OSNOVO

cable transmission

ПОЛНОЕ РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Программное обеспечение для организации централизованной системы мониторинга параметров

OSNOVO MONITORING SYSTEM

www.osnovo.ru

Содержание

1. Назначение

Программное обеспечение «OSNOVO Monitoring System» (далее по тексту OMS) предназначено для организации централизованной системы мониторинга различных параметров оборудования OSNOVO (управляемые коммутаторы, инжекторы, медиаконвертеры и тд.), а также контроллера TMS-01 и выносных датчиков к нему серии TMS (датчик температуры и влажности TMS-STH, датчик сетевого напряжения TMS-SV, датчик фазы сетевого напряжения TMS-SL).

Вся полученная информация выводится в едином окне с возможностью сортировки хостов (устройств), столбцов с результатами проверки параметров и тд.

Для удобства использования ПО OMS предусмотрены журналы отчетов по нескольким категориям (аварии, проверки и тд.), графики проверок, возможность выгрузки статистки проверок в CSV файл, возможность сохранения резервной копии настроек ПО и тд.

Дистрибутив ПО OMS содержит предустановленные фильтры (пресеты) для основных параметров мониторинга управляемого оборудования OSNOVO и контроллера TMS-01 с набором датчиков.

2. Особенности программного обеспечения

- ✓ Централизованный доступ ко всей информации о результатах проверок параметров сетевого оборудования;
- ✓ Мониторинг в реальном времени по протоколу SNMP основных параметров управляемого оборудования OSNOVO:
  - Температура на выносном датчике;
  - Относительная влажность воздуха на выносном датчике;
  - Напряжение питания на основном и резервном источниках питания;
  - Суммарная потребляемая мощность (в том числе вместе с PoE);
  - Мощность PoE на каждом порте устройства
- ✓ Мониторинг в реальном времени по протоколу SNMP параметров выносных датчиков, подключенных к контроллеру TMS-01:
  - Температура на выносном датчике TMS-STH;

- Относительная влажность воздуха на выносном датчике TMS-STH;
- Напряжение источника питания с помощью контроллера TMS-01
- Сетевое напряжение на выносном датчике TMS-SV;
- Наличие фазы сетевого напряжения на выносном датчике. TMS-SL

- ✓ Отправка результатов проверок на электронную почту;
- ✓ Звуковое оповещение в случае сбоя и восстановления после сбоя
- ✓ SMS оповещение в случае сбоя и восстановления после сбоя;
- ✓ Встроенный MIB браузер, позволяющий добавлять MIB файлы сетевого оборудования (см. раздел «8.3 MIB браузер»);
- ✓ Сканер IP адресов для быстрого поиска всех сетевых устройств в локальной сети;
- ✓ Журналы, отчеты и графики для удобного восприятия результатов мониторинга и их анализа.
- ✓ Другие типы проверок (ICMP, ARP, HTTP, WMI, NetBIOS и тд.)

3. Структура и принцип работы ПО «OSNOVO Monitoring System»

3.1 Структура ПО «OSNOVO Monitoring System»

ПО «OSNOVO Monitoring System» состоит из 2х частей:

1) Ядро (служба) мониторинга – служба Windows, которая является основным механизмом опроса сетевых устройств, сигнализации, и сбора статистики.
2) Приложение для рабочего стола Windows – непосредственно графическая консоль (рис. 1) для ведения базы мониторинга, добавления новых хостов (сетевых устройств), проверок, просмотра их состояния, редактирования всех настроек программы, просмотра графиков, создания отчётов.

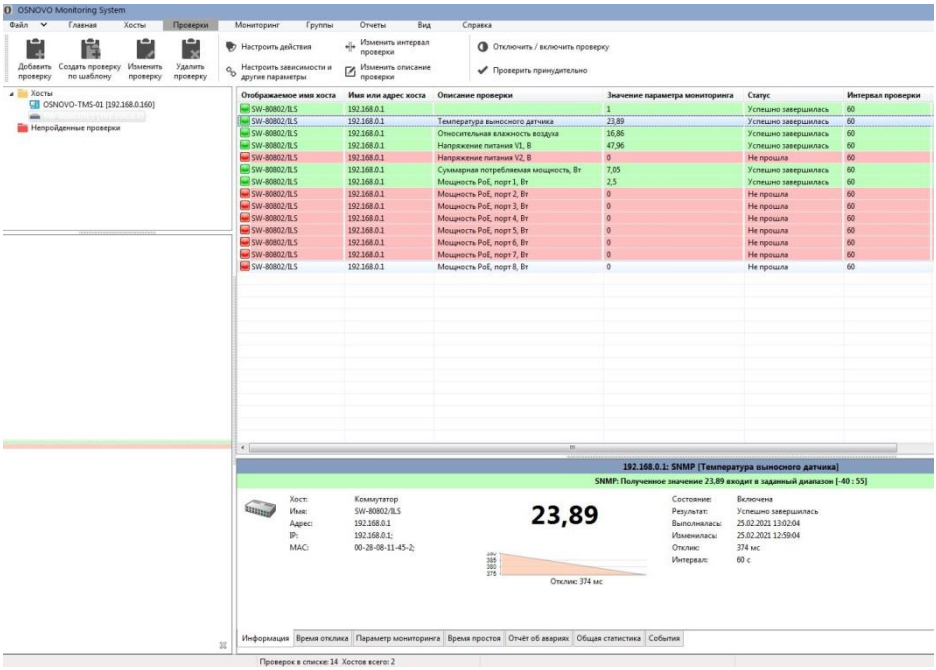


Рис. 1 Графическая консоль ПО OMS

3.2 Принцип работы ПО «OSNOVO Monitoring System»

Работа ПО основывается на периодическом опросе хостов (сетевых IP устройств), находящихся в базе мониторинга путем последовательного выполнения заданных для каждого из них проверок.

В зависимости от результата выполнения этой процедуры проверки получают статус (пройдена – зеленая, не пройдена – красная), результаты записываются в файловую базу данных.

1. С помощью графической консоли или web-интерфейса создаётся файловая (локальная) база мониторинга хостов и проверок.

2. Служба мониторинга принимает введённые данные и начинает циклическое выполнение проверок, обновление их статуса, формирование файловой базы статистики времени выполнения

проверок и значений параметров мониторинга (температура, влажность, напряжение и тд.)

3. Графическая консоль получает статус выполненных проверок и отображает его в виде цветовой раскраски списка, строит графики, формирует отчёты на основе накопленной статистики.

4. В случае сбоя, служба мониторинга инициирует выполнение действий: запись в журнал (в базе данных и дублирование в файловый, локальный), SMS информирование, E-mail информирование, перезапуск/остановка служб и/или ПК, выдача сообщения на экран, проигрывание звукового файла, запуск внешних программ и команд с параметрами. Выполнение последних трёх действий служба делегирует графической консоли, поэтому она должна быть запущена в это время.

5. Служба мониторинга при проверке хостов сети использует множество стандартных протоколов: SNMP, TCP, ICMP, ARP, HTTP, FTP, WMI, NetBIOS. Графическая консоль и служба мониторинга поддерживают постоянную связь по TCP-протоколу. Таким образом, все изменения, внесённые в базу мониторинга (изменение параметров проверок, добавление новых и так далее), незамедлительно взаимодействуют со службой мониторинга. Все результаты проверок сразу же передаются от службы графической консоли и отображаются в ее интерфейсе.

4. Системные требования

3.1 Общие рекомендации

Для корректной работы программы необходим компьютер или сервер:

- ✓ Минимальный объём оперативной памяти - 2 ГБ.
- ✓ Microsoft® Windows XP или старше (server или workstation, 32 или 64 бит).

3.2 Производительность мониторинга

Для компьютера с минимальными системными характеристиками не рекомендуется создавать базы мониторинга более, чем на 2 000 проверок.

Примерно то же количество проверок является предельным, если вы используете для мониторинга виртуальную машину.

Для более объёмных баз мониторинга рекомендуется выделять отдельный физический сервер.

Максимальное число проверок, которое может быть выполнено одной службой мониторинга без существенной потери производительности, зависит от их типа:

- ICMP, SNMP v1,2c, ARP, HTTP, файловые проверки – самые менее ресурсозатратные типы проверок. Проверок такого типа одна служба мониторинга может выполнять до 10 000 с интервалом от 30 секунд.
- SNMP v3 – при запуске проверок этого типа выполняется около 40 сетевых запросов в секунду. Поэтому, к примеру, на компьютере с двухядерным процессором 1 Гц не рекомендуется мониторинг более 5 000 проверок этого типа с интервалом менее 60 секунд. Загрузка процессора при этом составит не менее 50%.

- WMI – проверки этого типа (WMI-запросы, сетевой диск, локальный принтер) требовательны к ресурсам. Поэтому не рекомендуется создавать более 200 проверок с интервалом до 30 секунд, 1 000 проверок с интервалом 150 секунд и так далее.
- NetBIOS – проверки этого типа (состояние службы, процесса, контроль ПО, журнал событий) требовательны к ресурсам, как и WMI проверки. Не рекомендуется создавать более 200 проверок с интервалом до 30 секунд, 1 000 проверок с интервалом 150 секунд и так далее.

Внимание! Не рекомендуется нагружать одну службу мониторинга более, чем 10 000 проверками при любых конфигурациях оборудования.

3.3 Поддерживаемые операционные системы

Программа работает в 32 и 64 битных версиях операционных систем:

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows 8 / 8.1
- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows XP (не рекомендовано)

Следует учесть, что включенный "Контроль учётных записей" (UAC, начиная с Windows 7) может вызвать трудности с удалённым получением информации в ходе выполнения проверок. Рекомендуется устанавливать программу с полными правами администратора ПК.

При проверках подключения к TCP-портам следует учитывать, что в ОС Windows XP и выше не допускается более 10 одновременных TCP-подключений. Это может сказаться на производительности программы. Следует с осторожностью использовать этот метод.

3.4 Требования к аппаратному обеспечению

Требования зависят от типа проверок в базе мониторинга и их интервала.

Следующие минимальные необходимые параметры системы приведены для распространённых типов проверок ICMP и SNMP v1, 2c:

- **CPU:** 1 ГГц, x86/x64.
- **ОЗУ:** 2048 МБ.
- **HDD:**

  Для установки программы необходимо иметь не менее 100 Мб свободного пространства. В процессе работы программа генерирует статистику. Объём зависит от количества проверок и их интервала. Для успешной работы программы в течение длительного времени без очистки статистики необходимо не менее 2 Гб свободного пространства. Объем статистики одной проверки за один опрос - 40 байт. При интервале в 60 секунд за сутки одна проверка накопит не менее 60 Кб данных.
- **Устойчивое сетевое соединение:**

  Взаимодействующие части программы (служба и графическая консоль) требуют наличия стабильного сетевого соединения по TCP-протоколу.
- **Разрешение экрана:**

  Рекомендуемое разрешение - 1200x800 или выше. Минимальное - 1024x768.

5. Порядок установки дистрибутива ПО «OSNOVO Monitoring System»

1. Скачайте дистрибутив ПО OMS с сайта www.osnovo.ru (рис. 2)

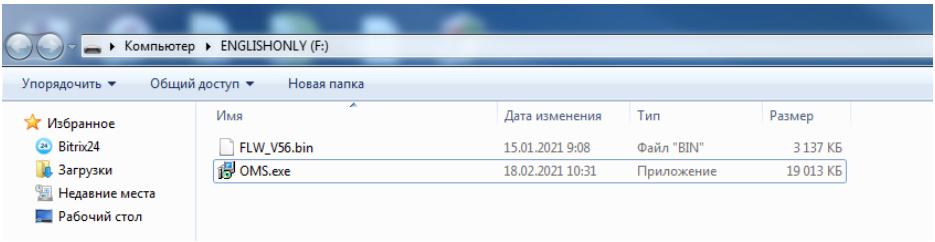


Рис. 2

2. Запустите его с правами администратора (рис. 3)

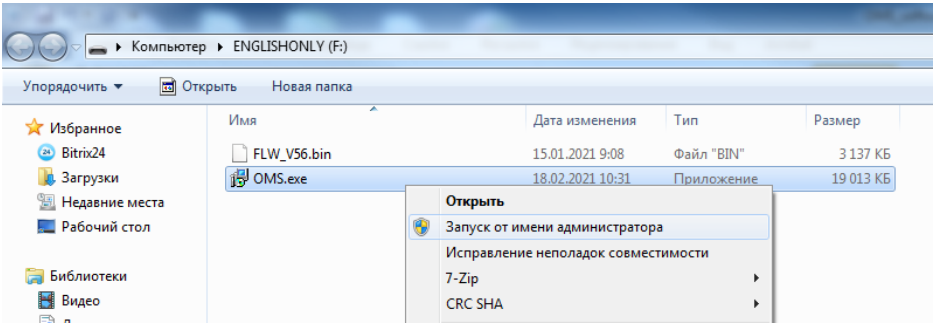
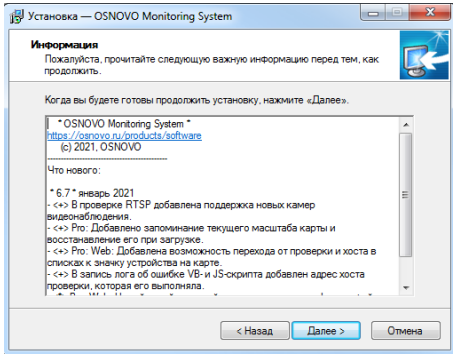


Рис. 3

3. Пройдите все шаги установки с указанием пути установки и прочими параметрами. (Рис 4-11)



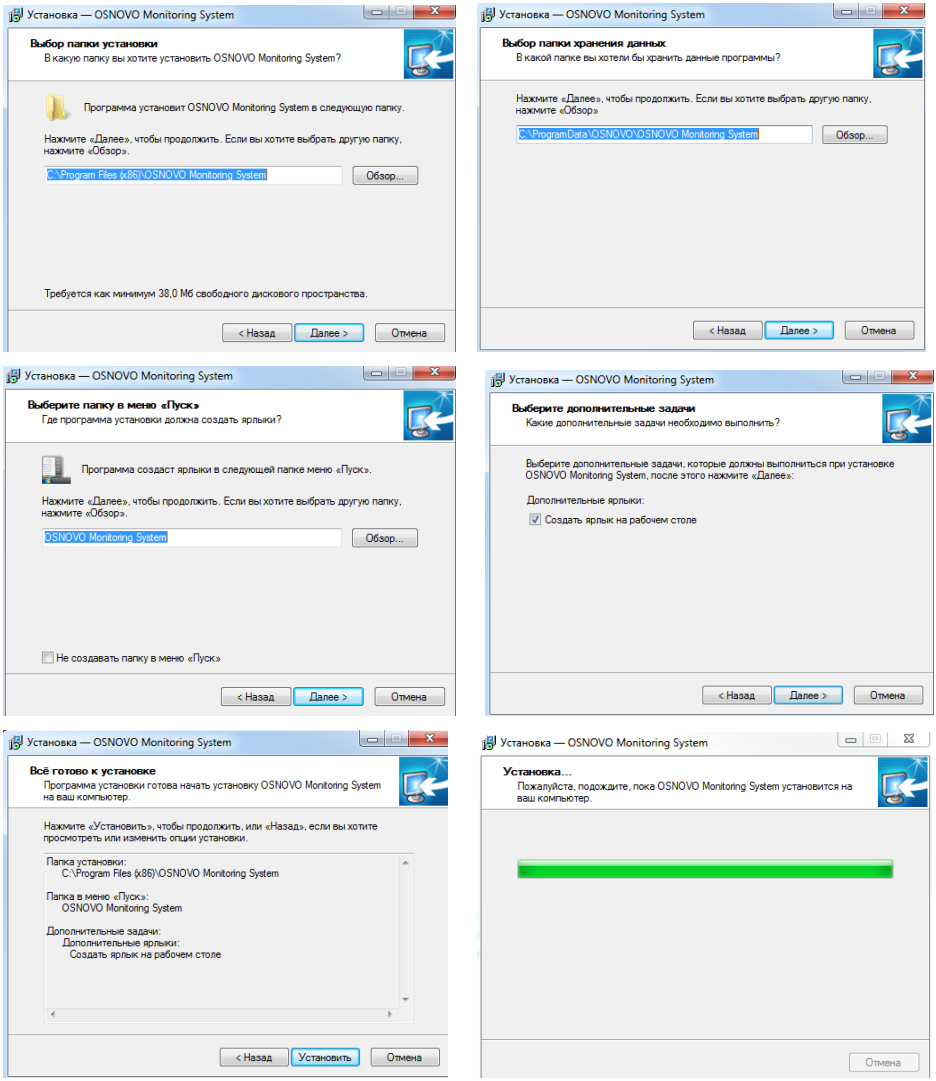


Рис. 4 -11

4. Запустите программу по окончании установки (запуск также возможен с ярлыка на рабочем столе ПК).

6. Начало работы с ПО «OSNOVO Monitoring System» и активация лицензионного ключа

Главное окно графической консоли OMS представлено на рис. 12

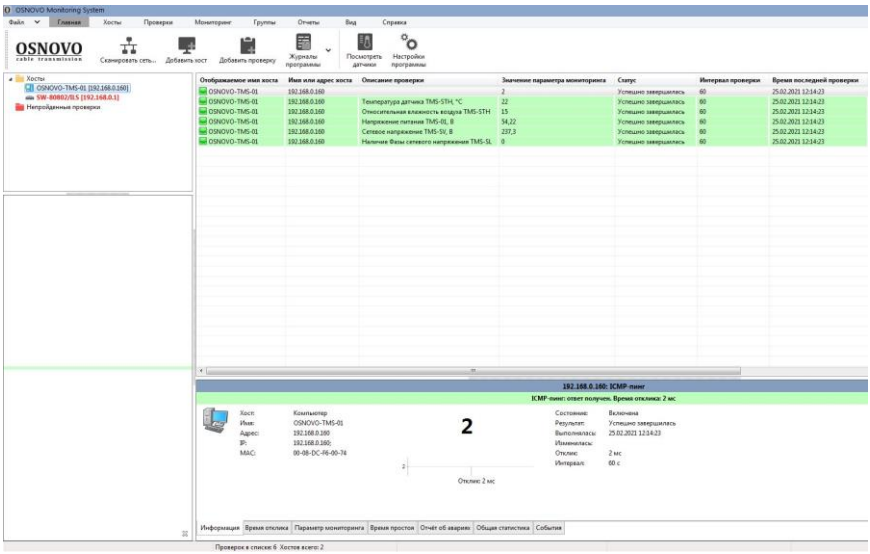


Рис. 12 Главное окно ПО OMS

По умолчанию пользователю предоставляется бесплатная 30-дневная версия ПО. Чтобы снять ограничение на пробный 30-дневный период необходимо пройти активацию программы с помощью лицензионного ключа. Количество доступных проверок зависит от версии приобретенного ПО OMS (25, 100 и тд проверок, подробная информация находится на сайте osnovo.ru)

Порядок активации лицензионного ключа:

1) Откройте в главном меню пункт «Справка» (рис. 13)

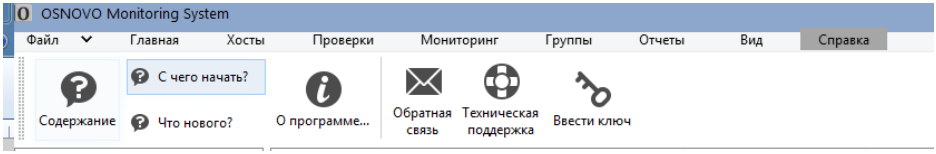


Рис. 13

2) Выберите пункт «Ввести ключ» (рис. 14)

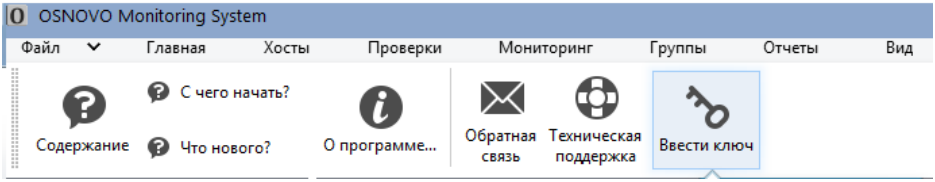


Рис. 14

3) Введите в появившееся поле ключ (он же регистрационный код) с клавиатуры или вставьте заранее скопированный в буфер ключ комбинацией Ctrl+V или кнопкой «Вставить из буфера» (рис. 15)

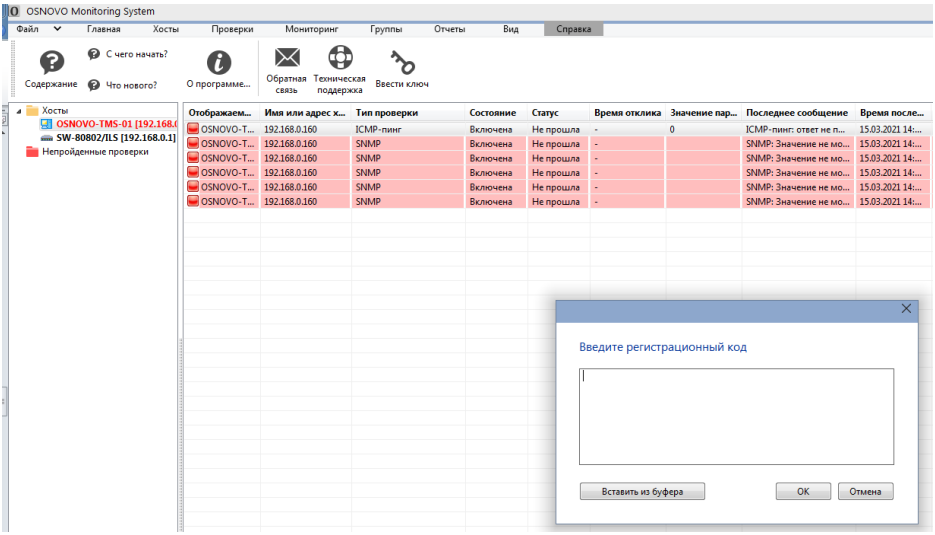


Рис. 15

4) Нажмите ОК

В случае, если ключ прописан корректно Вы увидите подтверждение регистрации. Если ключ прописан некорректно (ошибки при вводе), устаревший ключ и тд – повторите весь порядок активации заново.

7. Описание интерфейса ПО «OSNOVO Monitoring System»

Весь интерфейс графической консоли ПО OMS разделен на 6 частей:

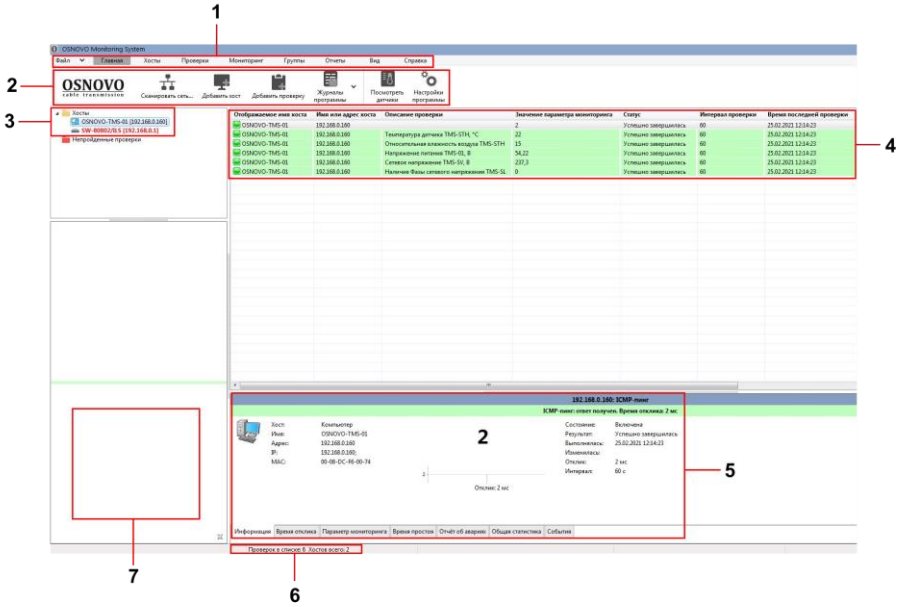


Рис. 16 Интерфейс ПО OMS

№ п/п	Назначение
1	Главное меню
2	Панель инструментов
3	Список хостов для мониторинга
4	Список проверок
5	Панель информации
6	Строка состояния
7	Панель навигации

1, 2 Главное меню и панель инструментов

Из главного меню программы осуществляется вызов всех доступных функций программы, которые отображаются в поле «Панель инструментов»

Из пункта меню Файл (рис. 17) вызываются функции:

1. Настройки программы
2. Создание резервной копии настроек программы и мониторинга
3. Восстановление настроек программы и мониторинга из резервной копии
4. Выгрузка статистики проверки в файл в формате CSV
5. MIB-браузер (см. раздел «8.3 MIB браузер»)
6. Выход из программы

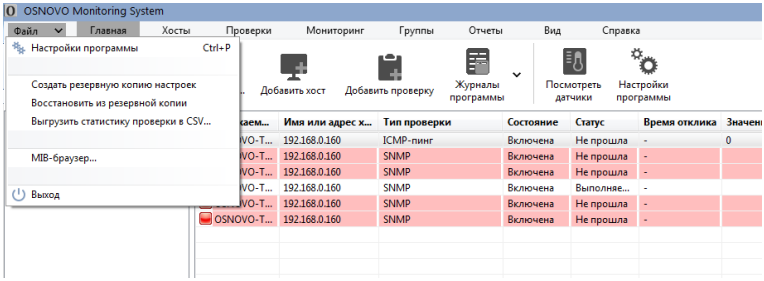


Рис. 17

Из пункта Главная (рис. 18) вызываются функции:

1. Сканировать сеть
2. Добавить хост
3. Добавить проверку
4. Журналы программы
5. Посмотреть датчики
6. Настройки программы

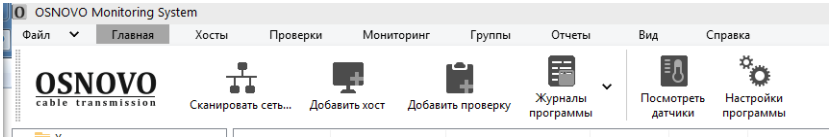


Рис. 18

Из пункта Хосты (рис. 19) вызываются функции:

1. Сканировать сеть
2. Импортировать из текстового файла
3. Добавить хост
4. Изменить хост
5. Удалить хост
6. Найти хост в базе
7. Задать время простоя
8. Очистить статистику
9. Настроить сбор статистики
10. Проверить принудительно
11. Включить все проверки
12. Отключить все проверки
13. Выделить все хосты

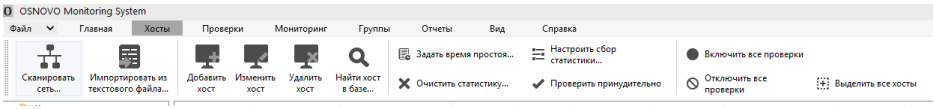


Рис. 19

Из пункта меню Проверки (рис. 20) вызываются функции:

1. Добавить проверку
2. Создать проверку по шаблону
3. Изменить проверку
4. Удалить проверку
5. Настроить действия
6. Настроить зависимости и другие параметры
7. Изменить интервал проверки
8. Изменить описание проверки
9. Отключить включить проверку
10. Проверить принудительно

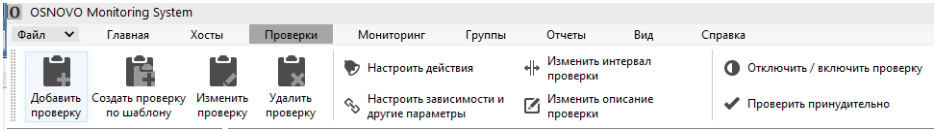


Рис. 20

Из пункта меню Мониторинг (рис 21) вызываются следующие функции:

1. Планировщик задач
2. Прием SNMP Trap
3. Мониторинг Syslog
4. Подключиться к службе мониторинга
5. Запустить мониторинг
6. Остановить мониторинг
7. Настройки мониторинга
8. Настройки сигнализации
9. Управление службой мониторинга

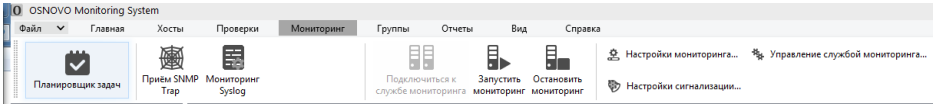


Рис. 21

Из пункта меню Группы (рис. 22) вызываются следующие функции:

1. Добавить группу
2. Удалить группу
3. Переименовать группу
4. Добавить вложенную группу

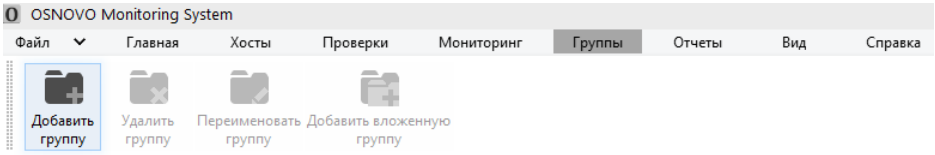


Рис. 22

Из пункта меню Отчеты (рис. 23) вызываются следующие функции:

1. Журналы программы
2. Журнал Windows
3. Отчеты и графики

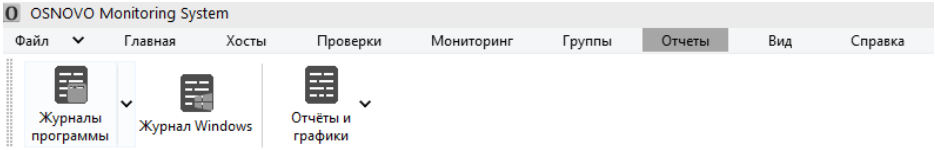


Рис. 23

Из пункта меню Вид (рис. 24) вызываются следующие функции:

1. Панель информации
2. Панель навигации
3. Панель помощи
4. Показывать дату на осях
5. Темный фон
6. Настроить столбцы списка проверок
7. Показывать только сбойные проверки

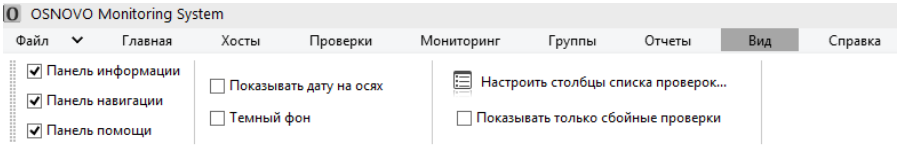


Рис. 24

Из пункта меню Справка (рис. 25) вызываются следующие функции:

1. Содержание файла справки FAQ
2. С чего начать?
3. Что нового?
4. О программе
5. Обратная связь
6. Техническая поддержка
7. Ввести ключ

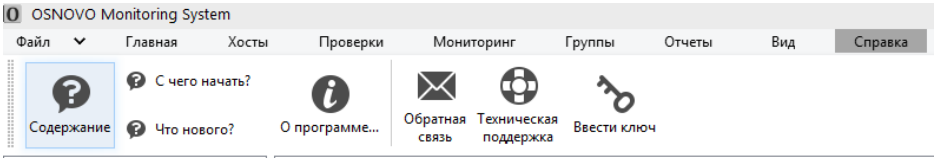


Рис. 25

3. Список хостов для мониторинга

В списке мониторинга в виде дерева располагаются хосты (сетевые IP устройства), объединенные в группы (папки). Для каждого хоста можно задать произвольное количество проверок.

При выборе конкретного хоста в дереве в списке проверок отображаются только те проверки, которые принадлежат этому хосту.

При выборе группы в списке проверок отображаются все проверки содержащихся в этой группе хостов.

По умолчанию в дистрибутив ПО OMS добавлено несколько хостов (контроллер TMS-01 с комплектом выносных датчиков и коммутатор OSNOVO с функцией мониторинга) с предустановленными проверками (пресеты), рис. 26

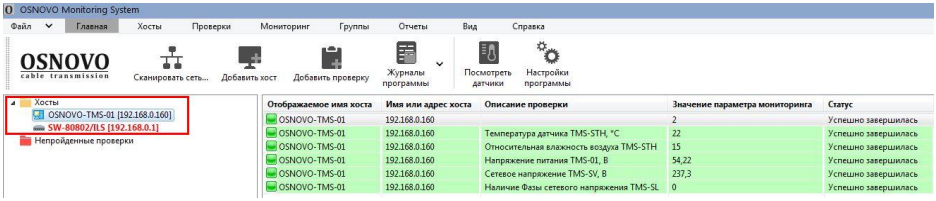


Рис. 26

4. Список проверок

В списке проверок отображаются записи проверок выделенной в дереве группы или хоста.

Как и в случае с пресетами хостов, по умолчанию в дистрибутив ПО OMS добавлены заранее сконфигурированные пресеты проверок с описанием (рис. 27)

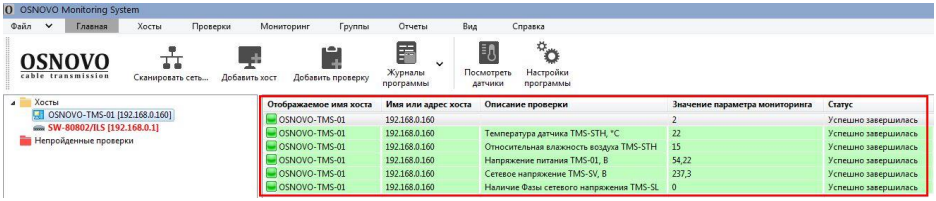


Рис. 27

5. Панель информации

На информационной панели в удобном виде отображается состояние выделенной в списке проверки и некоторые ее параметры

На закладке Информация отображается сводная информация по выделенной в списке проверке (рис. 28)

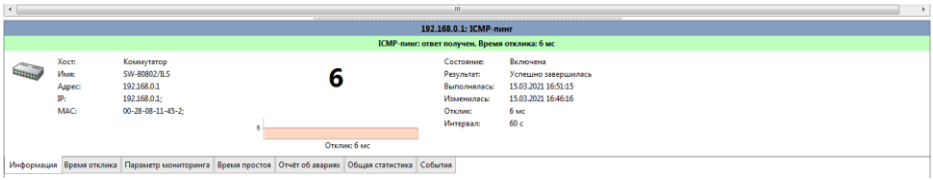


Рис. 28

На вкладке Время отклика отображается график изменения времени отклика хоста при проверке за последний час (рис. 29).

Рис. 29

На вкладке Параметр мониторинга отображается график изменения параметра мониторинга за последний час (рис. 30)

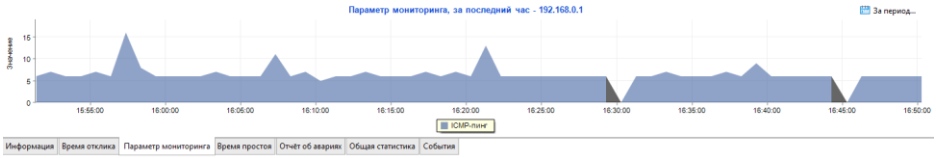


Рис. 30

На вкладке Время простоя отображается время простоя за выбранный период времени (рис 31)

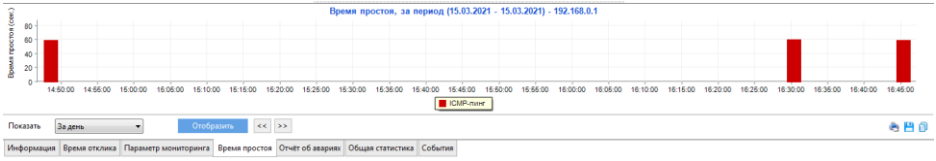


Рис. 31

На вкладке Отчет об авариях отображается в виде таблицы информация об авариях для выбранного параметра мониторинга (рис. 32)

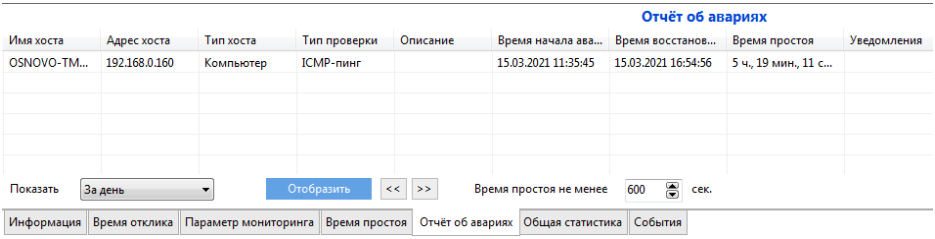


Рис. 32

На вкладке Общая статистика отображается в виде таблицы (рис. 33) сводная информация о проверке:

- ✓ число успешных завершений проверки;
- ✓ число отказов;
- ✓ количество перерывов в процессе мониторинга (во время остановки службы мониторинга);
- ✓ общее время простоя хоста;
- ✓ общее количество значений статистики;
- ✓ количество ошибок опроса сенсора;
- ✓ дата начала и дата конца сбора статистики.

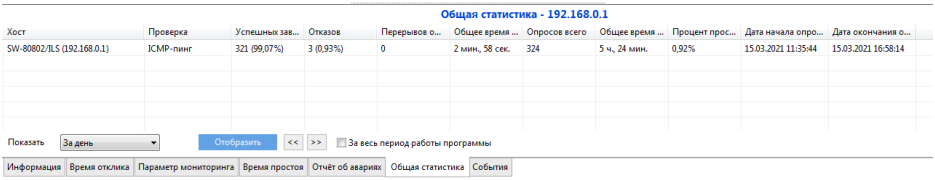


Рис. 33

Информационную панель можно спрятать, сняв галку с пункта главного меню Вид / Панель информации.

6. Строка состояния

Небольшое поле внизу интерфейса графической консоли ПО OMS отображающее общее количество хостов и сконфигурированных для них проверок (рис. 34)

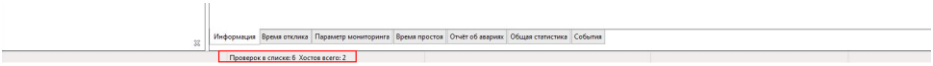


Рис. 34

7. Панель навигации

Если проверок в списке очень много (так, что они не умещаются в видимой области списка), переход к ним можно легко осуществить через панель навигации (рис 35, поле выделено красной рамкой)

По сути, панель навигации является уменьшенной копией списка проверок. Панель навигации позволяет вовремя отреагировать на сбой проверки, т.к. выделенная красным цветом запись сразу становится видна, несмотря на то, что находится вне видимой зоны списка.

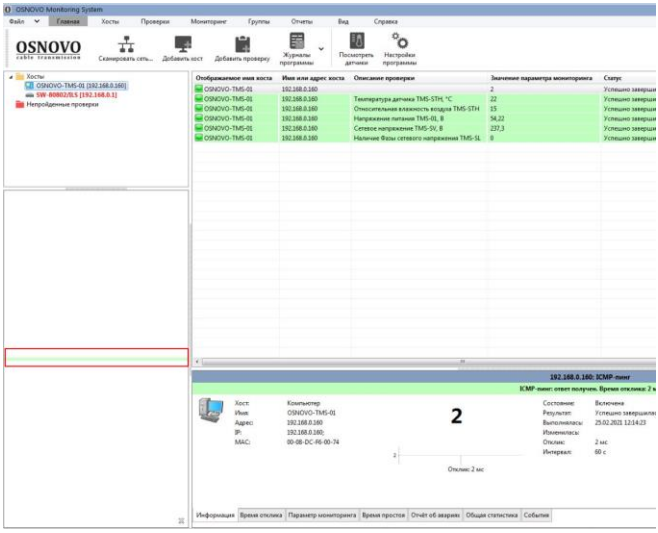


Рис. 35

Панель навигации можно спрятать, сняв галочку у пункта главного меню Вид / Панель навигации.

8. Подробное описание основных функций и возможностей ПО «OSNOVO Monitoring System»

8.1 Создание списка хостов сети

Список хостов (сетевых устройств), для которых в дальнейшем будут сконфигурированы проверки, создается несколькими способами:

1. С помощью «мастера сканирования сети»
2. Вручную через инструмент «Добавить хост»
3. По шаблону через соответствующий инструмент.

В дистрибутив ПО OMS в список хостов добавлены заранее сконфигурированные хосты – контроллер TMS-01 с набором датчиков и коммутатор OSNOVO с функцией мониторинга параметров. Также сконфигурированы основные проверки для этих хостов (рис. 36)

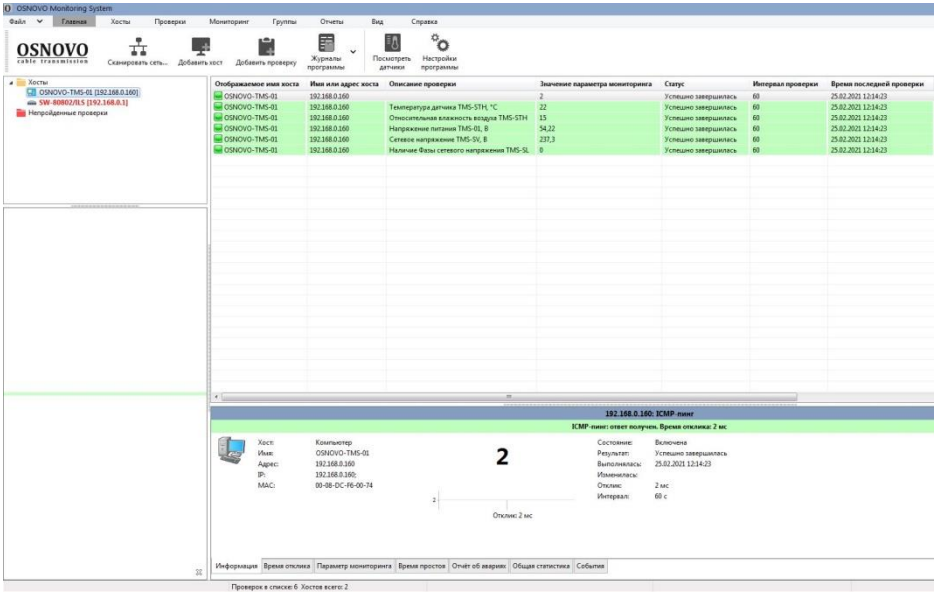


Рис. 36

8.1.1 Мастер сканирования сети

Чтобы вызвать Мастер сканирования сети необходимо выбрать во вкладке Главная инструмент Сканировать сеть (также дублирован в вкладке Хосты), рис. 37-38

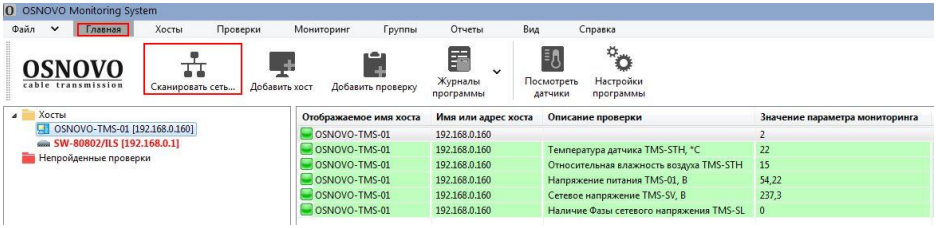


Рис. 37

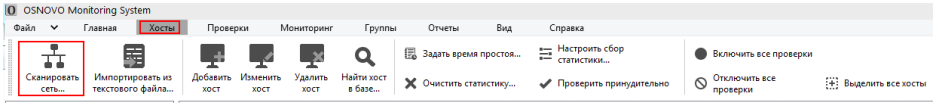


Рис. 38

Для поиска сетевых устройств (хостов) мастер использует 2 способа сканирования сети (рис. 39):

1) Сканирование диапазона IP адресов – данный способ позволяет обнаружить максимальное количество устройств и обладает следующими преимуществами:

- многопоточность, что обеспечивает высокую скорость сканирования диапазона;
- позволяет определять различные виды устройств: принтеры (локальные и сетевые), коммутаторы, хабы, сервера, сервера баз данных, роутеры, WiFi точки доступа и т.д.;
- применяет сразу несколько эффективных способов поиска устройств в сети (ICMP-пинг, сканирование списка TCP-портов, ARP-запросы);
- позволяет получать информацию из устройств по SNMP (коммутаторы, принтеры, WiFi и т.д.);
- позволяет сканировать сразу несколько диапазонов IP-адресов.

Если у вас большая коммутируемая сеть, то рекомендуется использовать этот способ сканирования.

2) Импорт из сетевого окружения – данный способ работает несколько быстрее, но не все устройства могут быть найдены.

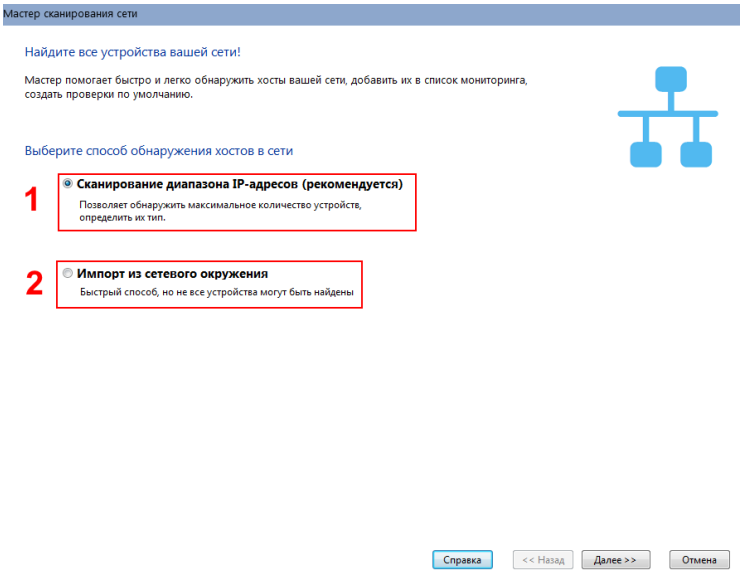


Рис. 39

При импорте из сетевого окружения необходимо на последующих шагах Мастера следовать его подсказкам.

Процедура процесса сканирования диапазона адресов описана ниже.

Шаг 1. Задание диапазона IP адресов (рис. 40)

На первом шаге задаются диапазоны сканирования. Процедура выполняется в несколько этапов:

1. В полях *Начальный адрес* и *Конечный адрес* вводятся границы сканирования подсети. Для автоматического определения диапазона возможных адресов вашей сети необходимо выбрать текущий сетевой *Интерфейс*
2. После заполнения полей адресов необходимо нажать кнопку *Добавить*, после чего выбранный диапазон занесется в список сканируемых диапазонов. Удалить диапазон из списка можно

нажатием соответствующей кнопки *Удалить*. Для того чтобы диапазоны в списке были просканированы, необходимо выделить их галкой.

3. Нажать кнопку Далее, чтобы перейти к Шагу 2

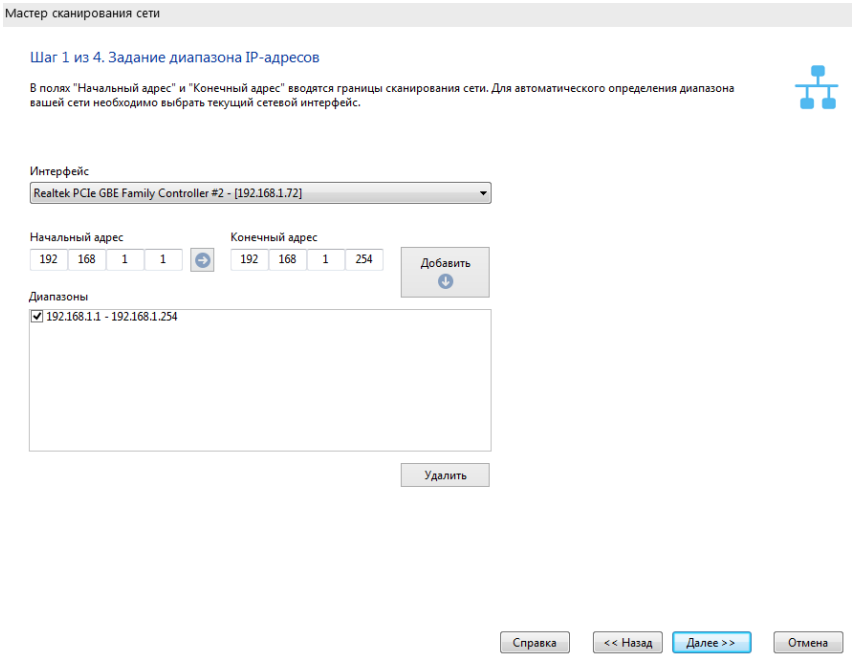


Рис 40

Шаг 2. Задание способа и параметров сканирования

Мастер предоставляет для выбора 4 способа поиска устройств в сети:

1. ICMP-пинг (рис. 41)

Параметр *Количество пакетов* отвечает за число ICMP-пакетов, отправляемых программой по каждому сканируемому адресу. В сетях с высоким трафиком одного пакета может быть недостаточно для получения отклика от существующего хоста. В этом случае рекомендуется задавать не менее 3-4 пакетов.

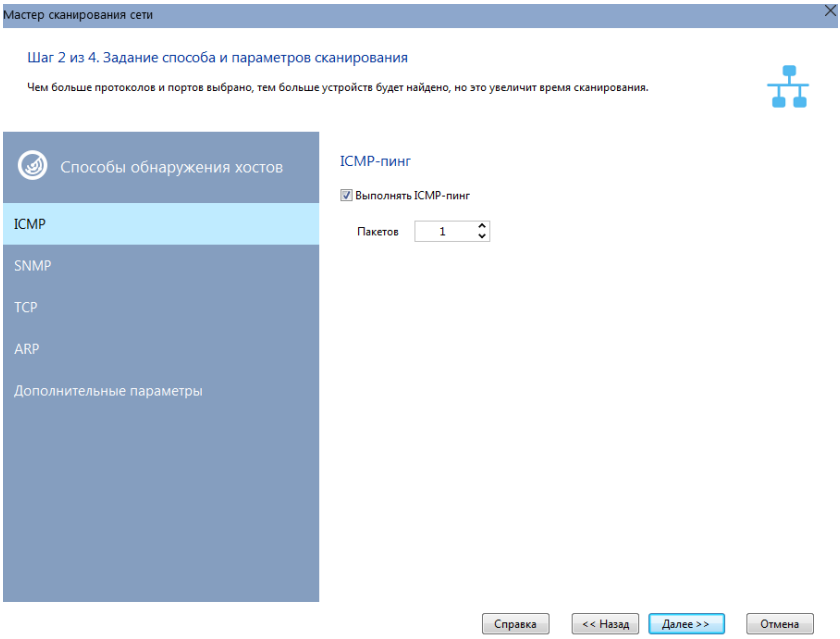


Рис. 41

2. Сканирование устройств, поддерживающих протокол SNMPv3 (рис. 42)

Необходимо в строке *Community или Username для SNMPv3* указать необходимые данные в синтаксисе протокола SNMP.

По полученной по SNMP информации Мастер может идентифицировать коммутаторы (switch), хабы, роутеры, принтеры, WiFi точки доступа, радиороутеры и т.д.

При поиске устройств с активным SNMP-агентом Мастер пытается подключиться к очередному адресу, используя заданные имена сообществ (Community). Эти имена могут быть перечислены через запятую в поле *Community или Username*. Наиболее распространенными, задаваемыми по умолчанию, именами сообществ являются public, private, rmon.

Если вы уверенны, что на ваших устройствах заданы другие имена, необходимо указать их в списке.

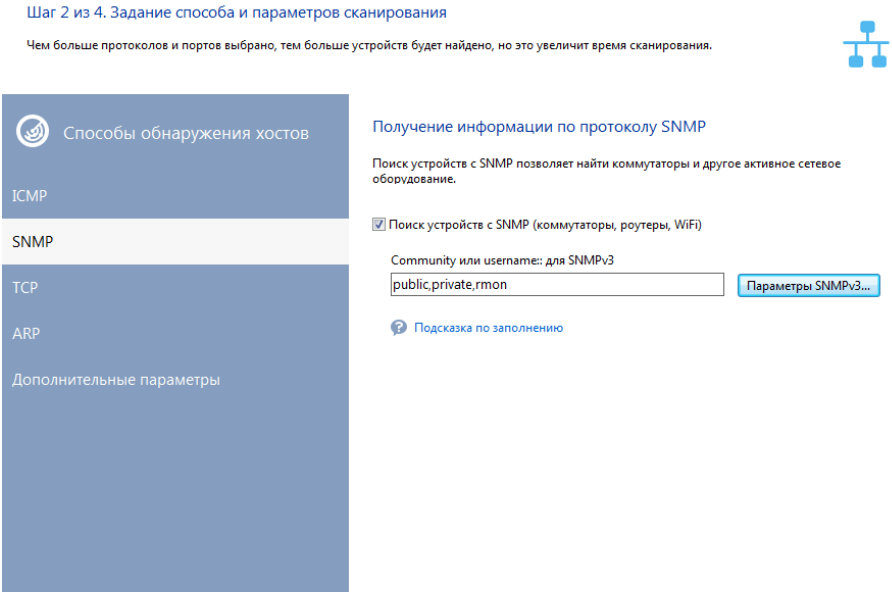


Рис. 42

3. Сканирование списка TCP портов (рис. 43)

Для сканирования TCP-портов необходимо задать список портов, по которым устройства могут быть найдены в сети. Самыми распространенными открытыми портами в сетях Microsoft являются 139 (NetBIOS), 21 (FTP), 80 (HTTP).

⚠ *ВАЖНО! При выборе метода сканирования портов необходимо учитывать, что ваши действия в большинстве случаев могут расцениваться брандмауэрами, как атака и повлечь за собой соответствующие последствия.*

Кроме этого, ОС Windows XP и выше не позволяют одновременного сканирования группы TCP-портов и на уровне драйверов искусственно замедляют процесс.

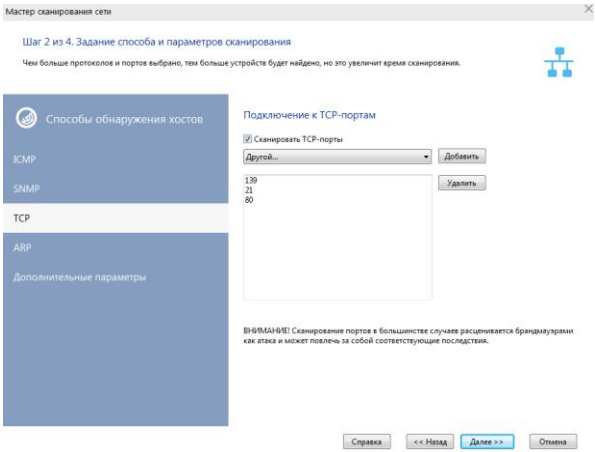


Рис. 43

4. ARP-пинг (IP>MAC), рис. 44

ARP-запросы заключаются в попытке определения MAC-адреса хоста по его IP-адресу. Если MAC-адрес может быть получен, Мастер помещает данный хост в список результатов поиска.

Существует вероятность, что программа может найти несуществующие хосты. Дело в том, что на коммутаторе в адресной таблице могут оставаться устаревшие или зарезервированные записи. В этом случае следует просто снять с них галки в окне результатов.

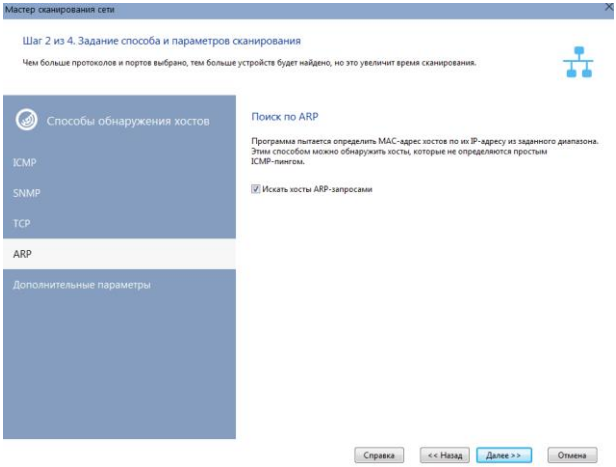


Рис. 45

В *Дополнительных параметрах* (рис. 46) для всех способов сканирования необходимо задать Время ожидания ответа – время, в течение которого Мастер будет ждать ответ от сканируемого хоста

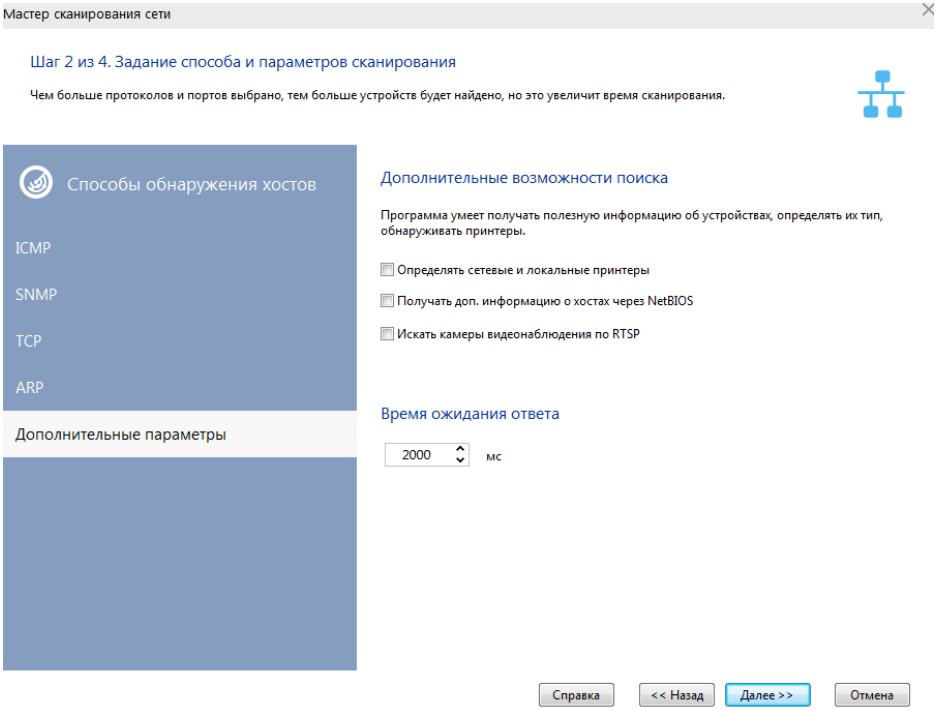


Рис. 46

Если в вашей сети есть серверы печати или сетевые принтеры, можно задать их поиск. Функция также может найти локально подключенные к компьютерам принтеры.

Мастер может автоматически найти все сервера, сервера БД в сети, получить другую полезную информацию о найденных компьютерах (тип ОС, комментарий и т.д.). Для этого необходимо выбрать опцию «*Получать доп. информацию через NetBIOS*». Функция будет работать только в том случае, если протокол NetBIOS разрешен политикой безопасности на вашем компьютере и компьютерах вашей сети.

Также доступен поиск IP камер по протоколу RTSP. Для этого отметьте пункт «*Искать камеры видеонаблюдения по RTSP*».

Шаг. 3 Поиск и отбор хостов для внесения в список мониторинга (рис. 47)

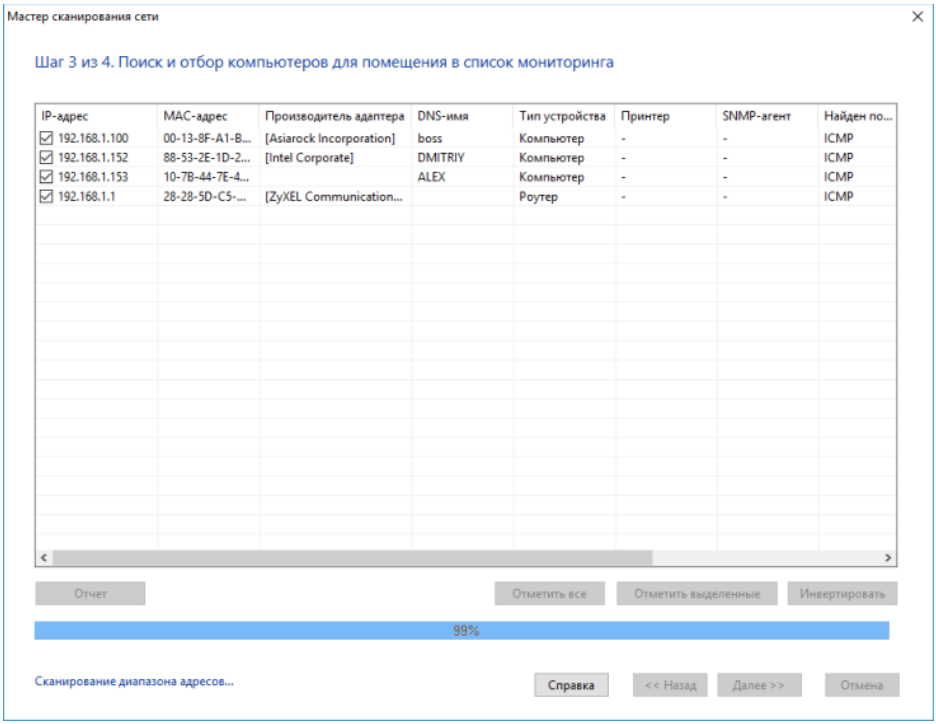


Рис. 47

Процесс сканирования начинается незамедлительно.

Сначала осуществляется попытка обнаружения сетевых и локальных принтеров. Эта процедура может занимать продолжительное время, в течение которого программа может не отвечать на запросы и будет недоступной кнопка «*Остановить*».

После этого производится поиск устройств по протоколу NetBIOS, что также может занять какое-то время.

После выполнения двух подготовительных процедур программа начинает непосредственный перебор всех IP-адресов заданных изначально диапазонов. О ходе процесса сигнализирует индикатор прогресса и надпись в нижнем левом углу Мастера *"Сканирование диапазона адресов..."*.

Ход процесса сканирования можно остановить, нажав кнопку *«Остановить»*.

Найденные в процессе сканирования хосты помещаются в список результатов. Существует возможность изменения типа найденного устройства прямо из окна результатов. Для этого необходимо выделить требуемую запись (допускается множественный выбор) и вызвать контекстное меню. В этом меню необходимо выбрать устанавливаемый тип устройства.

Для того чтобы поместить в список хостов не все найденные устройства, предлагается отметить желаемые устройства галками.

Кнопки *«Отметить все»*, *«Выделенные»*, *«Инвертировать»* помогают проводить множественный выбор устройств.

Можно оперативно выгрузить всю полученную информацию в CSV-файл. При этом, в отчет будут помещены и параметры сканирования сети. Для выгрузки информации необходимо нажать кнопку *«Отчет»*.

После завершения процесса сканирования нужно перейти на завершающий шаг, нажав кнопку «*Далее* >>».

Шаг 4. Внесение хостов в список (рис. 48)

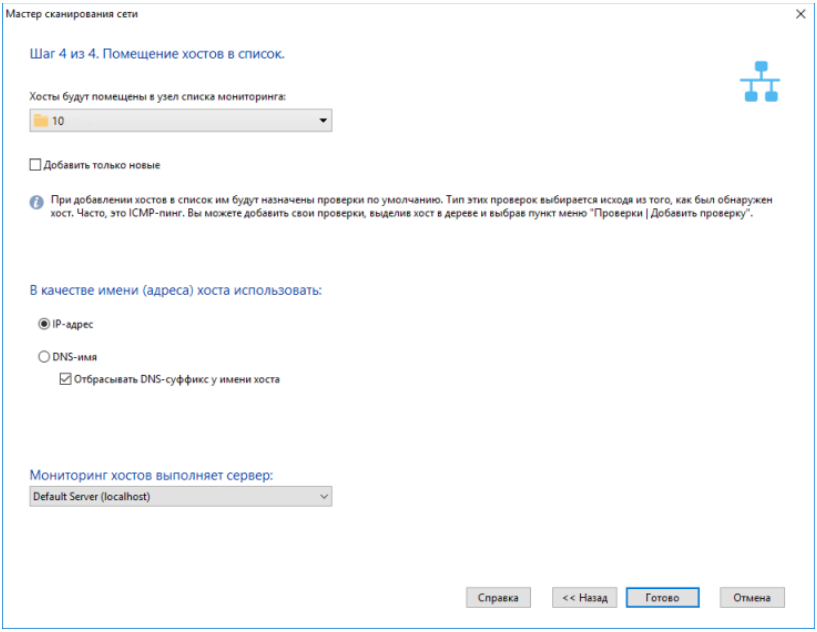


Рис. 48

На этом шаге Мастер предлагает задать существующий узел (группа хостов) списка мониторинга, в который будут помещены найденные хосты.

Перед помещением найденных хостов в список можно задать дополнительные параметры:

- Можно указать, что использовать в качестве имени (адреса) хоста - IP-адрес устройства или его DNS-имя. Для сетей с динамическим распределением IP-адресов необходимо выбрать DNS-имя, т.к. этот атрибут в данном случае будет постоянным. В сетях со статическими IP-адресами можно указать в качестве имени IP-адрес устройства.
- Отбрасывать DNS-суффикс у имени хоста. В качестве имени хоста Мастер может использовать определенные DNS-имена устройств. Часто такие имена имеют суффикс, например, mary.dep1.orgname.com. При выборе данного параметра имя хоста будет mary.

После нажатия кнопки *«Готово»* найденные хосты помещаются в выбранный узел. Им автоматически назначаются проверки (TCP, ICMP или ARP).

8.1.2 Добавление хостов вручную

Чтобы добавить хост в список вручную без использования Мастера сканирования сети перейдите на вкладку «*Хосты*» и выберите инструмент «*Добавить хост»,* рис. 49.

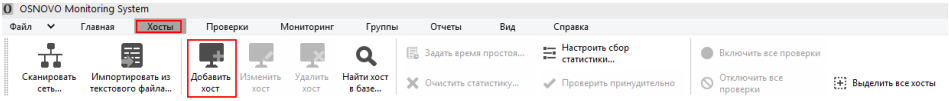


Рис. 49

Кроме того, добавить хост в существующую группу можно иначе (рис. 50):

1) Выделить в списке хостов группу
2) Вызвать контекстное меню правой кнопкой мыши и нажать «Добавить хост»
3) Ввести необходимые параметры. Обязательным является имя хоста или его адрес.

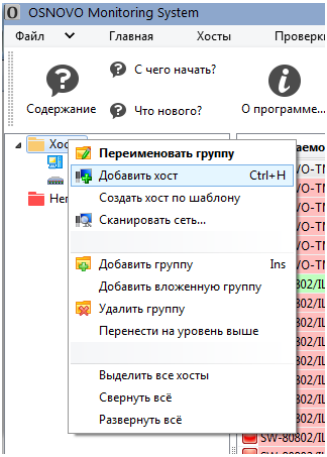


Рис. 50

Описание параметров добавляемого хоста.

Вкладка *«Основные»* (рис 51):

1. Имя или адрес хоста

Имя компьютера в сети или его IP-адрес. Значение данного поля является входным параметром для функций программы.

2. Отображаемое имя

По умолчанию в качестве надписи узла хоста в дереве выступает его адрес или сетевое имя. Текст узла можно изменить, задав любое желаемое имя в этом поле.

3. Тип

Тип устройства служит для визуального разделения хостов в дереве. Каждый тип сопровождается условным значком-пиктограммой.

4. MAC-адрес

Программа может реагировать на результат проверки путем включения компьютера. Для успешной работы функции включения компьютера по сети (Wake on LAN) необходимо для каждого хоста один раз задать MAC-адрес сетевого адаптера. MAC-адрес можно получить автоматически у включенных хостов либо ввести его вручную.

5. IP-адреса

Поддерживается хранение IP-адресов хоста.

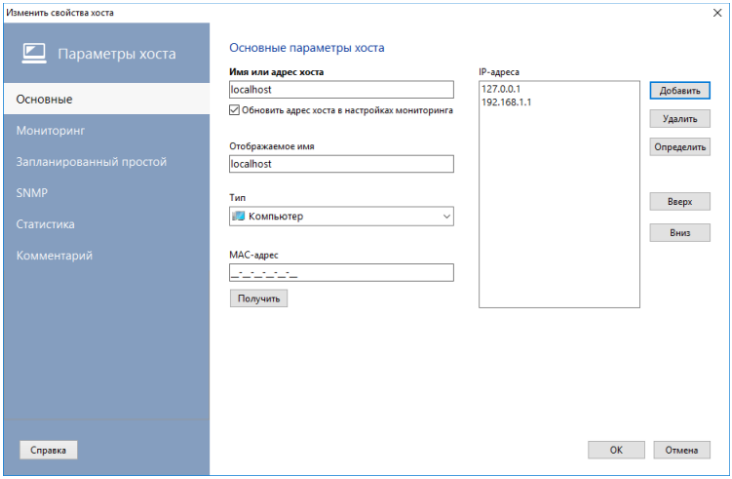


Рис. 51

Вкладка свойств добавляемого хоста *«Мониторинг»* (рис. 52).

В целях снижения сетевой нагрузки, можно выполнять не все проверки хоста, а только первую.

К примеру, если первой проверкой стоит ICMP-пинг хоста, то можно не запускать остальные проверки, если он не прошёл. И наоборот, если первая проверка какого-либо сервиса не проходит, то программа может запустить остальные, для более детальной диагностики.

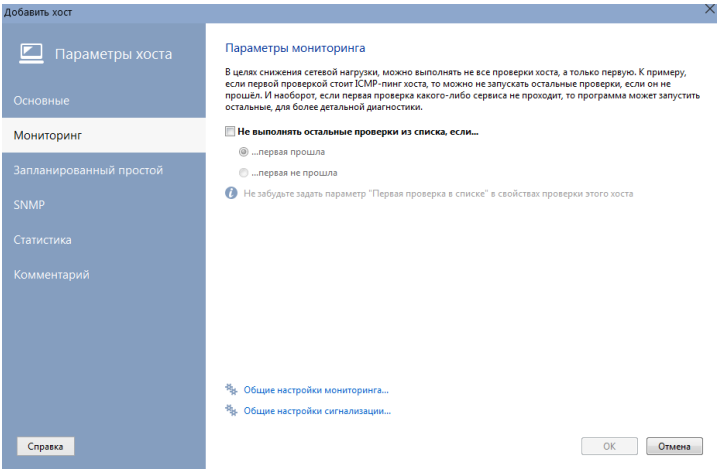


Рис. 52

Вкладка свойств добавляемого хоста *«Запланированный простой»* (рис. 53)

Если проверяемое устройство (к примеру, сервер) настроено на плановую перезагрузку в течение суток, то программа не будет реагировать на это событие сигнализацией, если задать время запланированного простоя устройства. Можно задать конкретный день недели планового простоя.

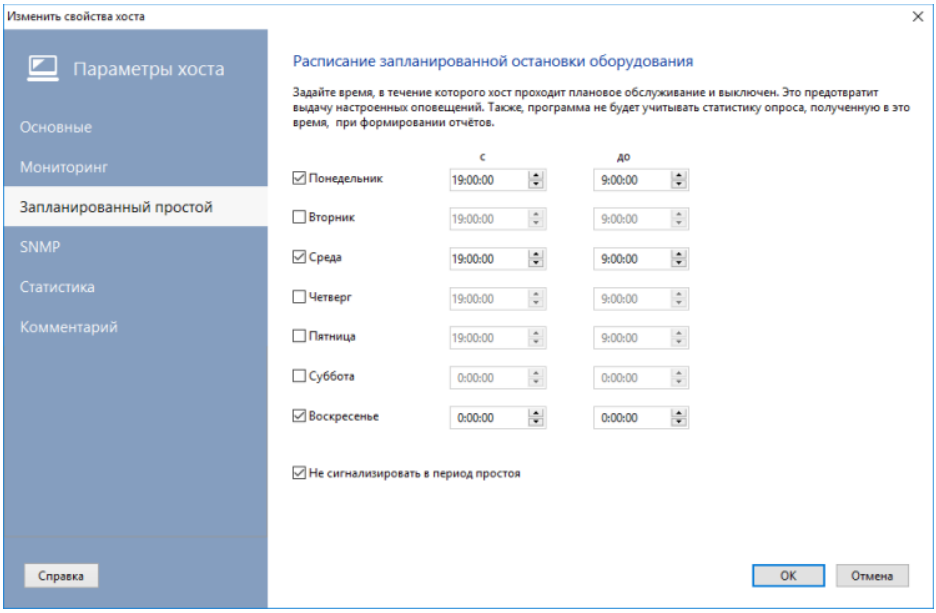


Рис. 53

Вкладка свойств добавляемого хоста *«SNMP»* (рис. 54)

Для некоторых типов проверок программе необходимо знать Community хоста (для устройств, поддерживающих управление по SNMP-протоколу). Можно задать этот параметр, включив параметр Агент есть. Введенное значение будет автоматически подставляться там, где это необходимо.

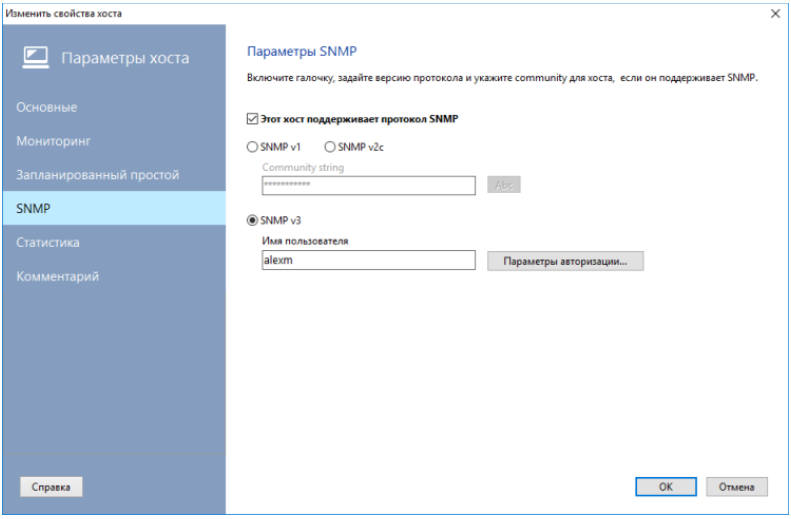


Рис. 54

Вкладка свойств добавляемого хоста *«Статистика»* (рис. 55)

В процессе мониторинга устройств ПО OMS постоянно собирает статистику значений времени отклика. Эта статистика хранится в виде файлов в рабочем каталоге программы. При большом количестве устройств объем этой статистики в течение года может достичь сотен мегабайт. Для управления сбором статистики предусмотрены параметры и инструменты на вкладке Статистика.

Если стабильная работа некоторых устройств не является критическим требованием (рабочие станции пользователей, к примеру), можно отключить сбор статистики для них, убрав галочку с параметра *«Хранить историю времени отклика»*.

Посмотреть объем накопленной статистики для выделенных хостов и в целом по всем картам можно тут же. Для удаления статистики у выделенных хостов нужно нажать соответствующую кнопку.

На основе накопленной статистики программа может построить отчеты и графики, доступные из главного меню Отчеты.

Программа может автоматически контролировать объем накопленной статистики и удалять ее по мере необходимости.

Эта вкладка становится доступной только при изменении параметров хоста.

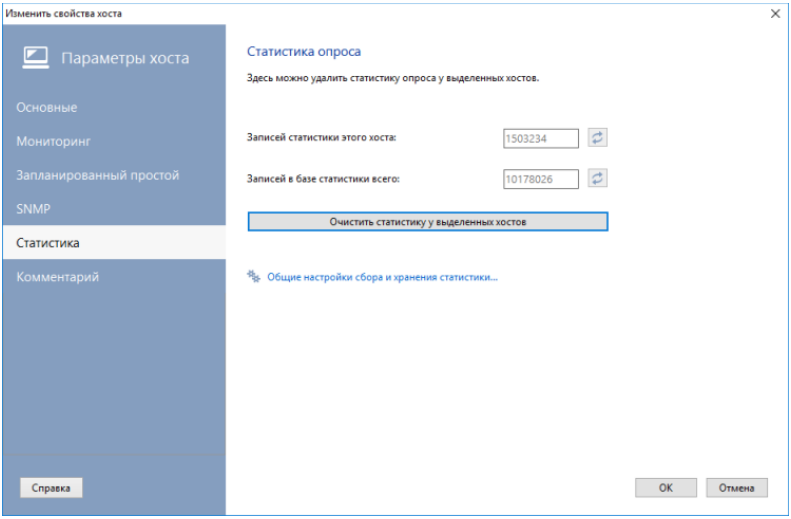


Рис. 55

Вкладка свойств добавляемого хоста *«Комментарий», рис. 56*

Каждый хост можно сопроводить пользовательским комментарием. В этом поле можно хранить информацию о пользователе компьютера, составе его системы, список ПО и т.д. Для удобства и быстроты ввода комментария предусмотрен механизм выбора атрибутов из списка. Список атрибутов может быть дополнен.

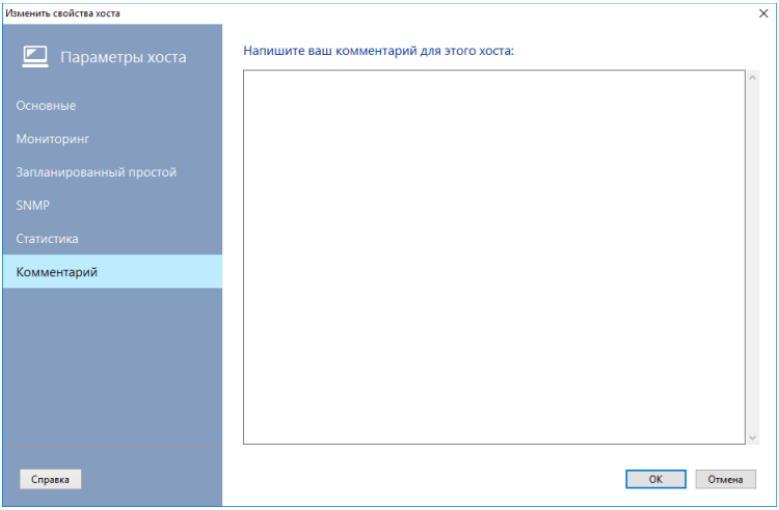


Рис 56

8.1.3 Добавление хоста по шаблону

Создание хоста по шаблону облегчает задачу формирования базы мониторинга.

К примеру, если у вас сложная схема мониторинга хоста — нужно проверять несколько сервисов, получать множество параметров разными проверками, то создание уже хотя бы 10 таких хостов может отнять какое-то время. Но гораздо проще единожды создать хост с типовыми проверками и продублировать его нужное число раз, меняя только адрес. При этом новый хост будет создаваться с тем же набором проверок, в которых будет прописан уже новый адрес хоста. И адреса в зависимостях и вычисляемых проверках также меняются на новые автоматически.

Для добавления хоста по шаблону выполните следующие действия:

1. Выделите в списке хостов группу.

2. В контекстном меню выберите пункт *«Создать хост по шаблону», рис 57.*

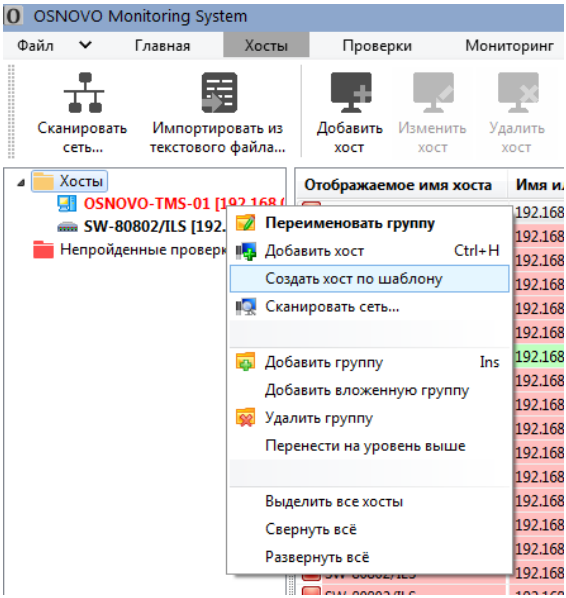


Рис 57

3. В появившемся списке выберите хост-шаблон, по образу которого нужно создать новый хост. Нажмите *ОК*. Новый хост с проверками появится в дереве и сразу же начнёт проверяться, рис 58

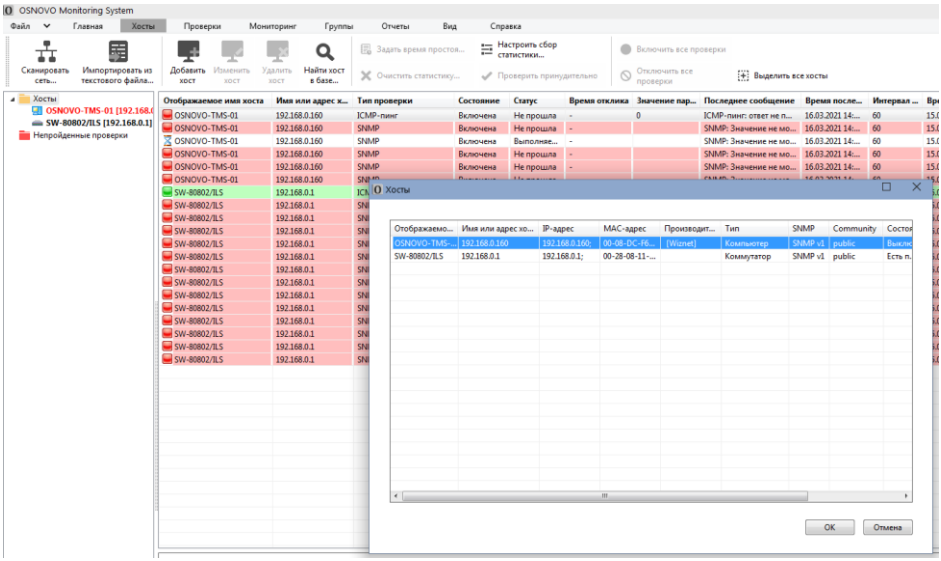


Рис 58

8.2 Работа со списком проверок

8.2.1 Добавление проверки

Для добавления новой проверки необходимо выполнить следующие действия:

1. Выделить в списке мониторинга хост. В поле списка проверок вызвать контекстное меню, выбрать пункт *«Добавить проверку»*, рис. 59

2. На экране появится Мастер настройки параметров мониторинга (окно Параметры проверки). Выберите нужный вид проверки из списка, рис. 60

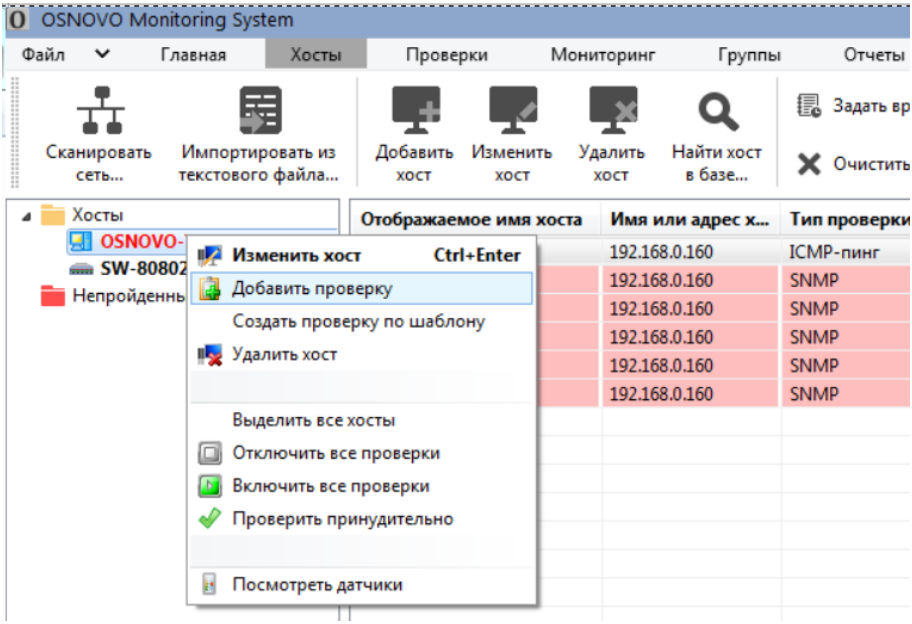

OSNOVO Monitoring System
Файл
Главная
Хосты
Проверки
Мониторинг
Группы
Отчеты
Сканировать сеть...
Импортировать из текстового файла...
Добавить хост
Изменить хост
Удалить хост
Найти хост в базе...
Задать вр
Очистить
Хосты
OSNOVO-
SW-80802
Непройденны
Изменить хост Ctrl+Enter
Добавить проверку
Создать проверку по шаблону
Удалить хост
Выделить все хосты
Отключить все проверки
Включить все проверки
Проверить принудительно
Посмотреть датчики
Отображаемое имя хоста
Имя или адрес х...
Тип проверки
192.168.0.160
ICMP-пинг
SNMP

Рис 59

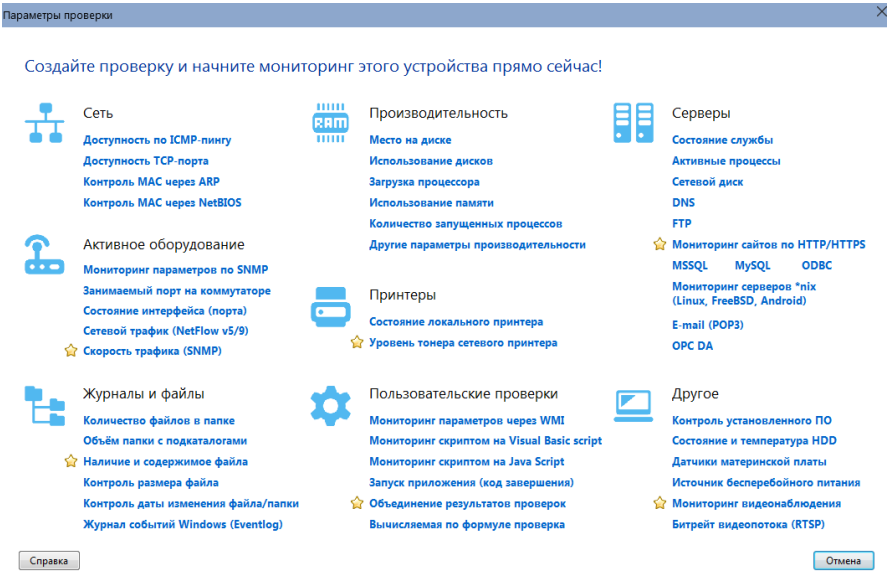

Параметры проверки
Создайте проверку и начните мониторинг этого устройства прямо сейчас!
Сеть
Доступность по ICMP-пингу
Доступность TCP-порта
Контроль MAC через ARP
Контроль MAC через NetBIOS
Активное оборудование
Мониторинг параметров по SNMP
Занимаемый порт на коммутаторе
Состояние интерфейса (порта)
Сетевой трафик (NetFlow v5/9)
Скорость трафика (SNMP)
Журналы и файлы
Количество файлов в папке
Объём папки с подкаталогами
Наличие и содержимое файла
Контроль размера файла
Контроль даты изменения файла/папки
Журнал событий Windows (Eventlog)
Производительность
Место на диске
Использование дисков
Загрузка процессора
Использование памяти
Количество запущенных процессов
Другие параметры производительности
Принтеры
Состояние локального принтера
Уровень тонера сетевого принтера
Пользовательские проверки
Мониторинг параметров через WMI
Мониторинг скриптом на Visual Basic script
Мониторинг скриптом на Java Script
Запуск приложения (код завершения)
Объединение результатов проверок
Вычисляемая по формуле проверка
Серверы
Состояние службы
Активные процессы
Сетевой диск
DNS
FTP
Мониторинг сайтов по HTTP/HTTPS
MSSQL MySQL ODBC
Мониторинг серверов *nix (Linux, FreeBSD, Android)
E-mail (POP3)
OPC DA
Другое
Контроль установленного ПО
Состояние и температура HDD
Датчики материнской платы
Источник бесперебойного питания
Мониторинг видеонаблюдения
Битрейт видеопотока (RTSP)
Справка
Отмена

Рис. 60

3. Настройте параметры проверки (шаг 1), задайте условия, при которых она будет считаться успешной.

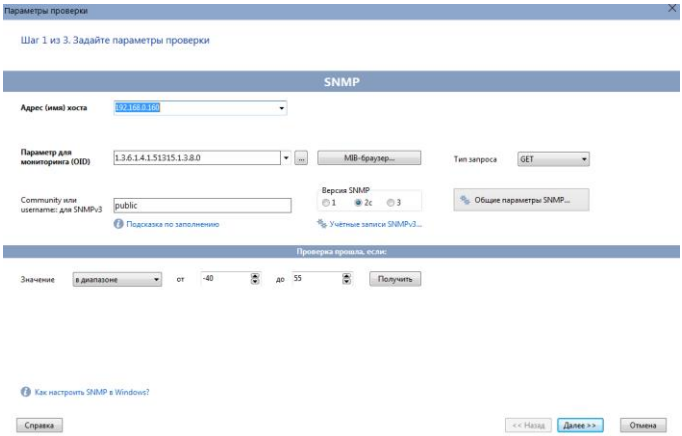


Рис. 61

Всегда обращайте внимание на логику проверки – «*Проверка прошла, если:»*

Проверьте, сможет ли программа получить значение параметра по введённым данным. Нажмите кнопку *«Далее»*.

4. На втором шаге настройки проверки для хоста можно задать дополнительные параметры проверки, рис. 62

Шаг 2 из 3. Задайте дополнительные параметры

Рис. 62

Зависимости

Данный параметр используется для исключения ложных срабатываний сигнализации. Проверки в удаленных сетях будут зависеть от проверки доступности шлюза. Если шлюз не ответит, то сигнализация не будет запущена и проверка получит статус «не прошла по зависимости», рис. 63

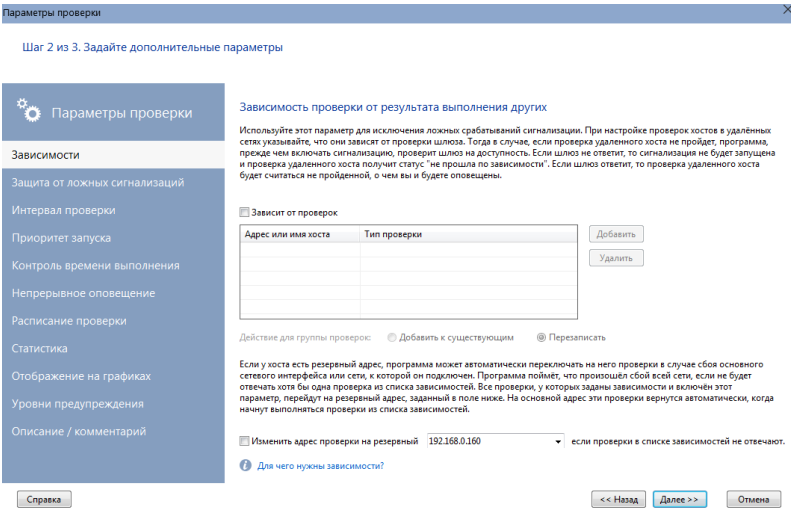


Рис. 63

Защита от ложных сигнализаций

Данный параметр отвечает за защиту от ложных сигнализаций путем увеличения задержки и количества попыток прохождения проверки. Изменение данного параметра может помочь при ложных срабатываниях сигнализации из-за кратковременных сбоев в каналах связи. Рис. 64

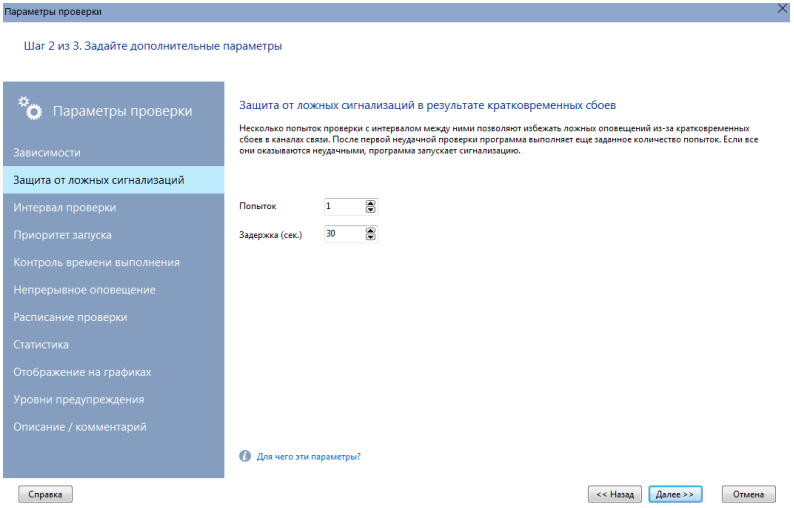


Рис. 64

Интервал проверки

Данный параметр отвечает за интервал запуска проверки. Не рекомендуется выставлять слишком короткий интервал во избежание загрузки процессора (особенно касается реусурсоемких проверок по протоколу WMI, скрипторв и баз данных). Рис. 65

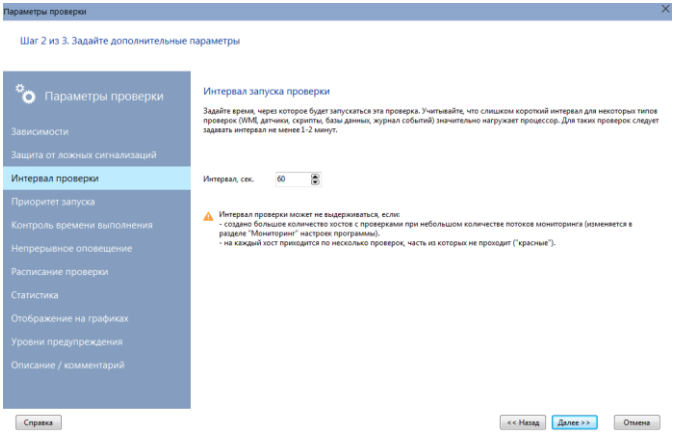


Рис. 65

Приоритет запуска

Данный параметр позволяет выполнять условия – если первая проверка не прошла (например ICMP пинг), то остальные проверки не выполнять. И наоборот: если первая проверка не прошла, то ПО приступает к выполнению следующих проверок. Рис. 66

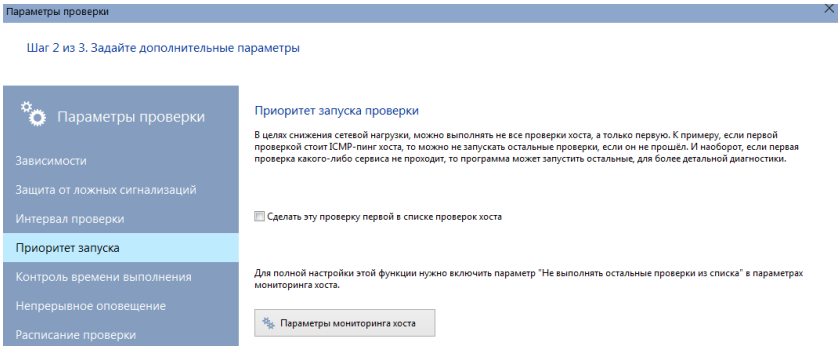


Рис.66

Контроль времени выполнения

Данный параметр отвечает за зависимость прохождения/непрохождения проверки от времени отклика ICMP пинга (если время выполнения проверки превысит заданное, то она будет считаться непройденной). Рис. 67

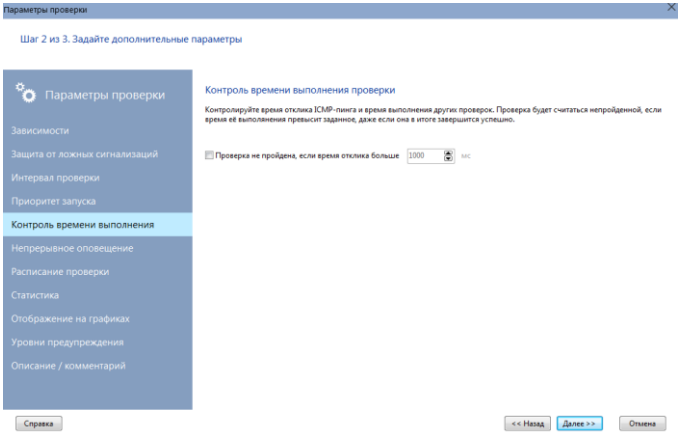


Рис. 67

Непрерывное оповещение

Данный параметр позволяет включить непрерывное оповещение при каждой проверки с учетом ее интервала. Рис. 68

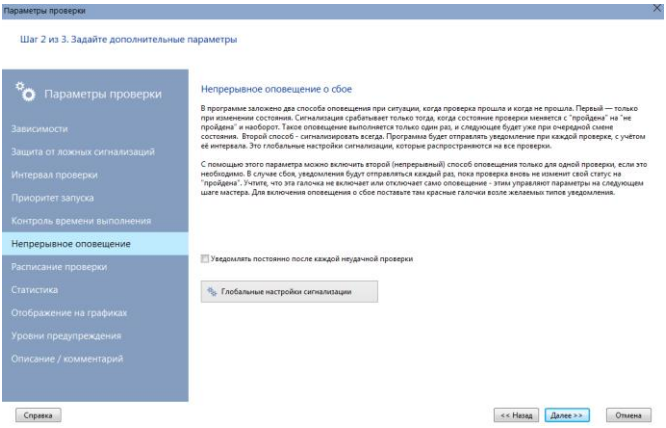


Рис. 68

Расписание проверки

Данный параметр позволяет запускать проверку по расписанию. Рис 69

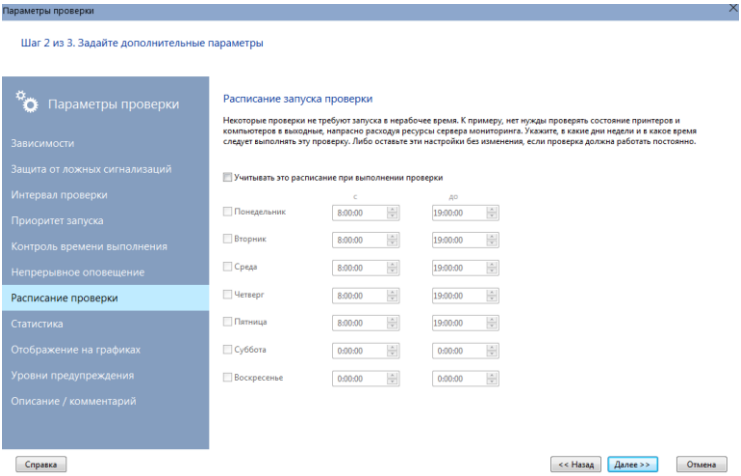


Рис. 69

Статистика

Данный параметр позволяет вкл/выкл хранение накопленной статистики для данной проверки. Рис. 70

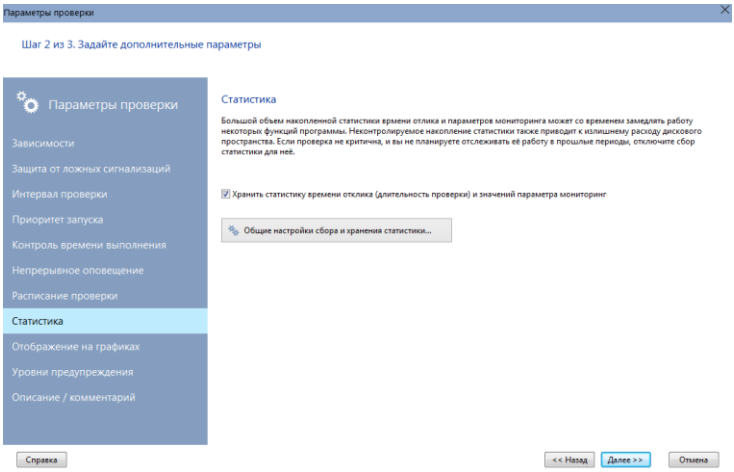


Рис. 70

Отображение на графиках

Данный параметр позволяет привести результаты проверки на графиках к нужным единицам измерения путем добавления множителя, а также задать наименование единиц измерения. Рис. 71

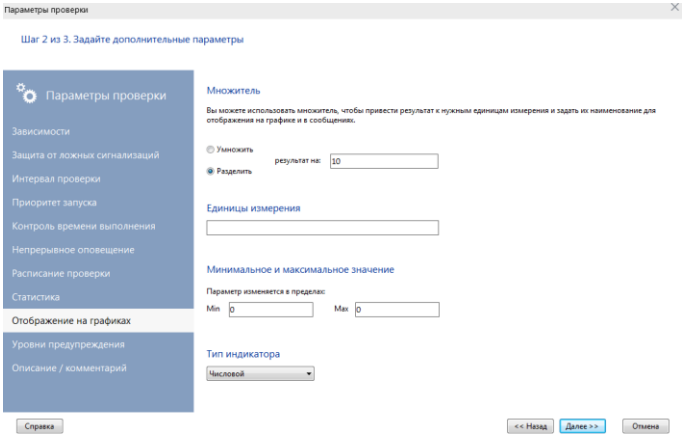


Рис. 71

Уровни предупреждения

Данный параметр позволяет задать больше уровней предупреждения между значениями проверки «пройдена» и «не пройдена» рис. 72

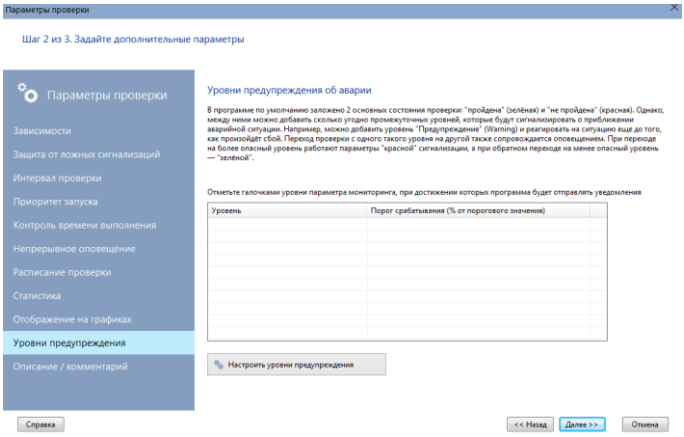


Рис. 72

Описание / комментарий

Данный параметр позволяет задать текстовое описание (комментарий) для проверки, чтобы различать однотипные проверки между собой. Рис. 73

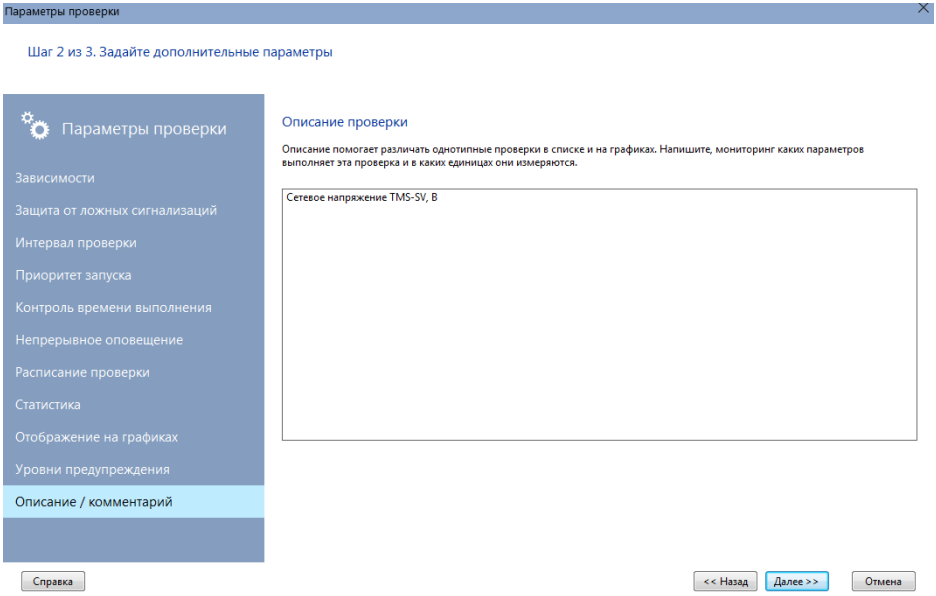


Рис. 73

5. На **3м шаге** работы мастера добавления проверок доступны настройки параметров сигнализации (оповещения) для добавляемой проверки.

Сообщение, e-mail, SMS

Это те действия, которые будут выполнены, если проверка пройдёт / не пройдёт. Зелёная галочка отвечает за действия, которые выполняются в случае успешной проверки, к примеру, при восстановлении после сбоя. Красная галочка отвечает за оповещение при сбое проверки. Рис. 74

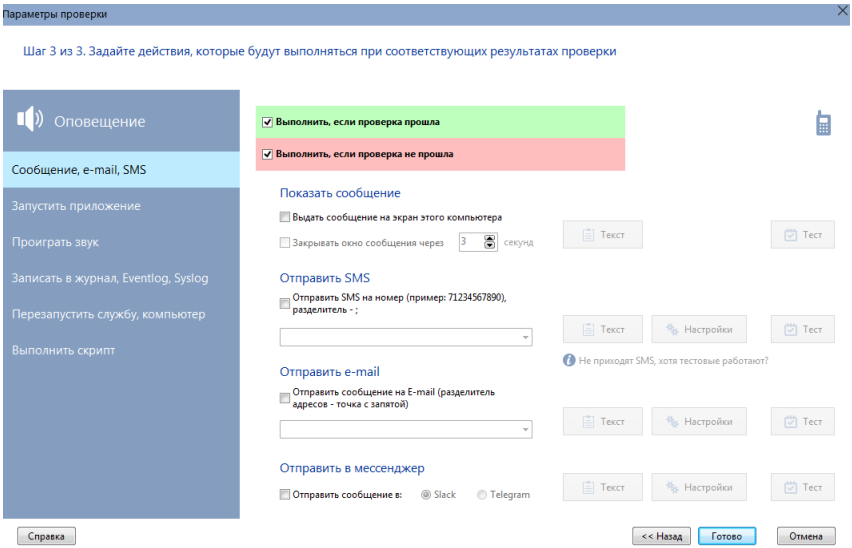


Рис.74

ПО выдает сообщение с настраиваемым текстом:

- На экран локального компьютера, при этом можно указать интервал времени, по истечении которого сообщение закроется автоматически;
- Как SMS на мобильный телефон с заданным номером в формате <код страны><номер_телефона> (например: 79021235566). Параметры SMS информирования задаются в настройках ПО OMS;
- Как E-mail на указанные адреса. Адрес отправителя, SMTP-сервера и др. задаются в настройках ПО OMS. Поддерживается SMTP-авторизация перед отправкой. При задании нескольких адресов их необходимо разделять точкой с запятой.
- Отправляет через мессенджеры Slack и Telegram. Для работы этого типа оповещения необходима предварительная настройка.
- Текст оповещения может быть настроен для каждой проверки отдельно. По умолчанию выдаётся текст из общих настроек программы. Чтобы создать уникальное для проверки сообщение, нужно нажать кнопку «Текст» (рис. 75) рядом с соответствующим типом оповещения.

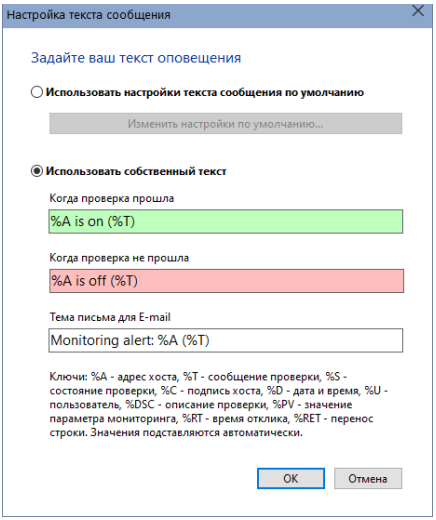


Рис. 75

Запуск приложения.

Запускает внешнее приложение с параметрами (если необходимо). Если в качестве приложения указать команду net (только в WINDOWS NT, XP, 2000, 2003), а в параметрах - send <имя компьютера> <текст сообщения>, то вы можете, работая на удаленной машине, получать сообщения от машины, где работает программа. Рис. 76

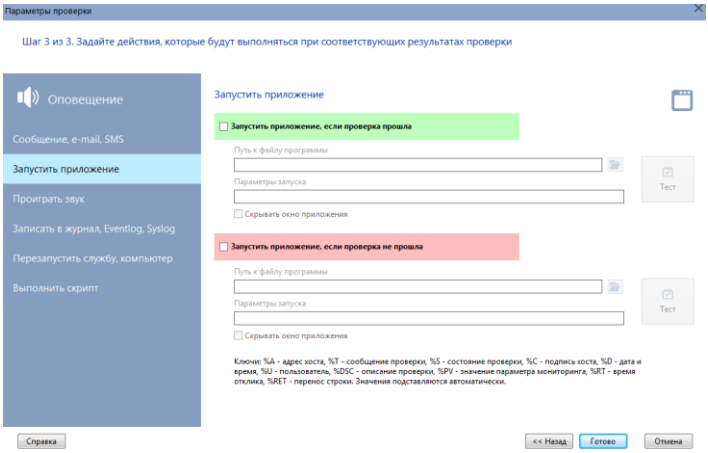


Рис. 76

Проиграть звук

Проиграть звук в формате WAV при удачной/неудачной проверке. Рис. 77

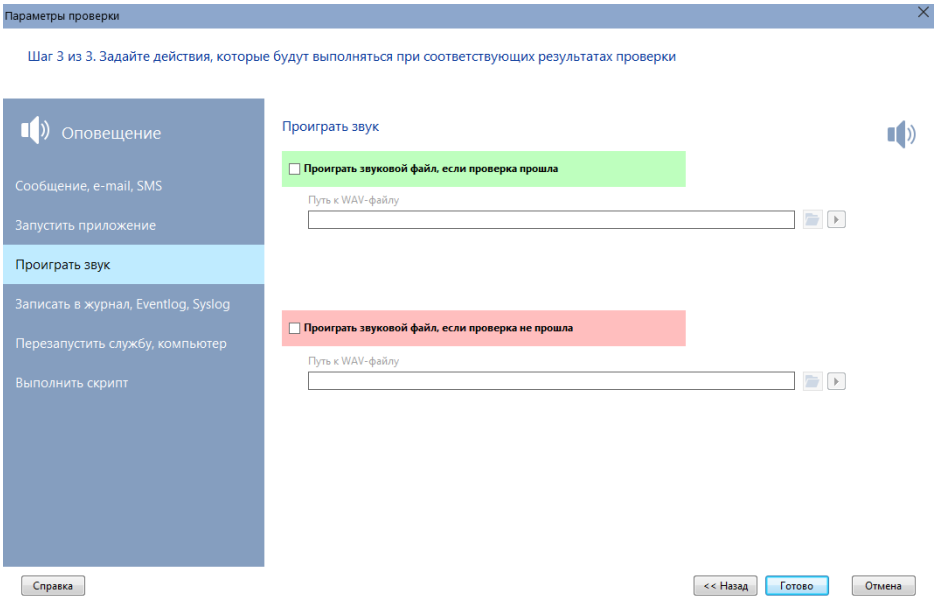


Рис. 77

Записать в журнал, Eventlog. Syslog

Записывает строку сообщения (текст настраивается) в журнал (рис. 78):

- Журнал программы, имя файла которого можно задать в настройках (по умолчанию - NMAlerts.log в личной папке пользователя <диск>:\Documents and Settings\All Users\Application Data\OSNOVO\Network Monitor\Logs\). На этой же вкладке можно сразу же просмотреть и уже созданный журнал.
- Журнал событий Windows (EventLog). Тип записи (уведомление, ошибка, предупреждение...) задается в соответствующем поле. Вызвать журнал событий можно через нажатие кнопки «Просмотреть журнал».

- Syslog. Стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в компьютерных сетях, работающих по протоколу IP.

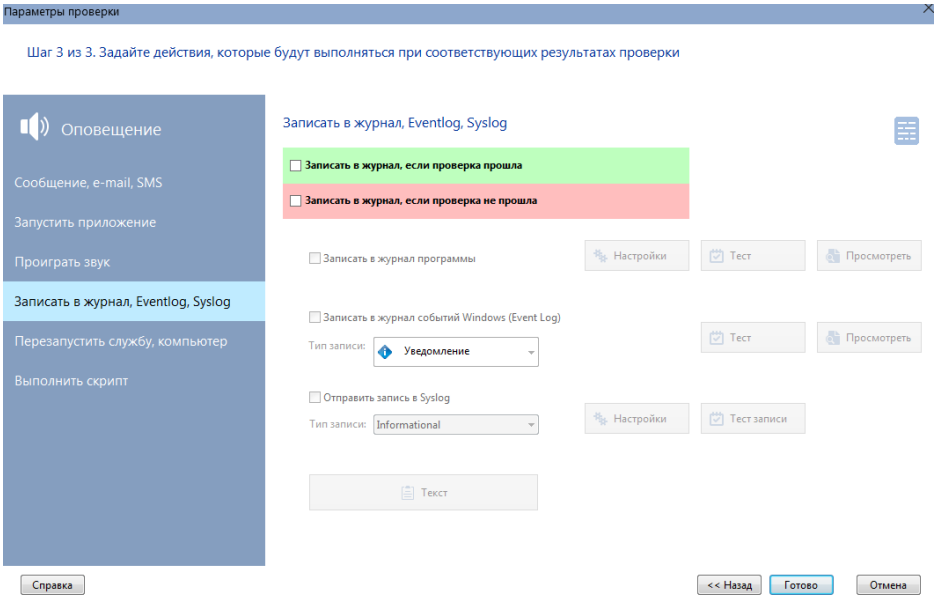


Рис. 78

Перезапустить службу, компьютер, Рис 79

Позволяет осуществлять запуск/останов/перезапуск заданной службы проверяемого компьютера, перезагрузку/завершение работы/включение проверяемого компьютера.

Для задания службы необходимо нажать кнопку '<<' , выбрать из списка требуемую службу.

Если пользователь, под которым работает программа, не имеет прав администратора на проверяемом компьютере, то для успешного выполнения операций со службами и питанием компьютера необходимо задать имя и пароль этого пользователя с необходимыми полномочиями.

Для задания имени и пароля необходимо включить параметр «Нужна авторизация» и заполнить поля «Логин» и «Пароль».

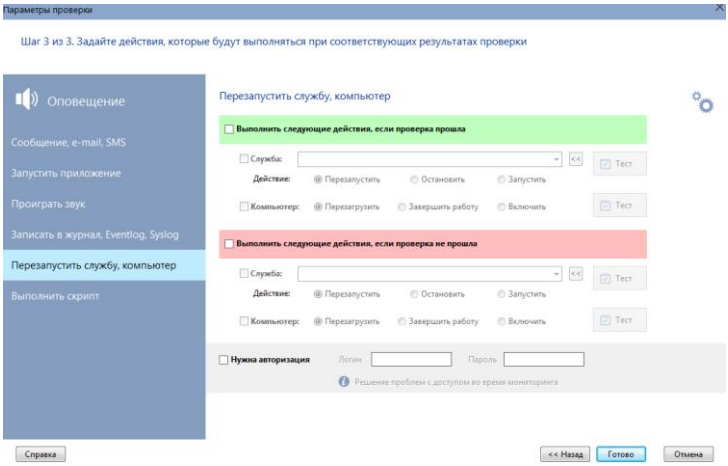


Рис. 79

Выполнить скрипт

Позволяет выполнить скрипт на языке VBScript или JScript. Код скрипта можно создать в любом текстовом редакторе и загрузить путем нажатия кнопки Загрузить.

Необходимо указать основную функцию скрипта в соответствующем поле.

Можно протестировать работу скрипта, нажав кнопку Тест.

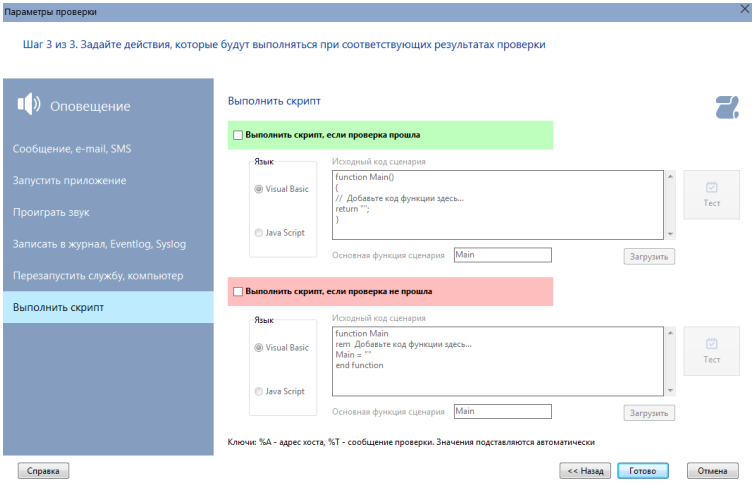


Рис. 80

8.2.2 Создание проверки из шаблона

Если есть необходимость скопировать созданную и настроенную проверку по нескольким хостам, Вы можете воспользоваться функцией создания проверки из шаблона (рис. 81). Для этого выполните следующее:

1. Выделите в списке мониторинга один хост или несколько (с CTRL). Вызовите контекстное меню, выберите пункт «Создать проверку из шаблона».

2. В окне «Список проверок» отметьте галочками те проверки, которые необходимо скопировать на выделенные хосты.

3. Нажмите кнопку «ОК». Выбранные проверки будут добавлены хостам. Все параметры проверки, кроме адреса хоста, будут скопированы из шаблона.

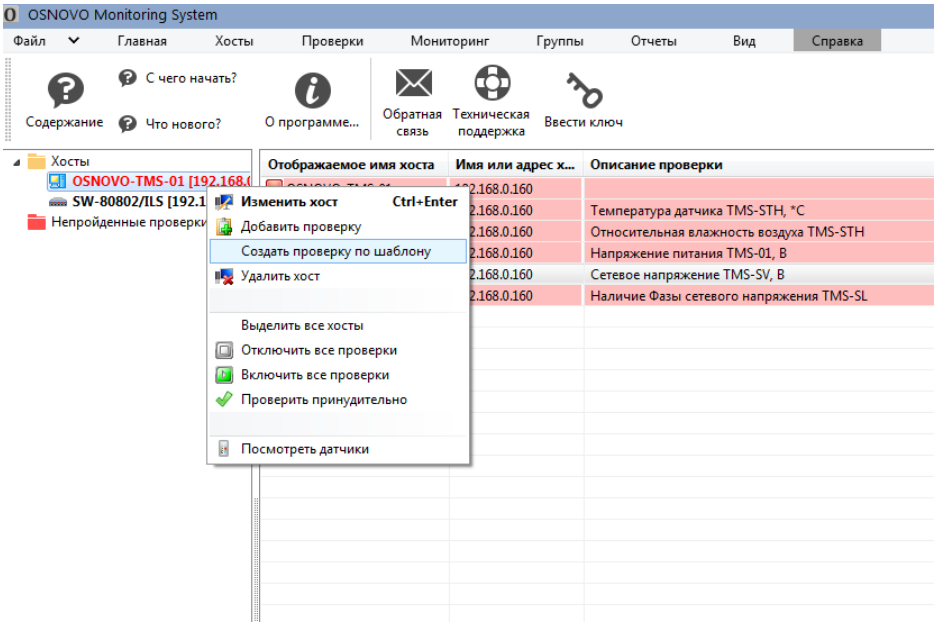


Рис. 81

8.2.3 Изменение параметров проверки

Для изменения параметров проверки необходимо выполнить следующие действия (82):

1. Выделить в списке строку проверки.

2. Вызвать контекстное меню, выбрать пункт «Изменить проверку».

3. На экране появится окно Мастера настройки параметров мониторинга (Параметры проверки).

4. Изменить требуемые параметры (см. 8.2.1 «Добавление проверки»). Нажать кнопку «Далее >>», затем «Готово».

Параметры проверки автоматически сохраняются в файл и сразу вступают в силу.

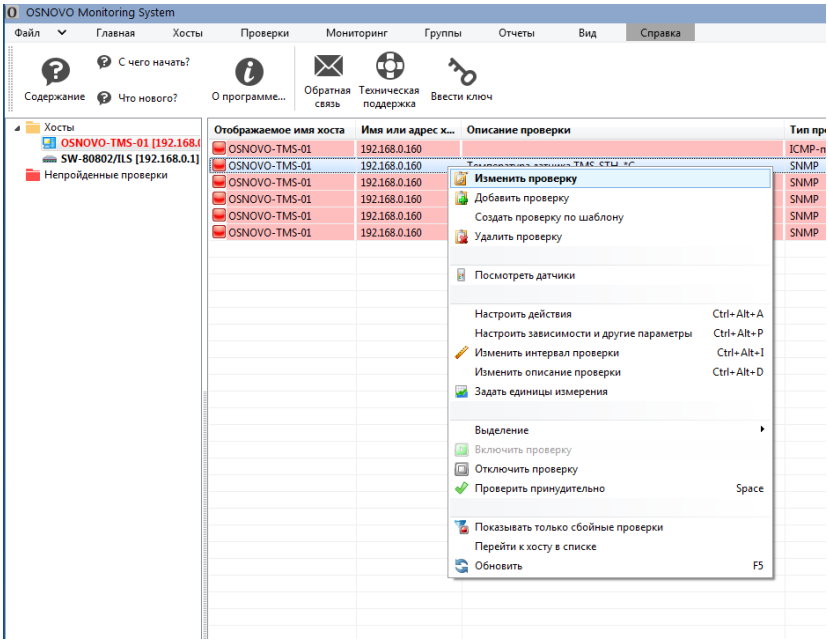


Рис. 82

8.2.4 Настройка действий для проверки

Для быстрой настройки действий для соответствующих результатов проверки необходимо выполнить (рис. 83):

1. Выделить в списке одну или несколько проверок.

2. Вызвать контекстное меню, выбрать пункт «Настроить действия».

3. На экране появится окно Мастера настройки параметров мониторинга (Параметры проверки).

4. Настроить требуемые действия (см. 8.2.1 «Добавление проверки»). Нажать кнопку «Готово».

Настроенные действия назначаются сразу всем выделенным проверкам, автоматически сохраняются в файл и сразу вступают в силу.

Эту же процедуру можно выполнить, выделив одну или несколько проверок и отметив на информационной панели пиктограмму требуемого действия.

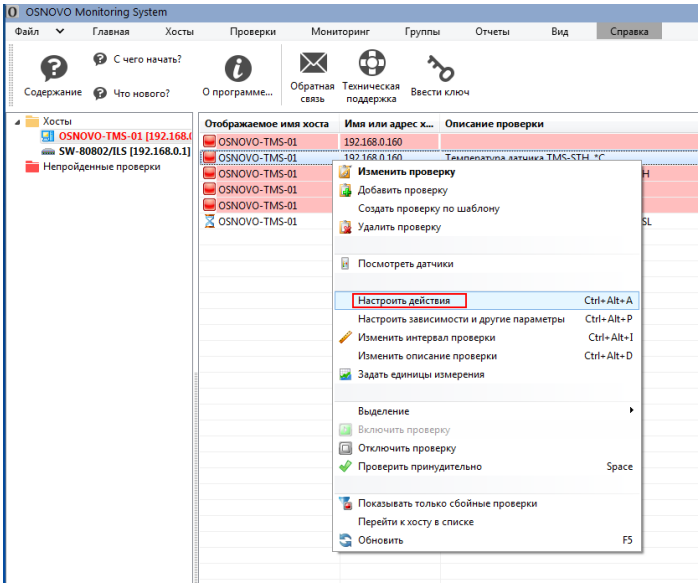


Рис. 83

8.2.5 Удаление проверки

Для удаления проверки необходимо выполнить следующие действия (рис. 84):

1. Выделить в списке строку проверки.

2. Вызвать контекстное меню, выбрать пункт «Удалить проверку».

Выбранная проверка удаляется из списка мониторинга и из файла.

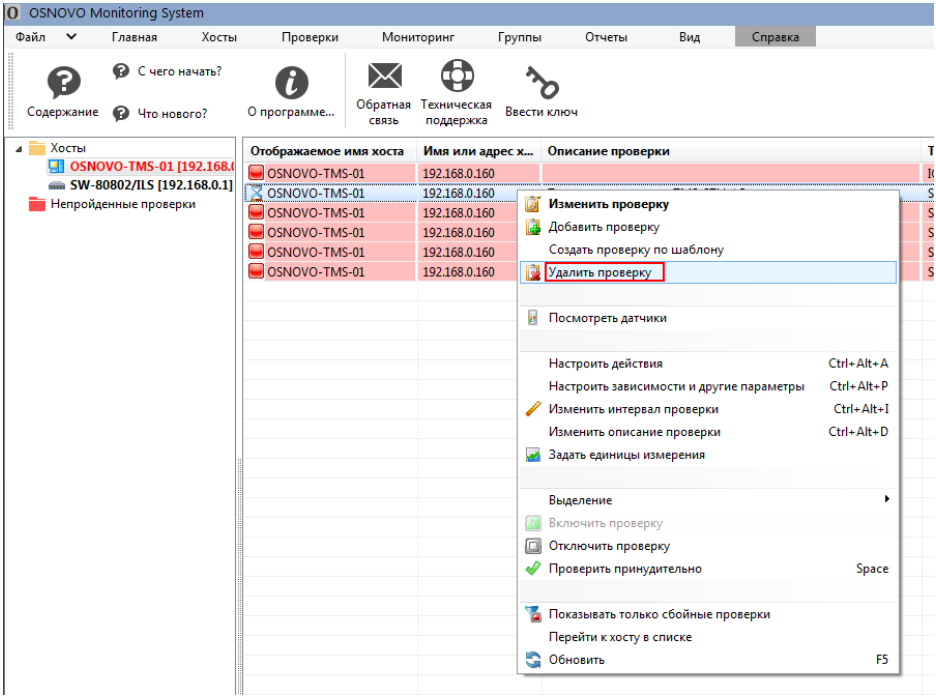


Рис. 84

8.2.6 Включение и отключение выполнения проверки

Чтобы на время отключить проверку не удаляя ее, необходимо выполнить следующие действия (рис 85):

1. Выделить в списке строку включенной проверки.

2. Вызвать контекстное меню, выбрать пункт «Отключить проверку».

Отключенная проверка выделяется желтым цветом в списке.

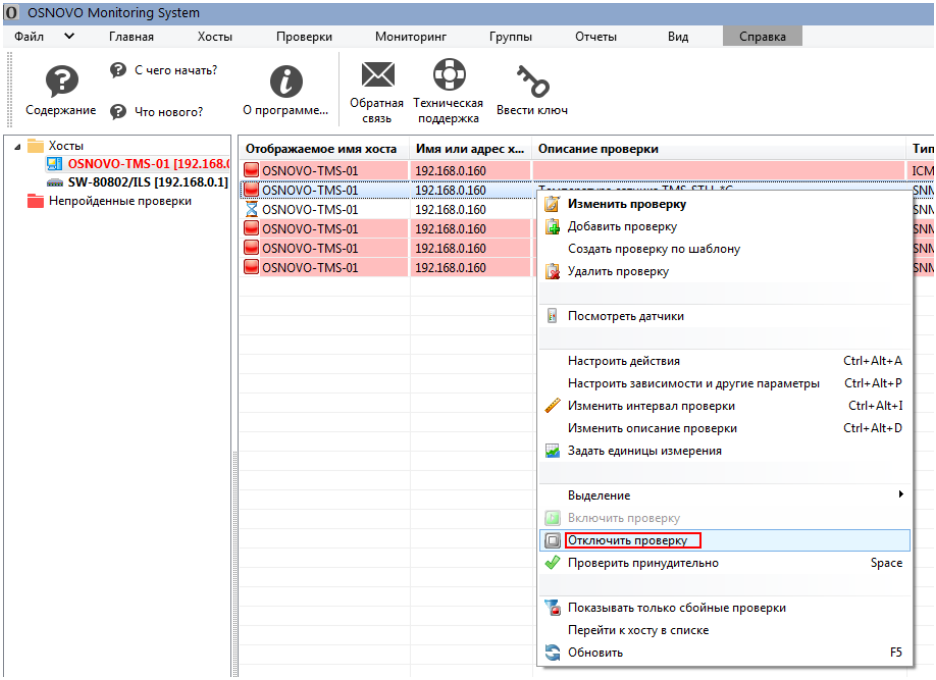


Рис. 85

Для включения проверки необходимо выполнить следующие действия (рис. 86):

1. Выделить в списке строку отключенной проверки.

2. Вызвать контекстное меню, выбрать пункт «Включить проверку».

Включенная проверка выделяется прежним цветом (соответствующим предыдущему статусу).

Признак включения/выключения проверки автоматически сохраняется и вступает в силу.

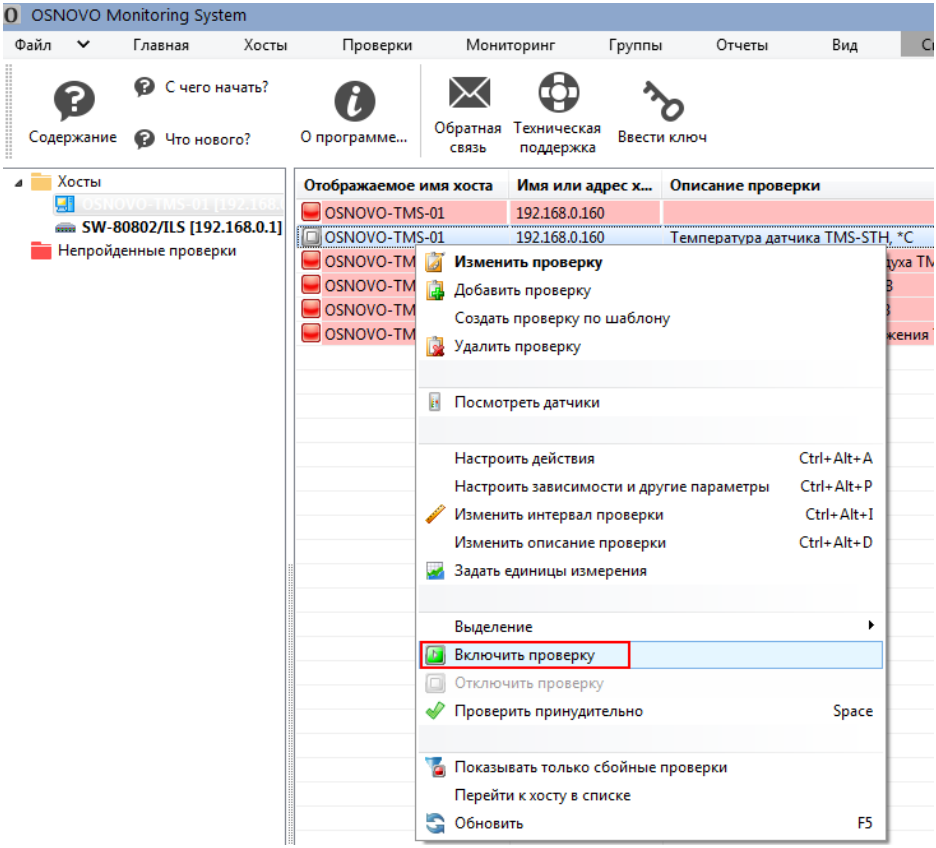


Рис. 86

8.2.7 Принудительный запуск проверки

Для того чтобы запустить проверку принудительно, не дожидаясь, когда до нее дойдет очередь в процессе мониторинга, нужно выполнить действия (рис. 87):

1. Выделить в списке строку проверки.

2. Вызвать контекстное меню, выбрать пункт «Проверить принудительно».

Запуск проверки стартует незамедлительно.

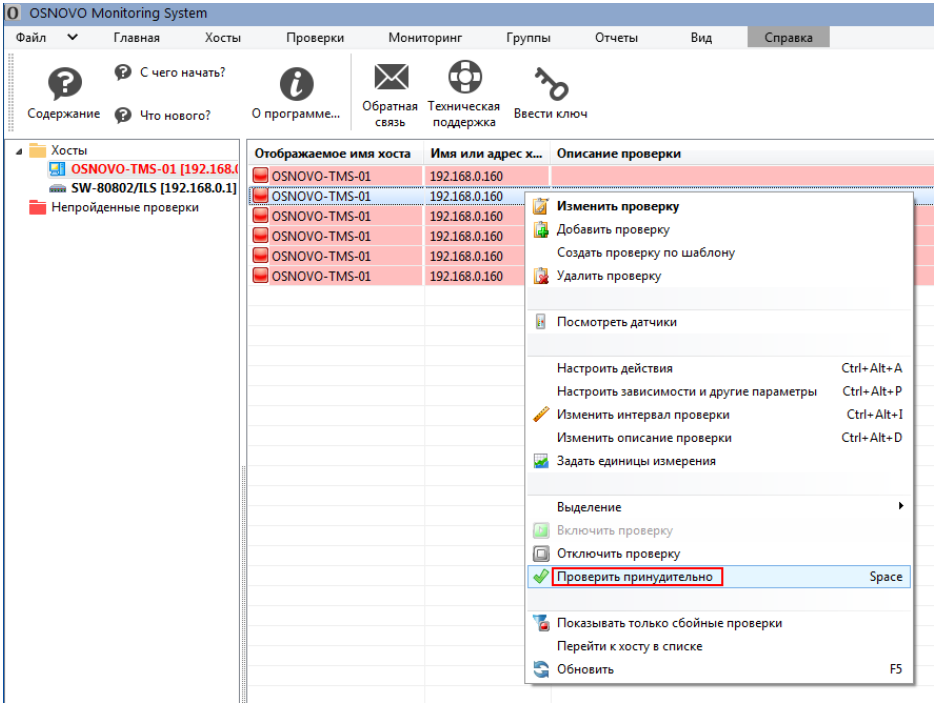


Рис. 87

8.3 MIB браузер

MIB браузер – функция программы, позволяющая просматривать иерархию SNMP MIB-переменных в древовидной форме. С помощью неё можно загружать и компилировать стандартные и проприетарные файлы MIB.

Чтобы добавить новые проверки параметров для управляемого сетевого оборудования OSNOVO через SNMP протокол необходимо загрузить в MIB браузер файл с расширением (.mib), доступный по запросу. MIB файл - это текстовый файл с информацией обо всех SNMP ресурсах (OID), поддерживаемых конкретным устройством.

MIB файл имеет специальную иерархическую структуру, в которой описаны все переменные и их предназначение. С помощью компилятора MIB множество отдельных MIB-файлов можно представить в виде одного дерева, в котором уже гораздо проще найти имя, адрес (OID) и описание необходимого параметра (например, температуру выносного датчика, мощность PoE на порте и тд.)

Чтобы запустить MIB браузер нажмите «Файл» / «MIB браузер» (рис. 88)

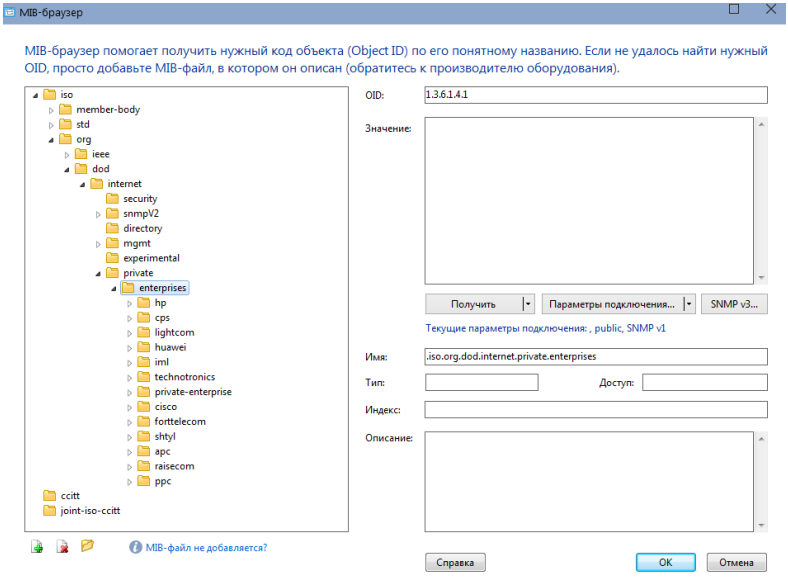


Рис. 88

- MIB-браузер используется при выборе переменной для мониторинга в проверке SNMP, для перевода кодов переменных, получаемых в сообщении SNMP trap, в читаемые имена и просто для просмотра информации, содержащейся в устройстве.

- В состав ПО OMS уже включены несколько стандартных файлов MIB, они находится в каталоге \mibs. Чтобы добавить свои файлы, просто перепишите их туда и перезапустите программу, либо используйте диалог добавления (кнопки под деревом MIB).

- С помощью MIB-браузера можно не только посматривать дерево MIB, но и получать по SNMP значения его переменных. Для этого нажмите кнопку Параметры подключения и задайте логин (community) и пароль (если SNMP v3). После этого вы можете либо получить значение выделенной в дереве переменной (запрос GET), либо следующей за ней (запрос GET NEXT). Программа также может сохранить в файл полный SNMP-дамп (все переменные с их значениями).

8.4 Панель датчиков и индикаторов

Вы можете визуально наблюдать за изменением параметров мониторинга не только на графиках, но и через специальные виджеты — датчики, индикаторы и диаграммы.

Они выведены на общую панель (dashboard), которая может быть размещена на отдельном мониторе — это окно не мешает работать с другими диалогами программы. Каждый датчик может отображать только один параметр мониторинга. Датчики создаются автоматически — по одному на проверку хоста, которая в процессе работы получает значение какого-либо параметра.

Чтобы вывести на экран панель датчиков, выделите в дереве хост и выберите в его меню пункт *«Посмотреть датчики»* (рис. 89)

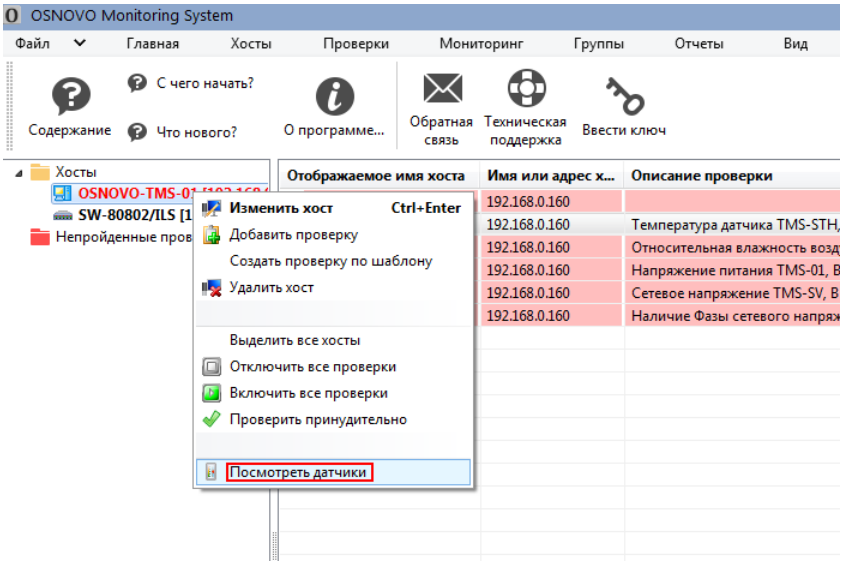


Рис. 89

Для каждого хоста создаётся отдельное окно датчиков. Датчики создаются только для проверок, у которых есть параметр мониторинга. Другими словами, количество датчиков может не совпадать с количеством проверок хоста.

Программа поддерживает несколько типов датчиков, в зависимости от типа параметра и заданных в проверке единиц измерения. Обычно тип устанавливается автоматически при создании проверки — программа знает, какой параметр как отображать. Но вы можете в любой момент изменить вид датчика в параметрах проверки

Доступны следующие типы датчиков:

1. *Стрелочный индикатор* рис. 90

Используется для отображения параметров, которые измеряются в процентах от 0 до 100.

К примеру, для загрузки процессора. Для того, чтобы отобразить значение на таком датчике, необходимо задать границы его изменения в окне параметров проверки (раздел «Отображение на графиках»). В поле «Параметр изменяется в пределах» задайте 0 — 100.

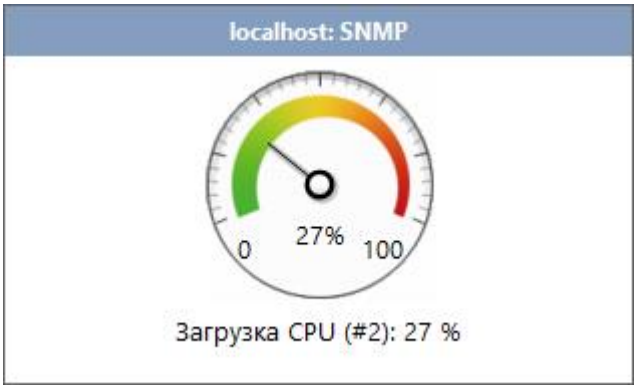


Рис. 90

2. *Круговая диаграмма*, рис. 91

Используется только для отображения свободного или занятого дискового пространства в различных проверках.

Для корректного отображения данных необходимо задать границы изменения этой переменной в окне параметров проверки (раздел «Отображение на графиках»). В поле «Параметр изменяется в пределах» задайте минимальный и максимальный объём диска.

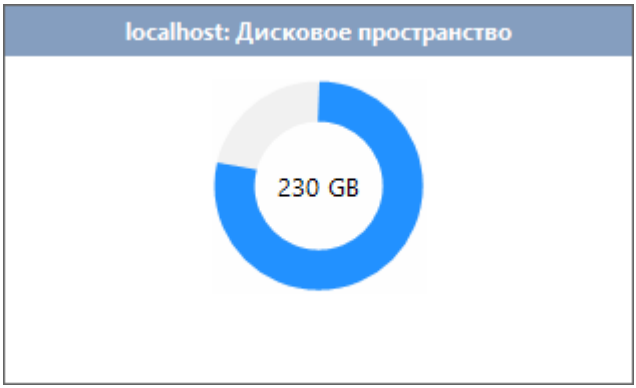


Рис. 91

3. *Вертикальная диаграмма*, рис. 92

Такой вид датчика используется только для проверок, которые получают текущую скорость трафика на сетевом интерфейсе.

Для корректного отображения данных необходимо задать границы изменения пропускной способности интерфейса в окне параметров проверки (раздел «Отображение на графиках»). В поле «Параметр изменяется в пределах» задайте 0 и максимально возможную скорость на этом интерфейсе.

Рис. 92

4. *Числовой индикатор*, рис. 93

Этот универсальный датчик используется для всех остальных параметров, которые нельзя подогнать под условия трёх предыдущих.

Для этого датчика не обязательно задавать минимальное и максимальное значение. Однако, если это сделать, то цвет цифр будет меняться плавно от синего к красному, проходя через оттенки зелёного и жёлтого. Это свойство отлично подходит для вывода температурных показателей на экран. Просто задайте в окне параметров проверки (раздел «Отображение на графиках») минимальную и максимальную температуру, и синий цвет цифр будет означать холод, а красный — перегрев.

Рис. 93

5. *График*, рис. 94

С помощью графика можно отобразить динамику изменения любого параметра, поставленного на мониторинг. Шкала значений масштабируется автоматически. График отображает данные за последний час.

Рис. 94

9. Настройки программного обеспечения Osnovo Monitoring System

Для того чтобы открыть окно с настройками ПО OMS необходимо нажать *Файл / Настройки программы* (или сочетанием клавиш Ctrl+P) Рис. 95

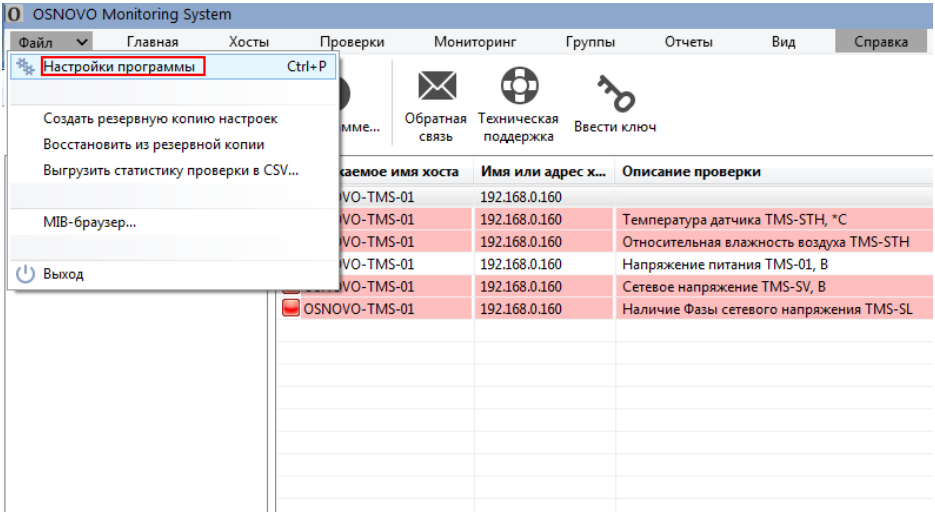


Рис. 95

9.1 Общие настройки

В разделе настроек «Общие» (рис 96) можно настроить параметры:

- *Сворачивать по ESC*

При выборе данной опции вы можете минимизировать приложение нажатием клавиши ESCAPE на клавиатуре. О других 'горячих' клавишах см. раздел "Горячие" клавиши.

- *Ярлык на рабочем столе*

Выбрав данную опцию, вы создадите ярлык к программе на рабочем столе Windows. Удалить его можно, сняв галочку с данной опции.

- *Автозапуск*

Клиентская часть программы (отображение результатов мониторинга) будет автоматически запускаться при старте Windows.

- *Минимизировать при запуске*

При старте программа будет автоматически минимизироваться в системный трей (область рядом с часами).

- *Каталог данных и настроек программы*

По умолчанию, все данные программы хранятся в папке профиля пользователя. Вы можете перенести эти данные в другое место

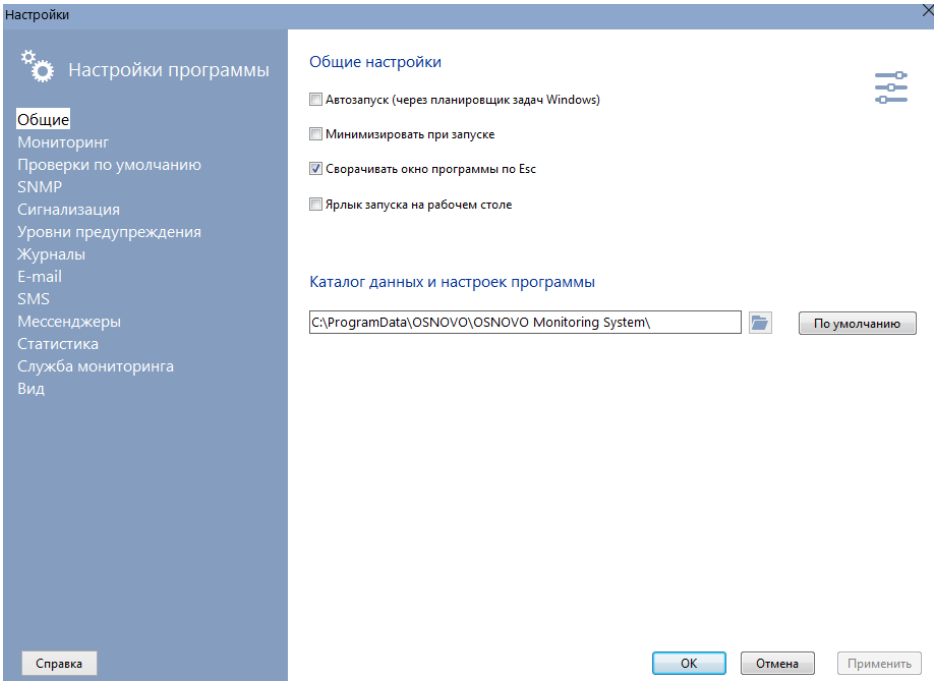


Рис. 96

9.2 Мониторинг

В разделе настроек «Мониторинг» (рис 97) можно настроить параметры:

- *Максимальное количество одновременно выполняемых проверок*

Число одновременно запущенных проверок не превысит этого значения. Следует с осторожностью увеличивать этот параметр, т.к. большое число потоков может привести к замедлению работы системы в целом. Рекомендуемое значение — 100, максимально возможное - 2000.

- *Приоритет процесса*

Приоритет, который получает процесс фонового мониторинга при разделении ресурсов в системе. Рекомендуемое значение — Нормальный.

- *Интервал запуска проверок по умолчанию*

Время, в течение которого проверка не будет выполняться. Установленное значение этого параметра присваивается автоматически при добавлении новой проверки. Можно задать интервал для проверок всех хостов в списке сразу, нажав кнопку «Задать для всех проверок».

- *Период обновления списка проверок (только в PRO-версии)*

Если взаимодействие службы мониторинга и графической консоли настроено через базу данных (подробнее об этом), то состояние проверок обновляется не сразу, а через заданный интервал. По умолчанию, это 5 секунд. Также, этот параметр влияет на период обновления статусов значков хостов на графической карте.

- *Ждать завершения проверок при остановке службы мониторинга*

При остановке службы OSNOVO Monitoring System Service программа пытается завершить все выполняемые проверки. Иногда это может занимать продолжительное время. При выключении этого параметра служба не завершает активные проверки.

- *Максимальное время выполнения VBScript и JScript*

Параметр, который позволяет регулировать время выполнения скриптов в программе. Некоторые скрипты могут работать продолжительное

время, и таймаута по умолчанию в 5 секунд может не хватить для их завершения. Для этого в программе есть этот параметр, позволяющий продлить время выполнения скриптов. К примеру, в проверке «Объём папки с подкаталогами» используется VBScript, который может работать по минуте и более, рекурсивно подсчитывая объём какой-нибудь папки (например, c:\Windows). При недостаточном таймауте проверка завершится с ошибкой. Этот параметр влияет на выполнение всех скриптов в программе.

Следует с вниманием относиться к установке слишком больших значений таймаута, потому что это может привести к слишком долгому выполнению проверок (в случае, если они зависли на сетевом запросе).

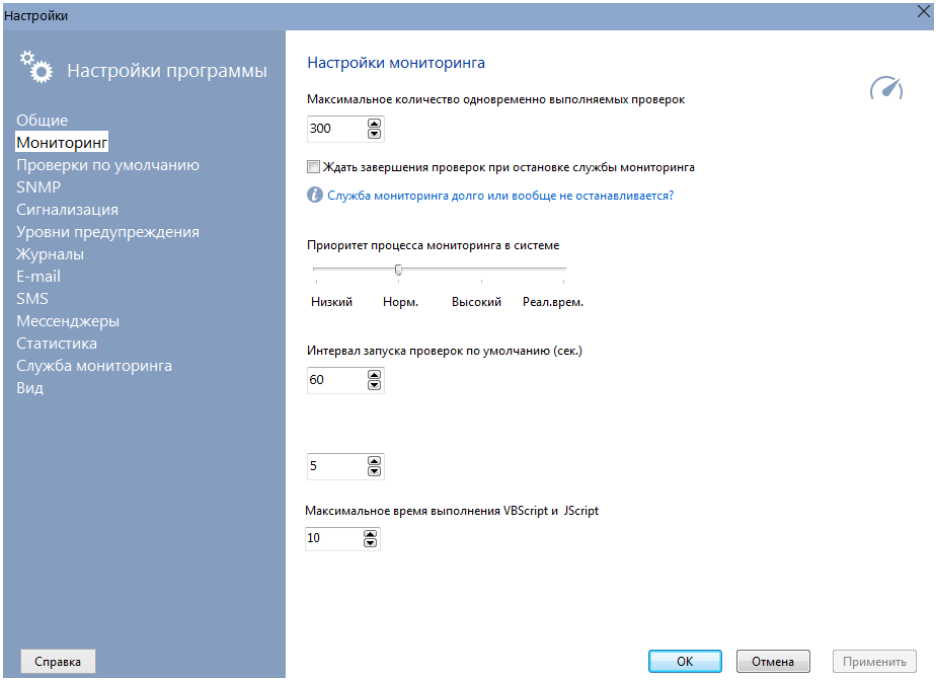


Рис. 97

9.3 Проверки по умолчанию

При добавлении нового хоста в список мониторинга (вручную, из результатов сканирования) ему автоматически могут быть назначены следующие проверки (рис. 98) с настраиваемыми параметрами:

- *ICMP-пинг*

– Время ожидания (в миллисекундах) - время, в течение которого программа ждет ответа от хоста.
– Количество пакетов - количество пакетов ICMP-пинга. Можно задать количество пакетов больше одного, чтобы исключить возможность ложного определения статуса объекта при потере одного пакета. Однако, увеличение количества пакетов ведет к увеличению времени проверки одного хоста.
– Размер пакета - объем ICMP-пакета в байтах.

- *TCP-порт*

– Порт - номер TCP-порта удаленной машины, к которому будет производиться попытка подключения.
– Время ожидания (в миллисекундах) - время, в течение которого программа ждет ответа от устройства.

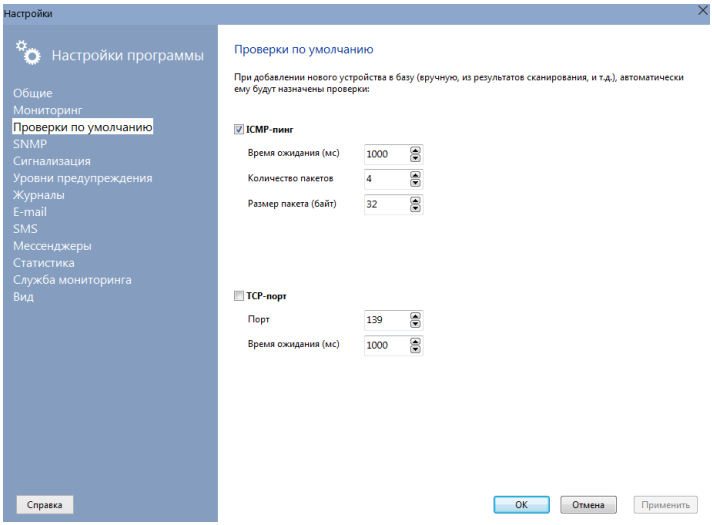


Рис. 98

9.4 Параметры SNMP

В разделе SNMP (рис. 99) задаются параметры, которые влияют на работу SNMP-функций программы:

- *Время ожидания ответа (мс)*

Время ожидания ответа от SNMP-агента во всех SNMP-функциях. Это глобальный параметр, который влияет на работу проверок, в которых используется подключение к удалённому хосту по SNMP. Если проверка возвращает ошибку 10060 "Время ожидания истекло", попробуйте увеличить этот параметр в 2-3 раза.

- *Использовать SNMP WinAPI*

Следует отключить этот параметр, если наблюдаются ошибки или подвисания программы при работе с SNMP (получение информации, мониторинг и т.д.). Эта опция разрешает использование функций из Windows API для получения информации по SNMP-протоколу, однако они не всегда корректно работают в процессе многопотокового мониторинга.

- *Учётные записи SNMP v3*

В этом списке можно задать список всех учётных записей, которые используются при подключении к различным устройствам по защищённой версии протокола SNMP v3. Эти записи можно использовать при задании параметров проверки SNMP (для облегчения ввода), при получении информации и в других функциях, где это нужно.

- Переводить OID переменных SNMP trap в имя.

Сообщения, принимаемые программой от устройств по SNMP (trap), обычно содержат переменные в виде их кодов (OID), к примеру, 1.3.6.1.2.1.1.3.0=10. Это не всегда удобно для понимания смысла, поэтому программа, используя информацию дерева MIB, может переводить коды в более понятные наименования переменных, к примеру: «.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime=10».

- *Выполнять текстовые замены в SNMP-trap*.

Как и в предыдущей опции, программа может заменять имена переменных на любые строки. К примеру, вышеупомянутую переменную 1.3.6.1.2.1.1.3.0 можно представить в сообщении как "Время работы".

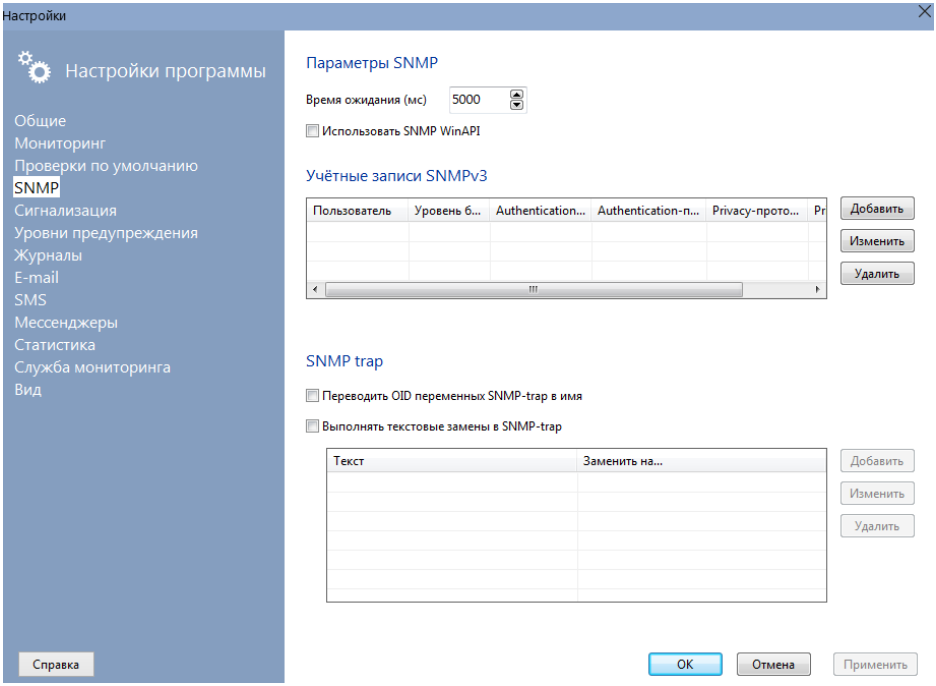


Рис. 99

9.5 Параметры сигнализации

В разделе «Сигнализация» (рис. 100) можно настроить параметры:

- *Реагировать на события*

– Всегда - сигнализация будет срабатывать при первом после загрузки программы опросе хостов.

– При изменении состояния - при первом опросе хостов программа запомнит состояние статуса проверок и при последующих их опросах будет реагировать только на изменение этого статуса.

- *Текст для сообщения, E-mail, SMS*

Задает текст сообщения, которое выдается на экран, отсылается как E-mail, SMS при срабатывании сигнализации на положительный результат проверки (Когда проверка прошла) и на отрицательный (Когда проверка

не прошла). Для подстановки в текст сообщения имени или адреса хоста, названия проверки, текущей даты и времени, подписи хоста в списке предназначены ключи:

- %A - адрес или имя хоста;
- %T - наименование проверки;
- %S - статус проверки ("OFF" или "ON"). Рекомендуется использовать его в тексте темы письма для сокращения длины;
- %D - текущие дата и время;
- %C - подпись хоста в списке;
- %U - текущий пользователь удаленного хоста;
- %DSC- описание проверки;
- %RET - символ переноса строки.

Все значения подставляются в текст сообщения автоматически.

- *Выдавать звуковые сигналы, не дожидаясь окончания предыдущего*.

Настройка позволяет настроить поведение звуковой сигнализации в различных функциях программы.

- *Показывать всплывающую подсказку (balloon tip) в tray*

При выборе этой опции программа будет выдавать на экран (в районе системного трея) всплывающую подсказку при срабатывании сигнализации. В подсказке будет отображаться сообщение, заданное при настройке сигнализации.

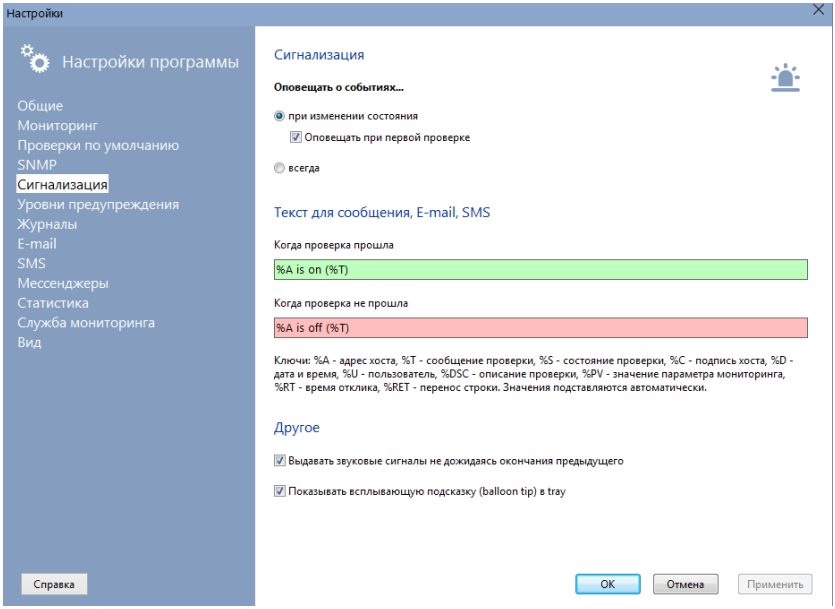


Рис. 100

9.6 Уровни предупреждения

В программе по умолчанию заложено 2 основных состояния проверки: "пройдена" (зелёная) и "не пройдена" (красная).

Однако, между ними можно добавить сколько угодно промежуточных уровней (рис. 101), которые будут сигнализировать о приближении аварийной ситуации. Например, можно добавить уровень "Предупреждение" (Warning) и реагировать на ситуацию еще до того, как произойдёт сбой. Переход проверки с одного такого уровня на другой так же сопровождается оповещением.

При переходе на более опасный уровень работают параметры "красной" сигнализации, а при обратном переходе на менее опасный уровень — "зелёной".

Каждый уровень характеризуется процентом от аварийного значения параметра. При добавлении нового уровня программа запрашивает его название и порог срабатывания в процентах. Цвет выделения проверки в списке назначается автоматически, в зависимости от введённого значения порога.

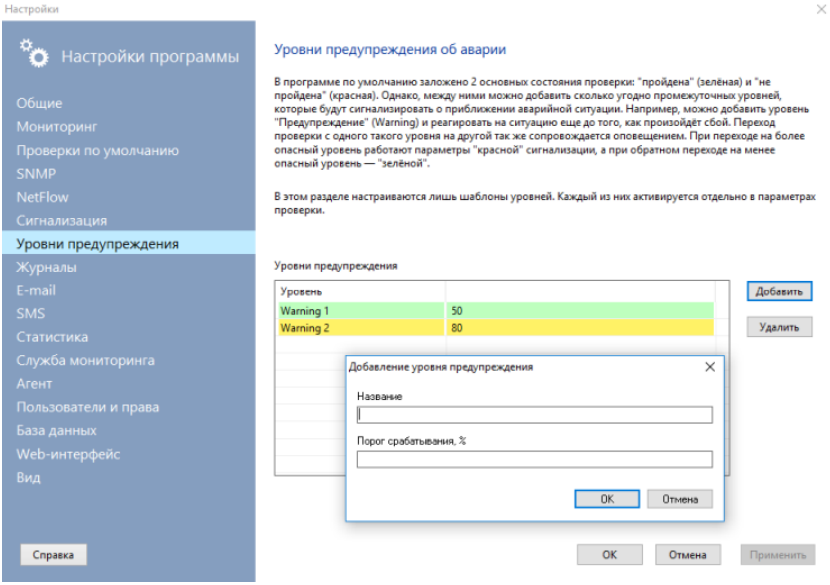


Рис. 101

9.7 Журналы

В этом разделе (рис. 102) можно настроить параметры:

- Имя файла журнала сигнализации

Полный путь к файлу журнала.

- *Добавлять или перезаписывать*

Действия при записи информации в существующий файл журнала. Если выбрано Добавлять, журнал не будет создаваться заново при новом запуске программы. При выборе Перезаписывать файл журнала будет очищаться каждый раз при новом запуске программы.

- *Обрезать длиннее*

Действие программы при достижении заданного объема файла журнала. Программа может автоматически контролировать объем файла журнала, не давая ему увеличиваться больше заданного значения. При достижении максимального объема программа удаляет первые записи журнала.

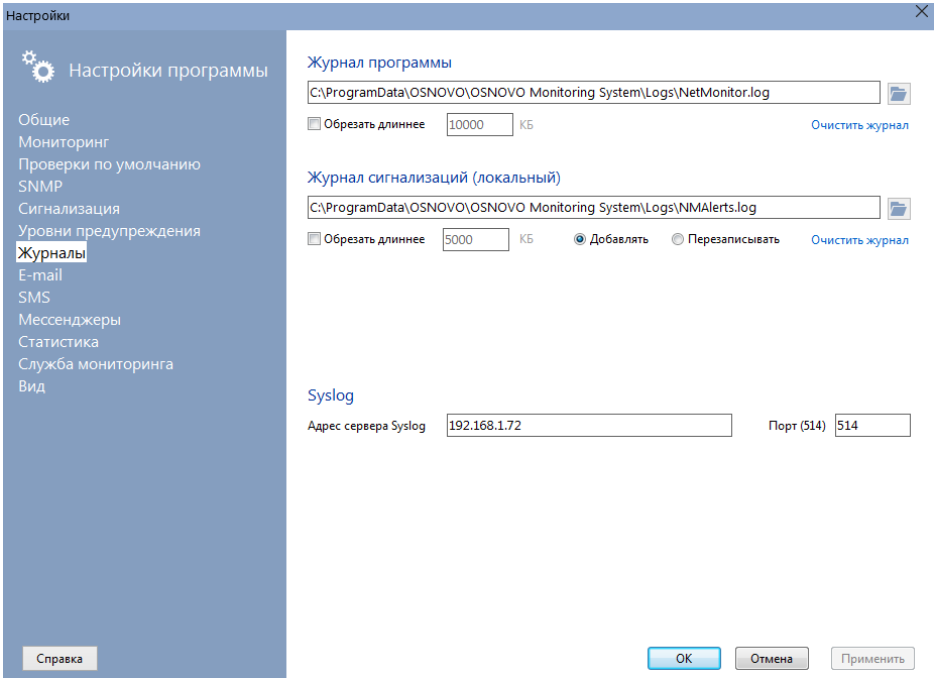


Рис. 102

9.8 Параметры E-mail

В этом разделе (рис. 103) можно настроить параметры отправки сообщения по электронной почте:

- *Адрес почтового (SMTP) сервера*;
- *Тип соединения и порт почтовой службы*. Поддерживается Безопасное соединение через TLS/SSL (порт 465) и обычное (стандартный порт - 25);
- *Адрес отправителя сообщения*;
- *Тема письма* (можно использовать ключи подстановки значений для текста сообщений);

- *Кодировка текста сообщения*.

- *SMTP-авторизация перед отправкой*

Если указанный вами почтовый сервер не обрабатывает неавторизованные сообщения (это можно узнать, прочитав соответствующую информацию на сайте почтового сервера), то вам необходимо будет установить флаг «Требуется SMTP-авторизация перед отправкой» и указать ваши «Логин» (имя пользователя) и «Пароль» (те, которые вы задавали при создании почтового ящика).

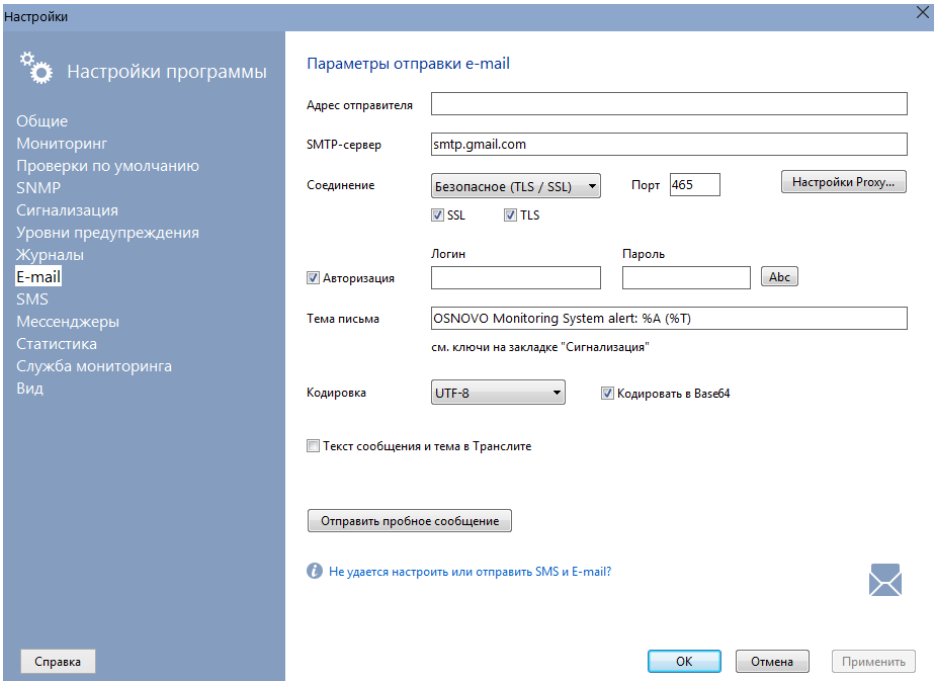


Рис. 103

9.9 Параметры SMS

Отправка SMS из программы может быть выполнена двумя способами (рис. 104):

1. *Путем отправки E-mail на SMS-шлюз вашего оператора сотовой связи*.

Для этого необходимо предварительно настроить параметры связи с SMS-шлюзом. В настройках отправки SMS необходимо указать адрес SMS-шлюза (можно узнать в абонентском отделе или поискать в Internet), правила формирования электронного письма (номер в теме письма, текст в теме письма), настроить параметры отправки e-mail. В поле номера телефона (окно Параметры проверки) следует указать номер телефона получателя (без знака "+"). Как правило, отправляя SMS через E-mail, вам не нужно платить деньги (зависит от оператора).

Внимание!
Если у вас возникли трудности в заполнении полей раздела E-mail и SMS или не удается их отправить, прочитайте раздел Вопросов и Ответов в разделе справки «FAQ»

2. *Через подключенный к компьютеру GSM-телефон*.

Основным требованием к телефону является возможность подключения его к компьютеру через USB или COM-порт. В случае подключения через USB-кабель необходимо установить драйвер, который создаст виртуальный COM-порт для данного телефона. Телефон должен иметь встроенный GSM-модем, поддерживающий основные AT-команды. Перед отправкой SMS из программы следует убедиться в нормальном функционировании модема телефона с помощью специальных программ для данной модели (как правило, они поставляются вместе с драйвером. Пример: "PC Suite").

В настройках программы следует указать COM-порт, к которому подключен телефон, задать скорость взаимодействия (можно оставить по умолчанию) и строку инициализации модема телефона (по умолчанию, "ATE0"). Параметры Четность, Биты и Стоп-биты являются специфическими и зачастую не нуждаются в изменении. Проверить взаимодействие программы и телефона можно, нажав кнопку

«Проверка...» . Программа должна выдать общую информацию о телефоне (модель, производитель, номер SMS-центра и др.).

Отправляя SMS этим способом вы должны помнить, что ваш оператор сотовой связи снимет со счета плату по установленному тарифу. Некоторые длинные сообщения, которые не умещаются в формат одной SMS, автоматически разбиваются на несколько отдельных.

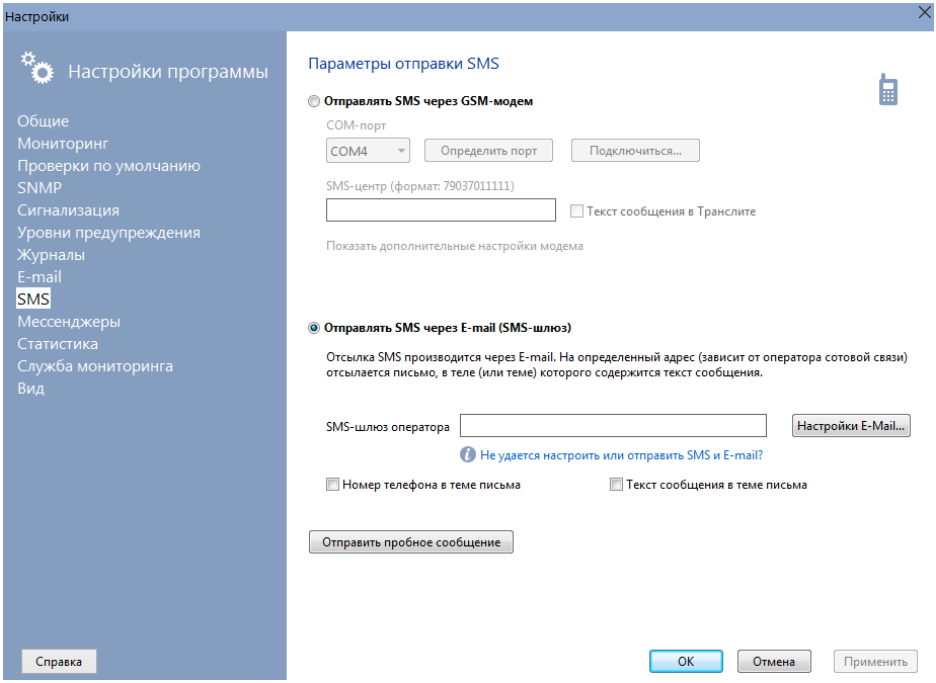


Рис. 104

9.10 Мессенджеры

ПО OMS может отправлять сообщения через сервисы популярных мессенджеров Slack и Telegram (рис. 105). Для того, чтобы этот тип оповещения мог работать, необходимо предварительно выполнить действия, описанные в документации этих сервисов.

- *Для Slack*:

– Зарегистрируйтесь в сервисе Slack.
– Включите интеграцию Slackbot для своей команды и получите свой Webhook URL.
– Укажите полученный Webhook URL вида https://hooks.slack.com/services/Txxxxxxxx/Bxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxxx в поле настроек.

- *Для Telegram:*

– Создайте в Telegram бота и получите его токен и ID чата, в который будут приходить сообщения.
– Укажите эти параметры в настройках.
– При необходимости, можно дополнительно задать параметры Proxy.

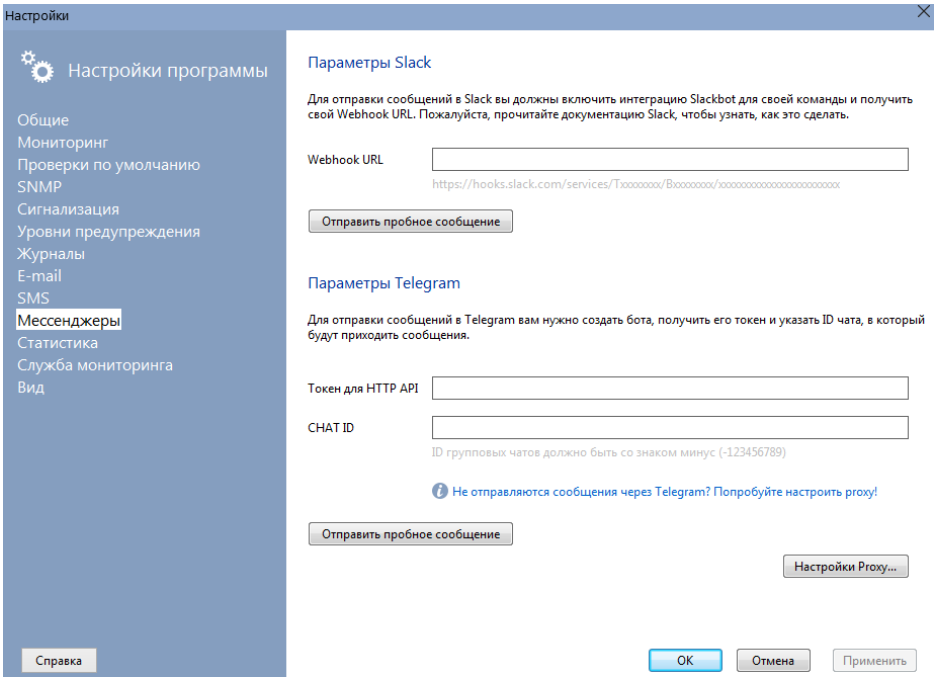


Рис. 105

9.11 Статистика

Большой объем накопленной статистики времени отклика (более 1 Мб на каждый хост) может существенно замедлить загрузку программы и ее работу. Рекомендуется периодически очищать ее (рис. 106), при необходимости сделав резервную копию.

Статистика времени отклика хранится в виде файлов с расширением .stat в каталоге данных программы (в папке профиля пользователя All Users): ...\OSNOVO\OSNOVO Monitoring System\RTStat\. Каждому хосту в списке мониторинга соответствует свой файл статистики.

Программа может автоматически (при загрузке) очищать накопленную статистику при достижении заданного объема файла. Для включения этой опции нужно поставить галочку в параметре «Автоматически очищать статистику времени отклика каждого хоста при достижении объема» и задать объем в килобайтах.

Если накопленная статистика имеет для вас значение, программа может сделать резервную копию файла перед удалением. Для этого нужно поставить галочку в параметре «Создавать резервную копию очищаемой статистики» файла .stat перед удалением.

В этом же разделе можно посмотреть общий объем накопленной статистики и произвести полную ее очистку, создав перед этим резервный архив.

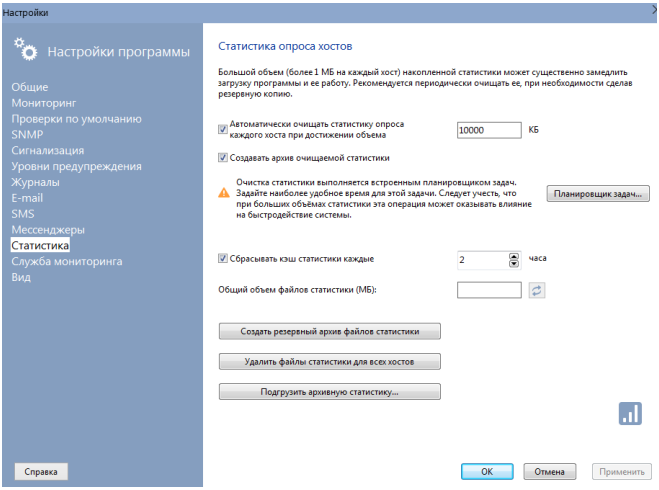


Рис. 106

9.12 Служба мониторинга

Механизм мониторинга хостов реализован в виде службы Windows. Это обеспечивает непрерывный контроль над работой важных служб и протоколов без вмешательства пользователя.

Для установки службы OSNOVO Monitoring System Service нужно нажать кнопку «Установить службу». Обычно выполнения этого действия не требуется в процессе использования программы, так как служба устанавливается автоматически. Для запуска/останова службы нужно нажать «Запустить» или «Остановить».

Внимание!
Следует учесть, что останавливая службу, вы останавливаете процесс мониторинга хостов.

В этом разделе настроек (рис. 107) можно управлять службой OSNOVO Monitoring System Service:

- *Производить ее запуск и остановку*

Для остановки процесса мониторинга необходимо остановить службу.

- *Производить установку и деинсталляцию службы*

Служба автоматически устанавливается при инсталляции программы на компьютер. Если есть необходимость удалить службу без деинсталляции самой программы, нужно нажать кнопку «Удалить службу».

- *Просматривать текущий статус службы*

- *Изменять TCP-порт связи графической консоли и службы*

Обмен информацией между графической консолью программы и службой происходит по TCP-протоколу. По умолчанию, в программе задан порт 57698. При необходимости этот порт можно изменить на любой другой, не занятый в системе. После изменения порта необходимо перезапустить службу и программу.

Следует учесть, что в ОС Windows Vista и ее более поздних версиях программы по умолчанию запускаются с правами пользователя. Однако для управления службами необходимы права администратора. В

связи с этим необходимо запустить программу от имени администратора. Либо использовать стандартные механизмы управления службами ОС Windows.

Очень важным условием при использовании проверки "MS SQL Server" с включенным параметром "Windows-аутентификация" является необходимость запуска службы от имени пользователя, прописанного в домене или в MS SQL Server. Для изменения имени пользователя, от которого запускается служба, необходимо выполнить действия:

- Нажать кнопку «Управление службами»;
- В появившемся окне «Службы» найти запись «OSNOVO Monitoring System Service» и двойным щелчком открыть диалог свойств службы;
- Перейти в диалоге на закладку Вход в систему, установить переключатель в положение «С учетной записью»;
- Нажать кнопку «Обзор», в открывшемся окне - кнопку «Дополнительно» и затем – «Поиск». Выбрать нужного пользователя, нажать кнопку «ОК» и еще раз «ОК»;
- В поле «Пароль» ввести пароль этого пользователя и еще раз - в поле «Подтверждение». Сохранить изменения кнопкой «ОК»;
- Перезапустить службу.

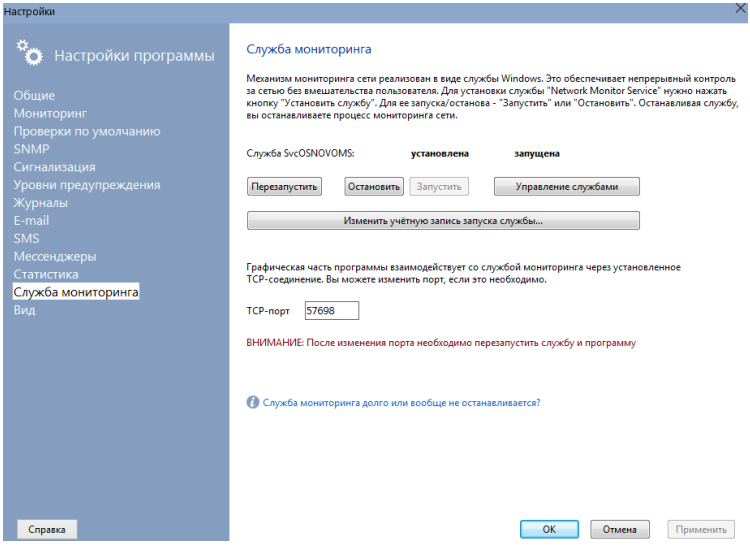


Рис. 107

9.13 Вид

В этом разделе (рис. 108) можно настроить параметры внешнего вида программы:

- *Столбцы списка проверок*

Можно скрыть ненужные столбцы или переименовать существующие. Изменить порядок расположения столбцов можно в самом списке в главном окне программы. Для этого выберите колонку, установите курсор на заголовке, нажмите левую кнопку мыши и тяните колонку в нужное место.

- *Сортировка хостов в дереве...*

Позволяет выбрать, как сортировать хосты в списке мониторинга. Хосты могут быть отсортированы как по адресу, так и по своему логическому имени (подписи) в порядке возрастания.

- *Символы для поддержки Unicode*

При использовании программы на компьютерах с языками, кроме русского и английского, необходимо выбрать соответствующую кодировку для корректного отображения специфических букв алфавита. Также может потребоваться изменение языка программ, не поддерживающих Unicode, в самой системе. Для этого нажмите кнопку «Язык системы...», затем в системном диалоге «Регион» перейдите на вкладку «Дополнительно» и нажмите «Изменить язык системы...», рис. 109

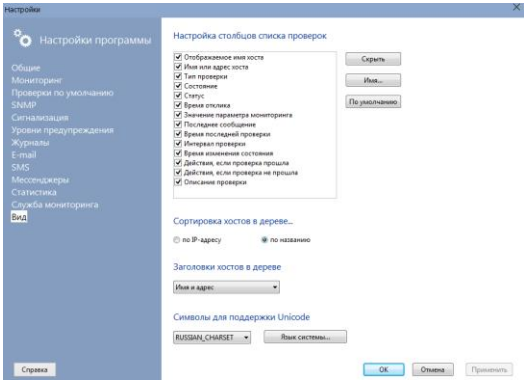


Рис. 108

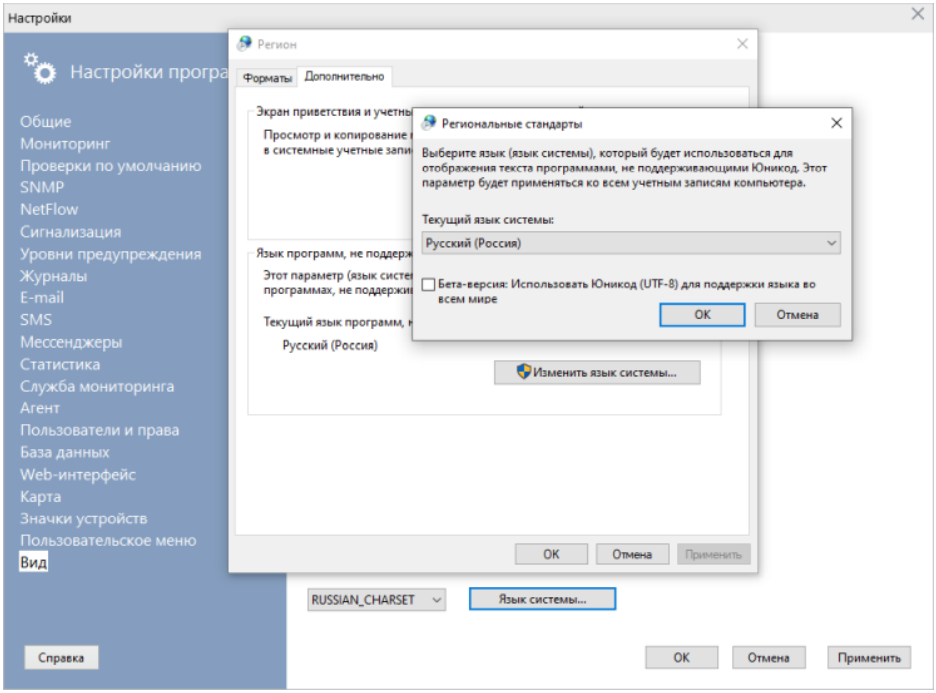


Рис. 109

Дополнительную информацию об элементах ПО OMS, их настройке и пр. Вы можете узнать из файла справки FAQ, доступного по пути «Справка / Содержание»

Составил: Елагин С.А.

Приобрести программное обеспечение OSNOVO Monitoring System и узнать дополнительную информацию по версиям ПО можно на сайте www.osnovo.ru