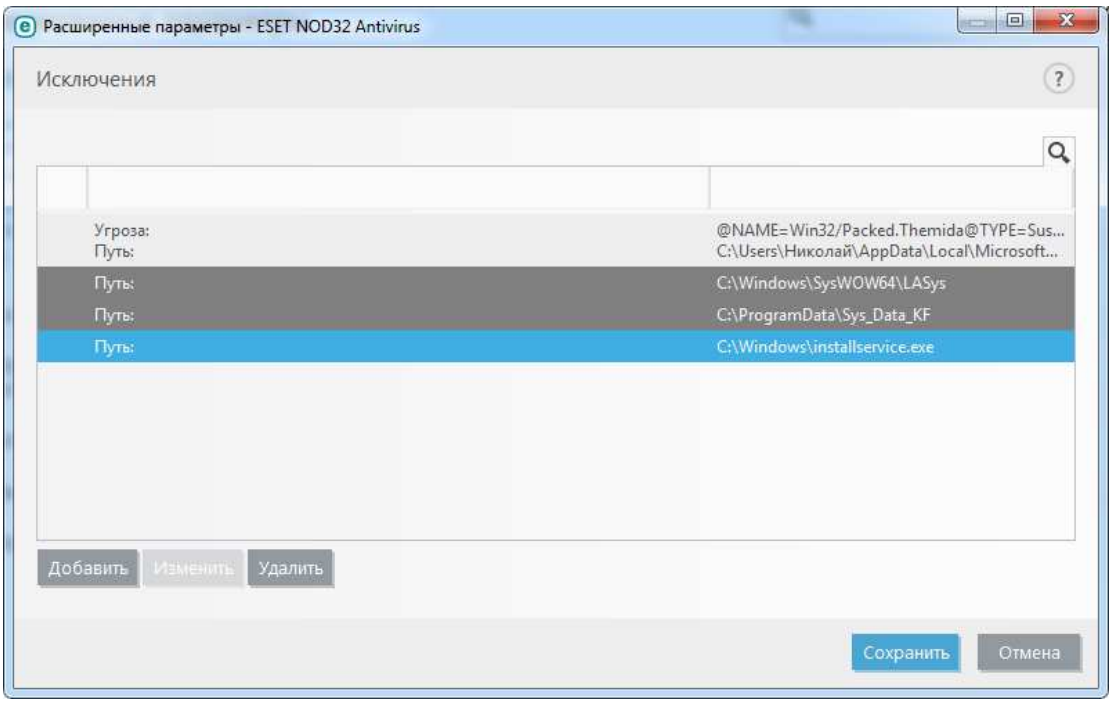
И для Nod32 надо добавить в исключение каталог временных файлов агента. На компьютерах с Windows 7 и новее это C:\ProgramData\Sys_Data_KF*.*
Для XP - C:\Documents and Settings\All Users\Application Data\Sys_Data_KF*.*



На пункте Исключения нажмите «Изменить»



И укажите в списке нужные пути исключений.



Это необходимо для того, чтобы файловый сканер антивируса не реагировал на файлы агента.

4 Антивирусы Avast, DrWeb, Avira.

Принцип внесения исключений в эти антивирусы тот же, что и во все остальные: для успешной дистанционной установки агента средствами программы LA Admin, надо на целевом компьютере внести в исключение путь до файла инсталляции агента C:\windows\installservice.exe

Все процессы следящего модуля имеют цифровую подпись и антивирусом не детектируются. Тем не менее, для последующей работы агента на компьютере, необходимо внести в исключение либо сам каталог установки агента с файлами по маске: C:\windows\system32\lasys*.* для 32 битных систем и syswow64\lasys*.* для 64 битных, либо конкретные файлы system.exe, svchost.exe, uamApp.exe, uamSrv.exe, sys.dll, laNetwork.exe из каталога установки агента.

Это позволит избежать «сюрпризов» в виде ложных срабатываний антивируса в будущем.