



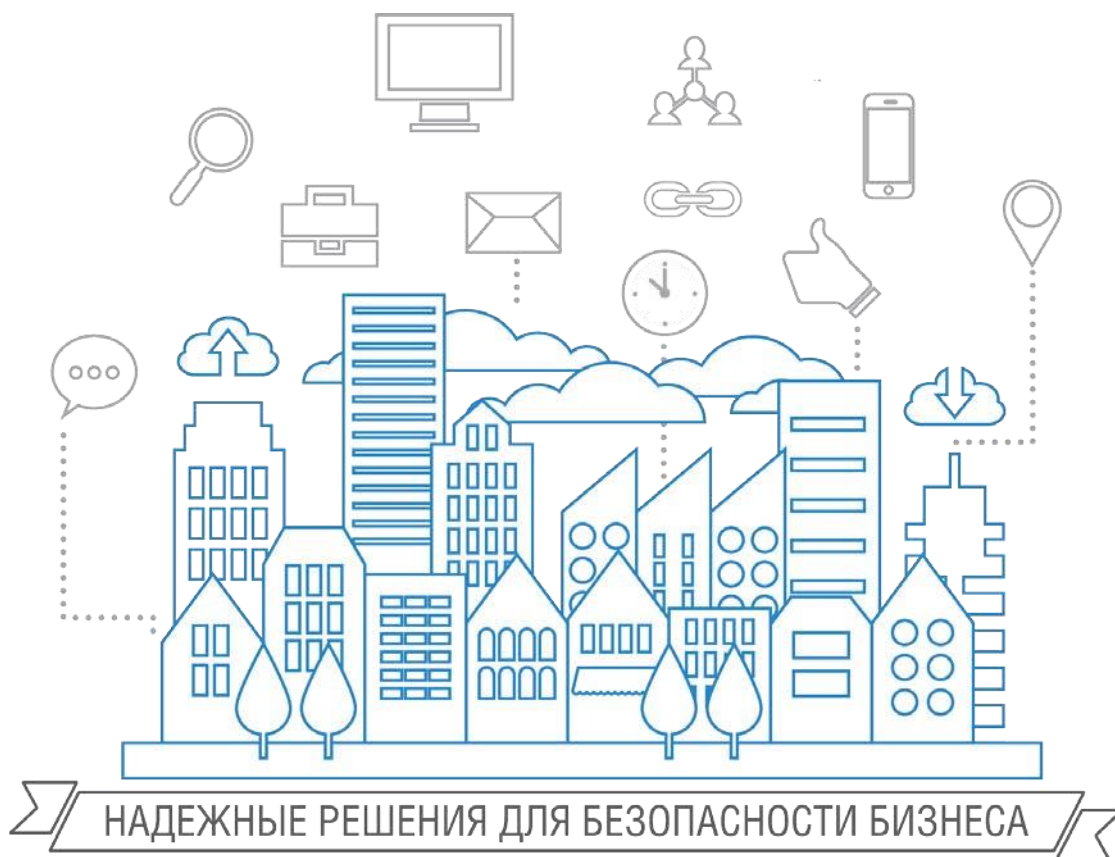
ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51 Почтовый адрес: 198096,
г. Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт -Пет ербу рге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

**Средство защиты информации
от несанкционированного доступа
«Блокхост-сеть 2.0»**

Руководство администратора

Контроль реестра



Санкт-Петербург, 2018

Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-сеть 2.0» (далее по тексту – СЗИ «Блокхост-сеть 2.0») и содержит описание работы с программным модулем контроля целостности реестра, входящим в состав СЗИ «Блокхост-сеть 2.0».

Знаки, расположенные на полях руководства, указывают на примечания. Степени важности примечаний:



Важная информация, информация предостерегающего характера.



Дополнительная информация, примеры.

Содержание

1 Назначение модуля контроля целостности реестра	4
2 Условия применения.....	6
3 Автономный вариант модуля контроля целостности реестра	6
3.1 Запуск локальной консоли управления модуля	6
3.2 Внешний вид локальной консоли управления модуля.....	8
3.3 Контроль целостности реестра локальной рабочей станции.....	10
3.4 Управление службами локальной рабочей станции.....	12
3.5 Управление драйверами локальной рабочей станции.....	13
3.6 Управление списком автозагрузки программ локальной рабочей станции.....	14
4 Вариант модуля контроля целостности реестра с удаленным управлением	15
4.1 Запуск консоли управления модуля	15
4.2 Виды аутентификации	16
4.2.1 Локальная аутентификация	16
4.2.2 Сетевая аутентификация.....	17
4.2.3 Редактор политик	22
5 Отображение и фиксация нарушений	28
5.1 Отображение нарушений	28
5.2 Фиксация нарушений.....	28

1 Назначение модуля контроля целостности реестра

Программный модуль контроля целостности реестра СЗИ «Блокхост-сеть 2.0» (далее по тексту - модуль контроля целостности реестра, модуль, программа) реализован в двух вариантах:

1) *автономный вариант*, устанавливается на рабочее место пользователя и позволяет:

- контролировать целостность объектов реестра Windows¹ локальной рабочей станции;
- включать/выключать автозапуск системных служб и драйверов локальной рабочей станции через соответствующие ключи реестра;
- редактировать список автозагрузки программ локальной рабочей станции через соответствующие ключи реестра.

2) *вариант с удаленным управлением*, устанавливается на рабочее место администратора безопасности и позволяет:

- контролировать целостность объектов реестра Windows локальной/удаленной рабочей станции;
- включать/выключать автозапуск системных служб и драйверов локальной/удаленной рабочей станции через соответствующие ключи реестра;
- редактировать список автозагрузки программ локальной/удаленной рабочей станции через соответствующие ключи реестра;
- формировать политику контроля целостности реестра рабочих станций в сети.

Модуль контроля целостности реестра осуществляет контроль целостности реестра Windows по следующим типам событий:

- переименование/удаление контролируемого раздела;
- добавление подраздела в контролируемый раздел;
- удаление существующего подраздела из контролируемого раздела;
- изменение названия подраздела в контролируемом разделе;
- добавление нового параметра в контролируемый раздел;
- изменение названия параметра в контролируемом разделе;
- удаление параметра в контролируемом разделе;
- изменение значения параметра в контролируемом разделе.

Механизм контроля целостности реестра выполняет проверку целостности реестра путём сравнения с эталоном и при обнаружении ошибки информирует об этом пользователя.

Модуль контроля целостности реестра позволяет осуществлять восстановление поврежденного или несанкционированно измененного раздела/параметра/значения параметра реестра.

Модуль контроля целостности реестра осуществляет контроль целостности собственных программных компонентов по алгоритму CRC-32 и при обнаружении изменений в файле происходит предупреждение о нарушении целостности. Запуск измененных файлов невозможен. Этот механизм используется для контроля программного модуля после сбоев и отказов оборудования.

Модуль контроля целостности реестра запускается в качестве сервиса (службы) Windows

¹ Под объектами реестра Windows понимаются разделы (ветви), параметры (ключи) и значения параметров реестра.



(GIS.RegistryControl.Service) при загрузке системы и постоянно находится в памяти до перезагрузки компьютера. Модуль фиксирует в журналах аудита нарушение целостности поставленных на контроль объектов реестра.

Программный модуль контроля целостности реестра применяется в составе СЗИ «Блокхост-сеть 2.0».

Знаки, расположенные на полях документа, указывают на примечания. Степени важности примечаний:



Важная информация, информация предостерегающего характера



Дополнительная информация, примеры.

2 Условия применения

Установка модуля контроля целостности реестра производится на рабочие станции, функционирующие под управлением ОС семейства Windows.

В состав установленного программного обеспечения рабочей станции должны входить:

- .NET Framework 3.5;
- Windows Installer 3.1 и выше;
- СЗИ «Блокхост-сеть 2.0».

Состав программного обеспечения, необходимого для установки СЗИ «Блокхост-сеть 2.0», приведен в документах «СЗИ «Блокхост-сеть 2.0». Руководство по инсталляции (автономный вариант)» и СЗИ «Блокхост-сеть 2.0». Руководство по инсталляции (вариант с удаленным управлением)».

3 Автономный вариант модуля контроля целостности реестра

Автономный вариант модуля контроля целостности реестра позволяет:

- контролировать целостность реестра локальной рабочей станции;
- включать/выключать автозапуск системных служб и драйверов локальной рабочей станции через соответствующие ключи реестра;
- редактировать список автозагрузки программ локальной рабочей станции через соответствующие ключи реестра.

Перечисленные возможности осуществляются через **локальную консоль управления** модуля.

3.1 Запуск локальной консоли управления модуля

Запустить консоль управления модуля можно одним из способов:

- 1) на панели задач нажать кнопку «**Пуск**» и выбрать пункт «**Все программы**» → «**GIS.RegistryControl**» → «**GIS.RegistryControl.exe**» (рис. 3.1);

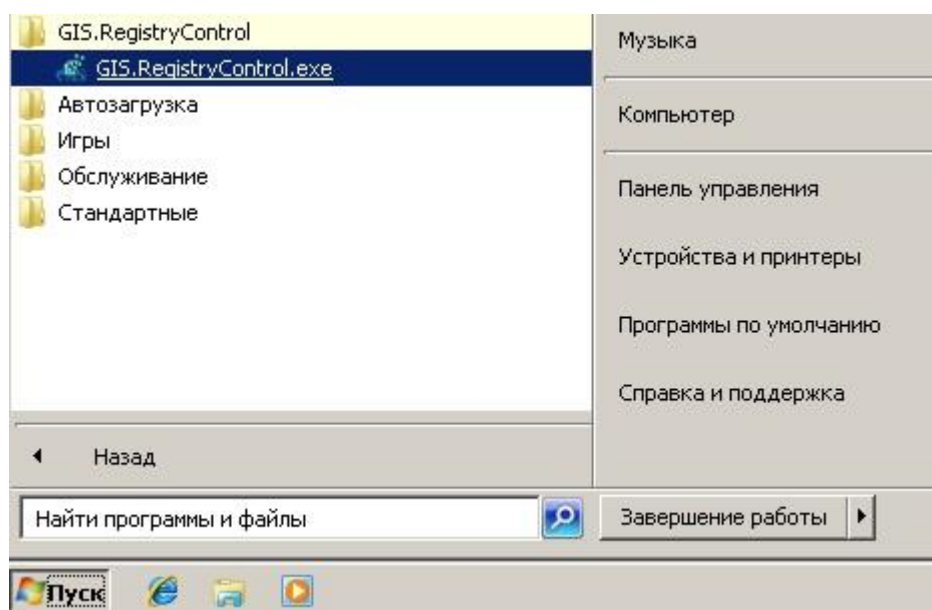


Рисунок 3.1. Запуск консоли управления модуля из меню «Пуск»

- 2) в области уведомлений нажать правой кнопкой мыши на значок  и выбрать пункт

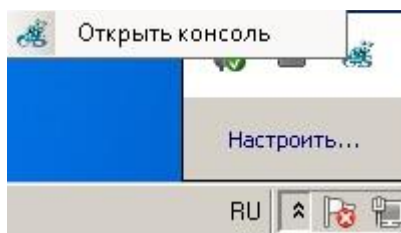



Рисунок 3.2. Запуск консоли управления модуля из области уведомлений



Запуск консоли управления модуля желательно осуществлять от имени пользователя, имеющего права администратора.

После запуска консоли управления появится окно **локальной** аутентификации (рис. 3.3), для прохождения которой необходимо ввести пароль и нажать кнопку подтверждения .

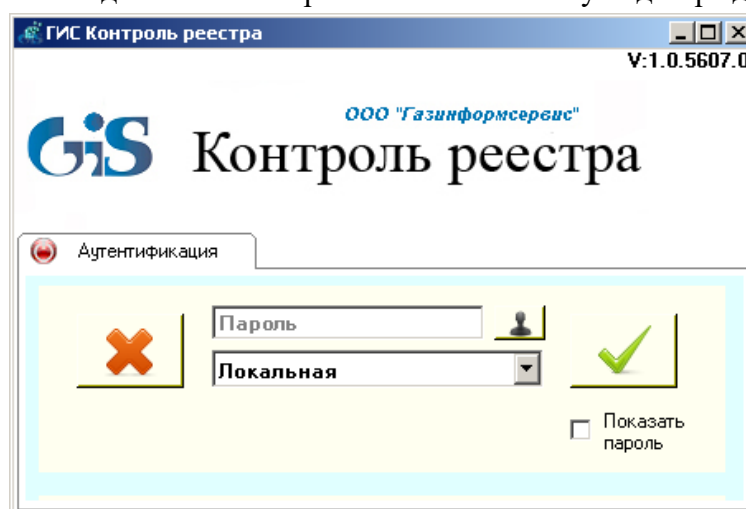





Рисунок 3.3. Окно аутентификации

По умолчанию для прохождения локальной аутентификации установлен пароль «1234567890».

Для отображения введенного пароля необходимо установить указатель напротив поля «Показать пароль». Для закрытия окна аутентификации необходимо нажать кнопку «Закрыть» .

Для изменения пароля администратору безопасности необходимо нажать кнопку , при этом окно аутентификации примет вид, показанный на рисунке 3.4, ввести старый и новый пароли, затем нажать кнопку .

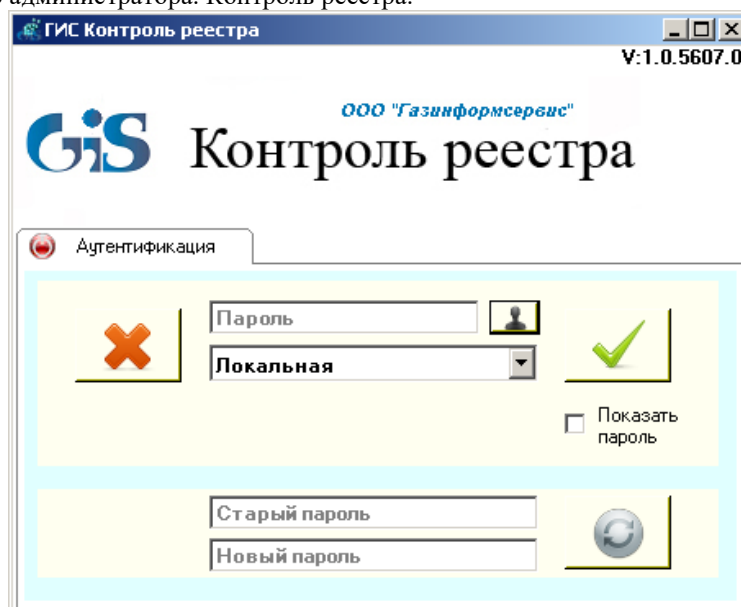


Рисунок 3.4. Смена пароля

3.2 Внешний вид локальной консоли управления модуля

После прохождения **локальной** аутентификации появится локальная консоль управления модуля (рис. 3.5).

Консоль управления содержит следующие вкладки:

- Вкладка «Контроль реестра» позволяет формировать перечень контролируемых объектов реестра (разделов, параметров и значений параметров реестра Windows);
- Вкладка «Службы» позволяет через соответствующие ключи реестра включать и отключать автозапуск системных служб локальной рабочей станции;
- Вкладка «Драйверы» позволяет через соответствующие ключи реестра включать и отключать автозагрузку драйверов локальной рабочей станции;
- Вкладка «Автозагрузка» позволяет через соответствующие ключи реестра редактировать список автозагрузки программ локальной рабочей станции.

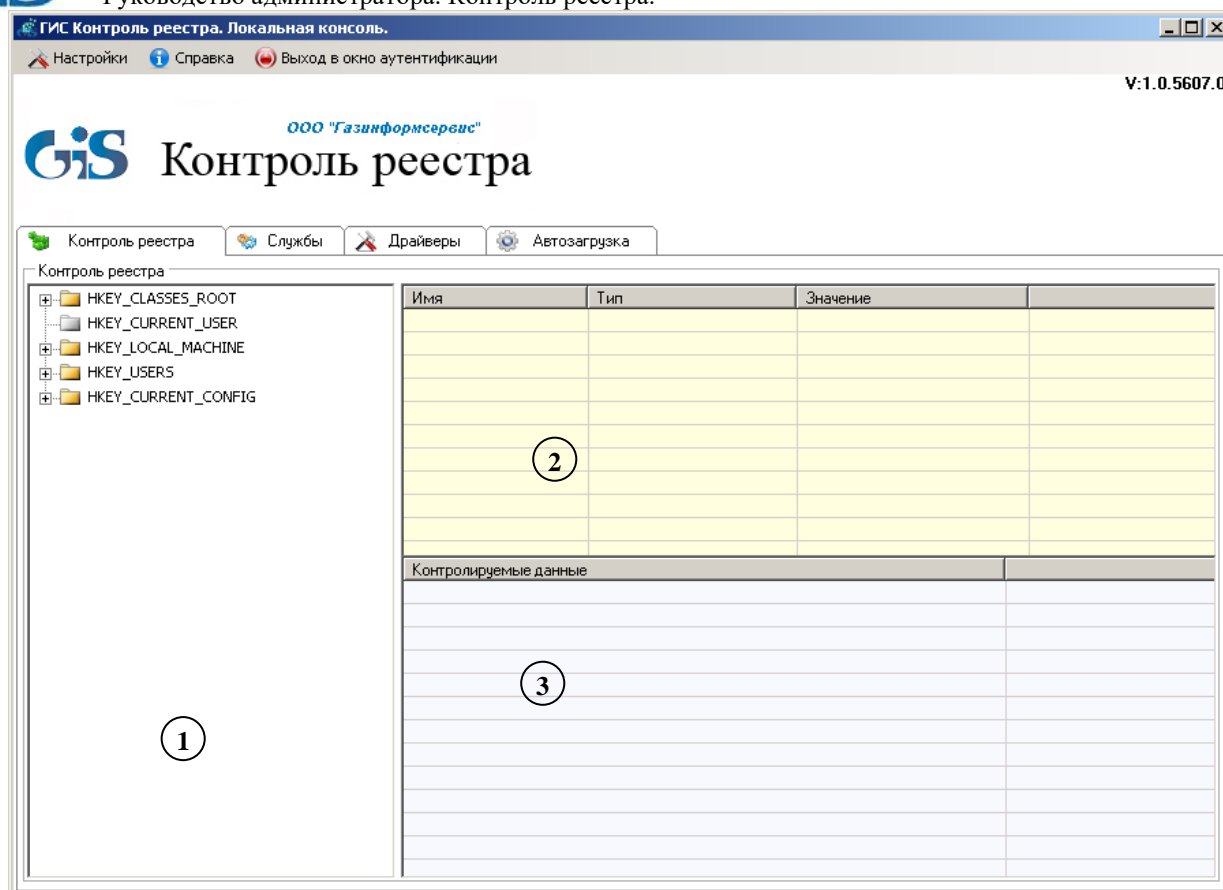


Рисунок 3.5. Локальная консоль управления модуля контроля целостности реестра

Кроме того, консоль управления содержит пункты меню:

- Пункт «Настройки» (рис. 3.6) содержит подпункты «Настройки Syslog» и «Выход»:

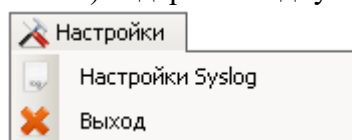


Рисунок 3.6. Вид пункта «Настройки»

При выборе подпункта «Настройки Syslog» появляется окно (рис. 3.7), в котором можно указать настройки Syslog-сервера для отправки сообщений об обнаруженных нарушениях целостности контролируемых объектов реестра.

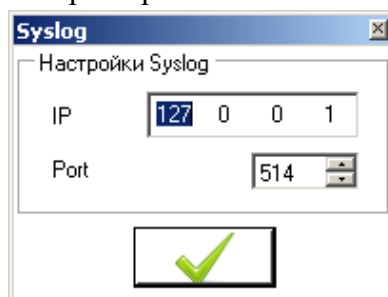


Рисунок 3.7. Настройки Syslog-сервера

- Пункт «Справка» позволяет получить справочную информацию о программе;
- Пункт «Выход в окно аутентификации» предназначен для выхода в окно аутентификации (рис. 3.3).

3.3 Контроль целостности реестра локальной рабочей станции

Вкладка «Контроль реестра» позволяет осуществлять контроль целостности реестра локальной рабочей станции и состоит из 3 областей (рис. 3.5):

- 1 – Область отображения дерева реестра локальной рабочей станции;
- 2 – Область отображения содержимого разделов реестра (наименования, типа и значений параметров);
- 3 – Область контролируемых данных.

При перемещении по дереву реестра содержимое его ветвей будет отображаться в области № 2 (рис. 3.8).

Для постановки на контроль объектов реестра необходимо выбрать их в дереве реестра и перетащить в область контролируемых данных:

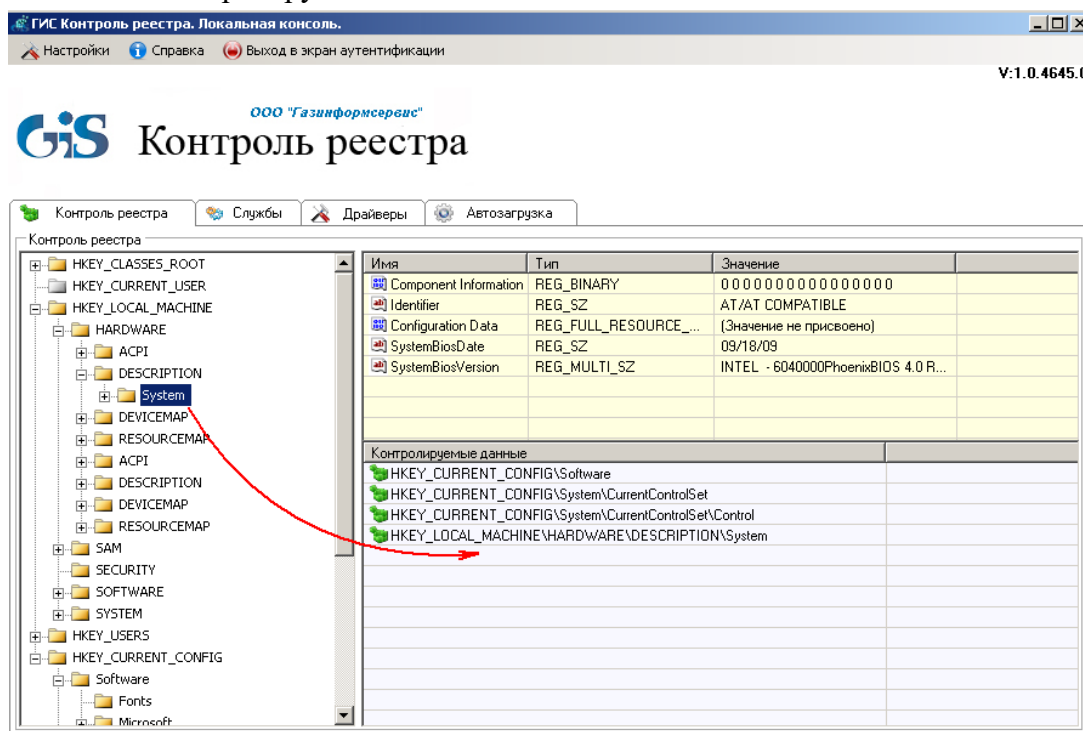


Рисунок 3.8. Отображение объектов реестра

Невозможно поставить на контроль:

- 1) корневые разделы реестра;
- 2) раздел реестра HKEY_CURRENT_USER, который является ссылкой на определенный подраздел раздела HKEY_USERS. Настройки соответствуют текущему (активному) пользователю, выполнившему вход в систему.

После добавления объектов реестра на контроль над ними доступны следующие действия (рис. 3.9):

- *Удалить* – удаление объектов реестра из области контролируемых данных;
- *Обновить* – сохранение изменений в контролируемом разделе в качестве эталона;
- *Восстановить* – восстановление целостности нарушенных объектов реестра;
- *Проверить раздел* (проверка раздела реестра и отображение нарушений). После завершения проверки появляется окно с информацией об изменениях (рис. 3.10).
- *Проверить только изменения* (проверка и отображение только изменений). После завершения проверки появляется окно с информацией об изменениях (рис. 3.11).

- *Экспорт настроек* (сохранение настроек контроля целостности в текстовый файл).

Пример содержимого файла с сохраненными настройками приведен на рис. 3.12. Сохраненные настройки могут быть в дальнейшем импортированы в область контролируемых объектов консоли управления модуля.

- *Импорт настроек* (импорт сохраненных в текстовом файле настроек в область контролируемых данных).

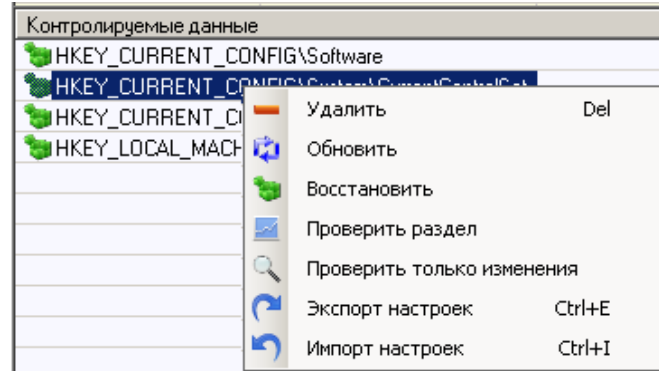


Рисунок 3.9. Контекстное меню

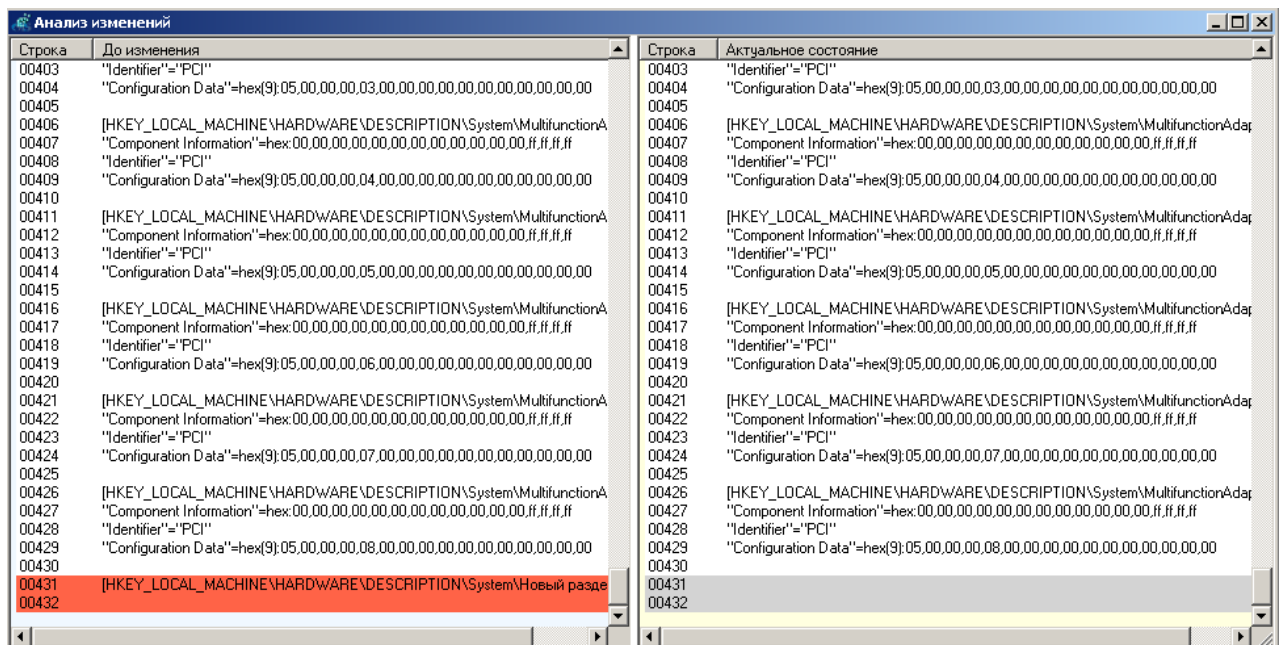


Рисунок 3.10. Проверка ветви реестра

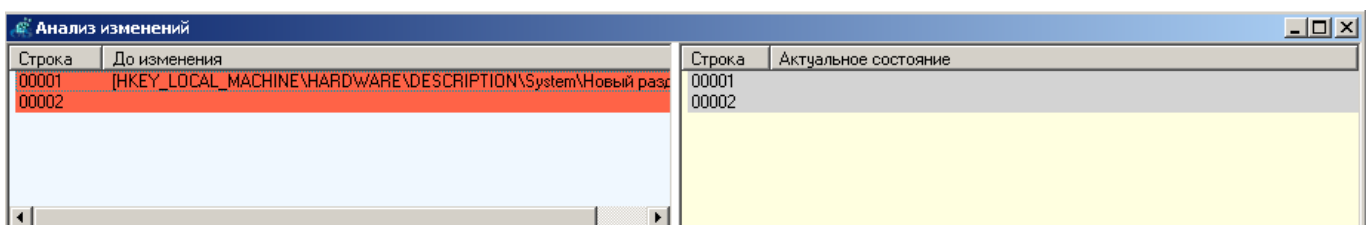
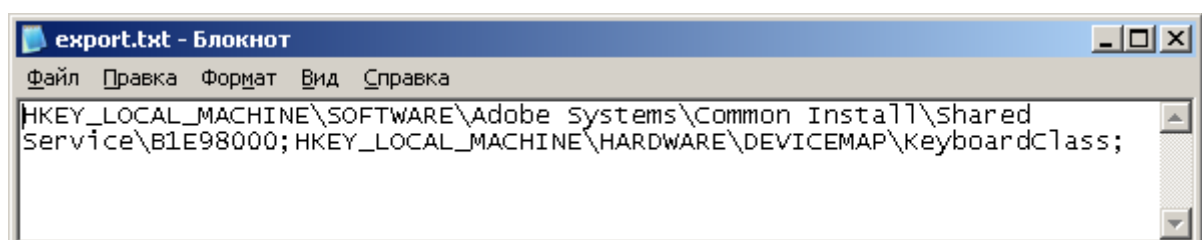


Рисунок 3.11. Проверка только изменений





Несанкционированное изменение ключей реестра может привести к краху системы!

3.4 Управление службами локальной рабочей станции

Вкладка «Службы» отображает список служб локальной рабочей станции (рис. 3.13).

Напротив служб, запускаемых при загрузке ОС, установлен указатель ☒.

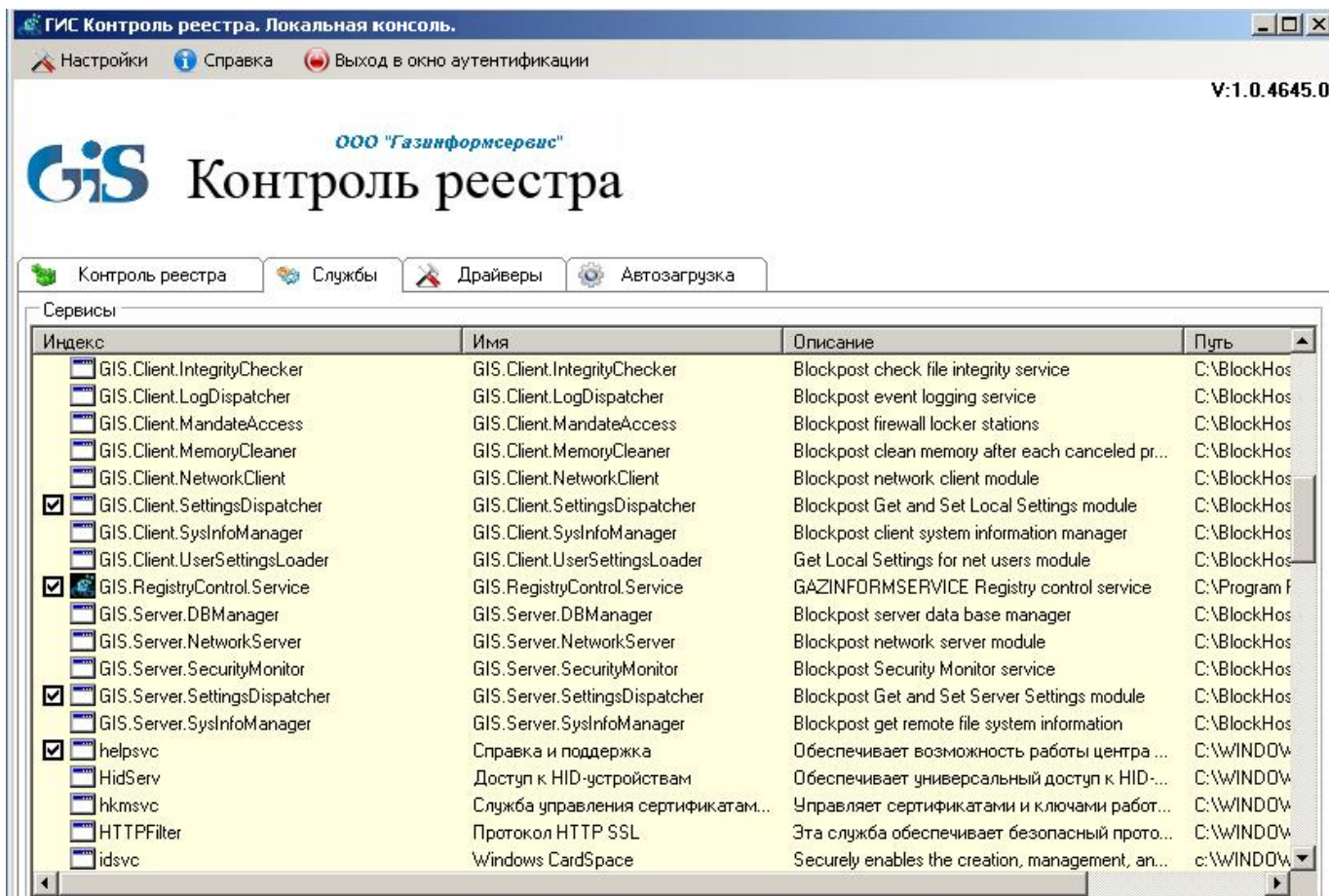


Рисунок 3.13. Вкладка служб локальной рабочей станции

Контекстное меню (рис. 14), вызываемое по щелчку правой кнопкой мыши на службе, позволяет включать/отключать автозапуск служб при загрузке ОС. Для этого нужно воспользоваться пунктами контекстного меню «Включить» или «Выключить».

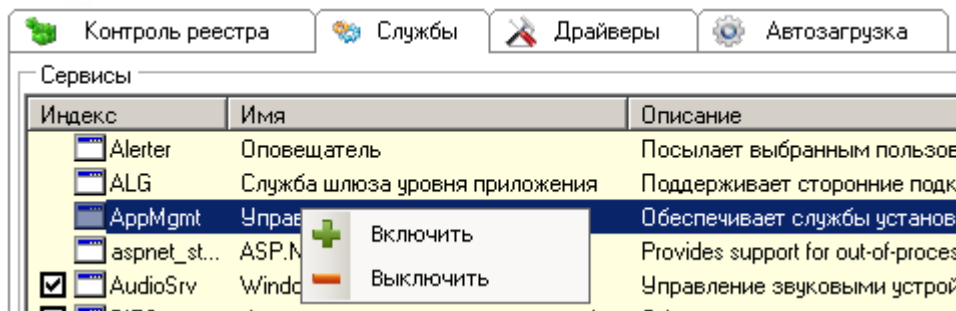


Рисунок 3.14. Включение/выключение автозапуска служб локальной рабочей станции

При выборе пункта «Включить» или «Выключить» появится сообщение, приведенное на рис. 3.15. При нажатии кнопки подтверждения автозапуск службы будет включен/отключен. В

соответствующие ключи реестра Windows при этом будут внесены изменения. Применение настроек автозапуска системных служб произойдет при последующей загрузке ОС.



Рисунок 3.15. Подтверждения произведенных изменений

3.5 Управление драйверами локальной рабочей станции

Вкладка «Драйверы» отображает список драйверов локальной рабочей станции (рис. 3.16). Напротив драйверов, загружаемых при загрузке ОС, установлен указатель ☒.

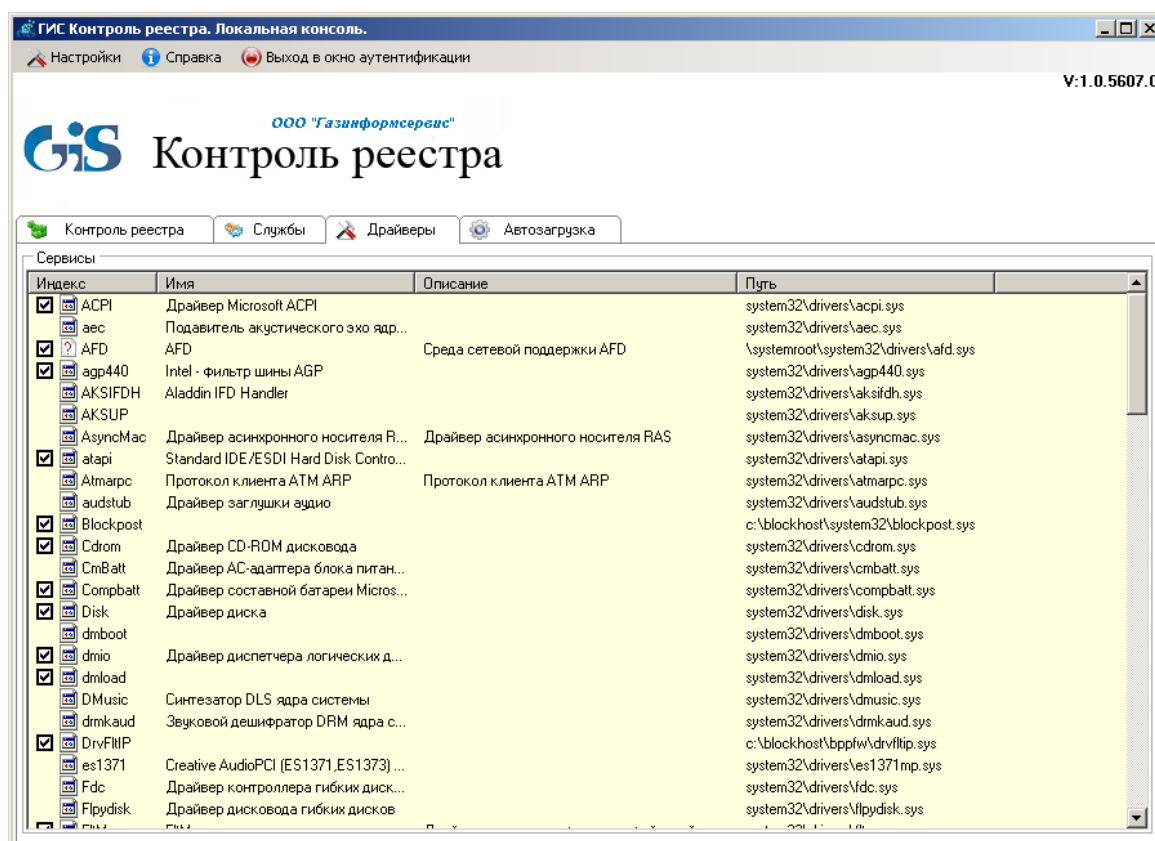


Рисунок 3.16. Вкладка драйверов локальной рабочей станции

Контекстное меню (рис. 3.17), вызываемое по щелчку правой кнопкой мыши на драйвере, позволяет через соответствующие ключи реестра включать и отключать автозагрузку соответствующего драйвера.

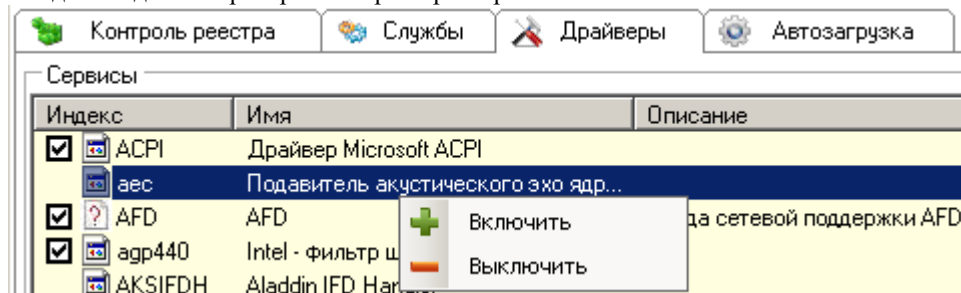


Рисунок 3.17. Включение/выключение автозагрузки драйверов локальной рабочей станции

При выборе пункта «Включить» или «Выключить» контекстного меню появится сообщение, приведенное на рис. 3.18. После нажатии кнопки подтверждения автозагрузка драйвера будет включена/отключена, при этом в соответствующие ключи реестра Windows будут внесены изменения. Применение настроек автозагрузки драйверов произойдет при последующей загрузке ОС.



Рисунок 3.18. Подтверждения произведенных изменений

3.6 Управление списком автозагрузки программ локальной рабочей станции

Вкладка «Автозагрузка» отображает список автозагрузки программ рабочей станции:

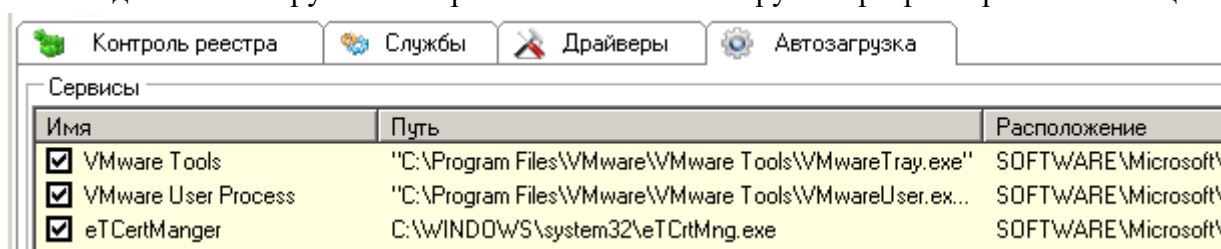


Рисунок 3.19. Вкладка «Автозагрузка»

Контекстное меню, вызываемое по щелчку правой кнопкой мыши на программе в списке (рис. 3.20), позволяет удалять соответствующие ей записи из реестра.



Рисунок 3.20. Редактирование списка автозагрузки рабочей станции

4 Вариант модуля контроля целостности реестра с удаленным управлением

Вариант программы с удаленным управлением позволяет:

- контролировать целостность реестра локальной/удаленной рабочей станции;
- включать/выключать автозапуск системных служб и драйверов локальной/удаленной рабочей станции через соответствующие ключи реестра;
- редактировать список автозагрузки программ локальной/удаленной рабочей станции через соответствующие ключи реестра;
- формировать политику контроля целостности реестра рабочих станций в сети.

Перечисленные возможности осуществляются через **локальную, серверную консоли** или **консоль редактора политик**.

4.1 Запуск консоли управления модуля

Запустить консоль управления модуля можно одним из способов:

- 1) на панели задач нажать кнопку «**Пуск**» и выбрать пункт «**Все программы**» → «**GIS.RegistryControlServer**» → «**GIS.RegistryControlServer.exe**»:

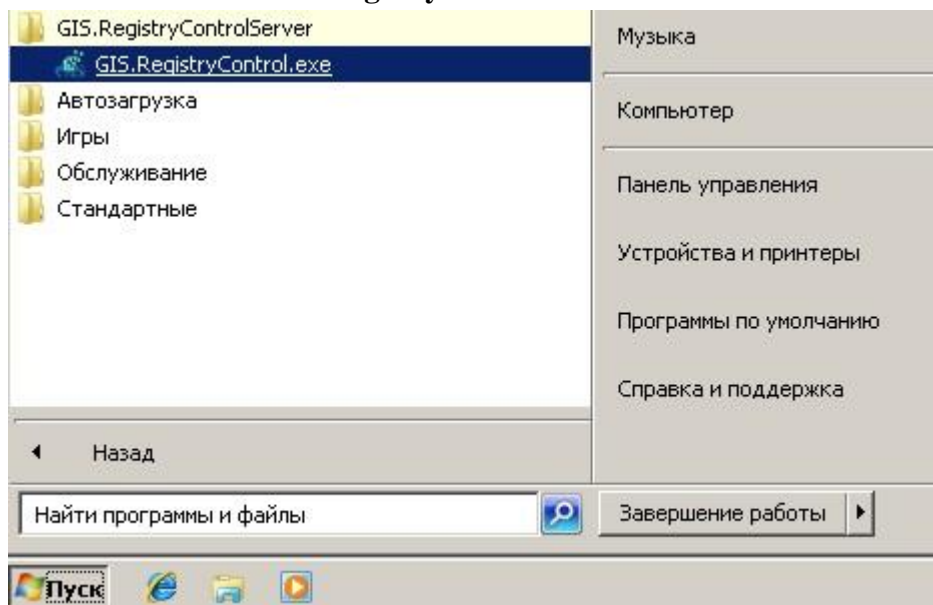



Рисунок 4.1. Запуск консоли управления модуля из меню «Пуск»

- 2) в области уведомлений нажать правой кнопкой мыши на значок  и выбрать пункт «**Открыть консоль**» (рис. 4.2).

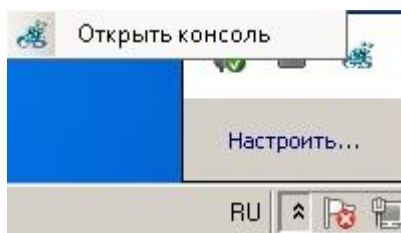



Рисунок 4.2. Запуск консоли управления модуля из области уведомлений



Запуск консоли управления желательно осуществлять от имени пользователя, имеющего права администратора.

4.2 Виды аутентификации

После запуска консоли управления появится окно аутентификации (рис. 4.3), для прохождения которой необходимо ввести пароль, выбрать **вид аутентификации** и нажать кнопку подтверждения .

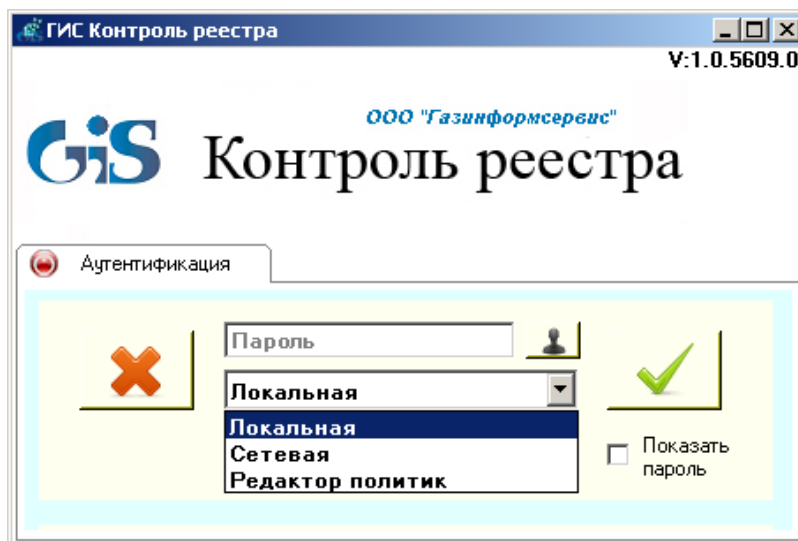


Рисунок 4.3. Окно аутентификации

В варианте программы с удаленным управлением предусмотрено три возможных вида аутентификации:

- *Локальная* (контроль реестра локальной рабочей станции);
- *Сетевая* (контроль реестра удаленных рабочих станций);
- *Редактор политик* (формирование политик контроля целостности реестра рабочих станций в сети).

4.2.1 Локальная аутентификация

Описание прохождения **локальной** аутентификации приведено в подразделе 3.1 настоящего документа.


После прохождения локальной аутентификации появится локальная консоль управления модуля, описание которой приведено в подразделе 3.2 настоящего документа.

Локальная консоль управления модуля позволяет:

- формировать перечень контролируемых объектов реестра (разделов, параметров, значений параметров реестра) локальной рабочей станции (см. подраздел 3.3 настоящего документа);
- через соответствующие ключи реестра включать и отключать автозапуск системных служб локальной рабочей станции (см. подраздел 3.4 настоящего документа);
- через соответствующие ключи реестра включать и отключать автозагрузку драйверов локальной рабочей станции (см. подраздел 3.5 настоящего документа);
- редактировать список автозагрузки программ локальной рабочей станции через соответствующие ключи реестра (см. подраздел 3.6 настоящего документа).

4.2.2 Сетевая аутентификация

Для контроля целостности реестра удаленных рабочих станций необходимо в окне аутентификации (рис. 4.4) выбрать вид аутентификации «Сетевая», ввести пароль, IP-адрес удаленной рабочей станции и нажать кнопку подтверждения.

По умолчанию для прохождения сетевой аутентификации установлен пароль «0987654321». Для его изменения можно использовать кнопку .

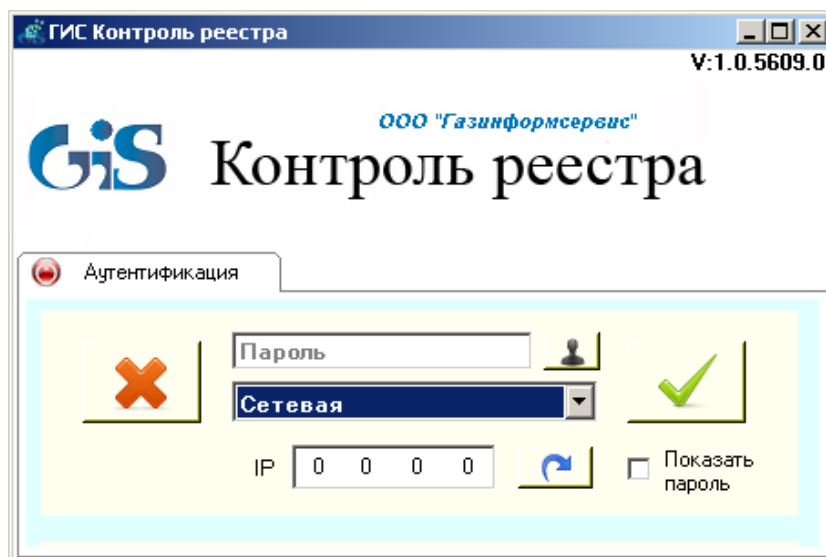



Рисунок 4.4. Сетевая аутентификация

Для просмотра ранее введенных IP-адресов необходимо нажать кнопку , после чего появится окно со списком адресов:

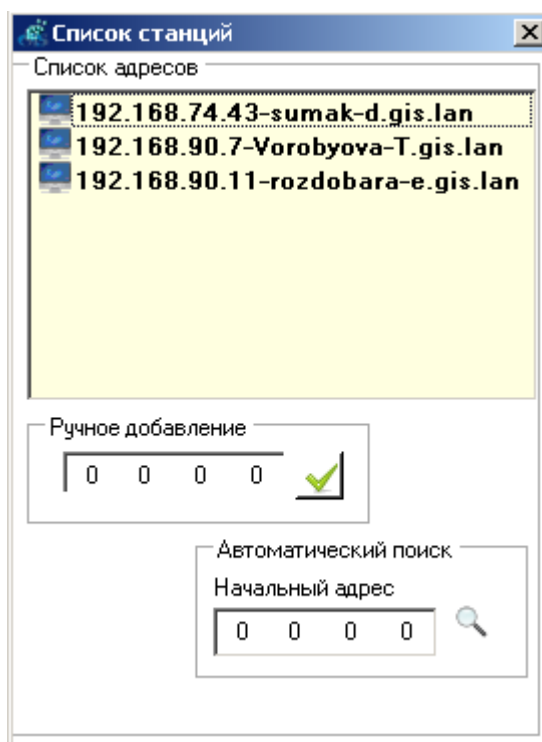


Рисунок 4.5. Список набранных адресов

Для добавления новых адресов в список можно использовать «Ручное добавление» (ввод адреса вручную) или «Автоматический поиск» (поиск адресов по заданному начальному адресу

После прохождения сетевой аутентификации появится серверная консоль управления модуля:

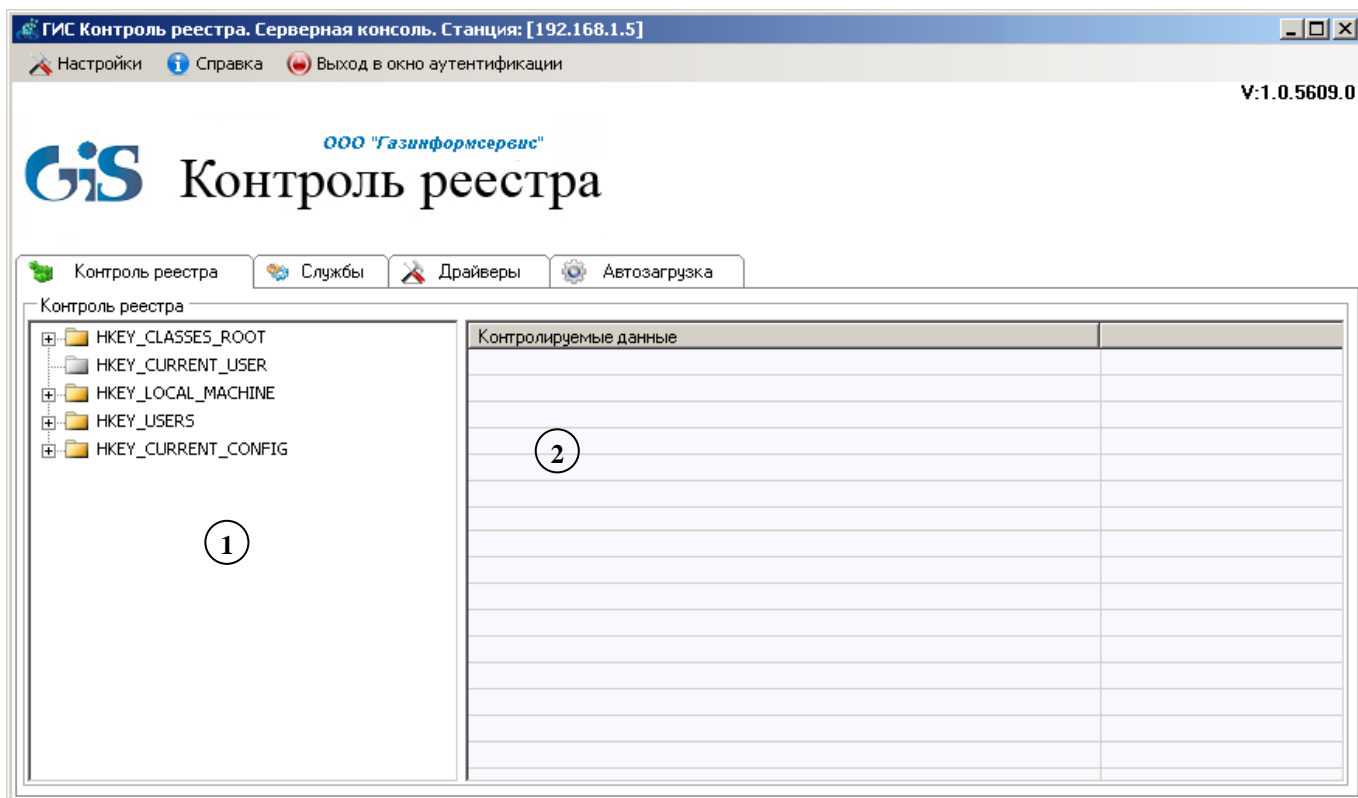


Рисунок 4.6. Серверная консоль управления модуля

Меню консоли управления содержит пункты:

- Пункт «*Настройки*» (рис. 4.7) содержит подпункты «*Настройки Syslog*» и «*Выход*»:

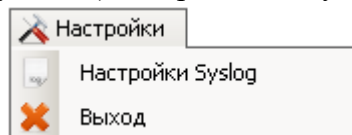


Рисунок 4.7. Вид пункта «Настройки»

При выборе подпункта «*Настройки Syslog*» появляется окно (рис. 4.8), в котором можно указать настройки Syslog-сервера для отправки сообщений об обнаруженных нарушениях целостности контролируемых объектов реестра.

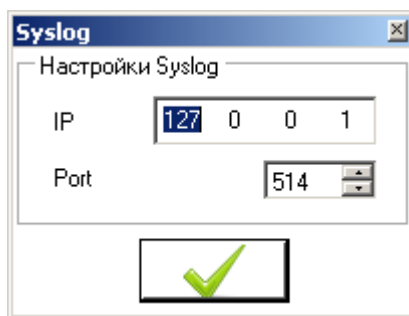


Рисунок 4.8. Настройки Syslog-сервера

- Пункт «*Справка*» позволяет получить справочную информацию о программе;
- Пункт «*Выход в окно аутентификации*» предназначен для выхода в окно аутентификации (рис. 4.4).

Серверная консоль управления содержит следующие вкладки:

- Вкладка «*Контроль реестра*» позволяет формировать перечень контролируемых объектов (разделов, параметров и значений параметров реестра Windows) удаленной рабочей станции;
- Вкладка «*Службы*» позволяет включать/выключать автозапуск системных служб удаленной рабочей станции через соответствующие ключи реестра;
- Вкладка «*Драйверы*» позволяет включать/выключать автозагрузку драйверов удаленной рабочей станции через соответствующие ключи реестра;
- Вкладка «*Автозагрузка*» позволяет редактировать список автозагрузки программ локальной/удаленной рабочей станции через соответствующие ключи реестра.

4.2.2.1 Контроль целостности реестра удаленной рабочей станции

Вкладка «Контроль реестра» позволяет осуществлять контроль целостности реестра удаленной рабочей станции и состоит из 2 областей (рис. 4.6):

- 1 – Область отображения дерева реестра локальной рабочей станции;
- 2 – Область контролируемых данных.

Для постановки на контроль объектов реестра необходимо выбрать их в дереве реестра и перетащить в область контролируемых данных:

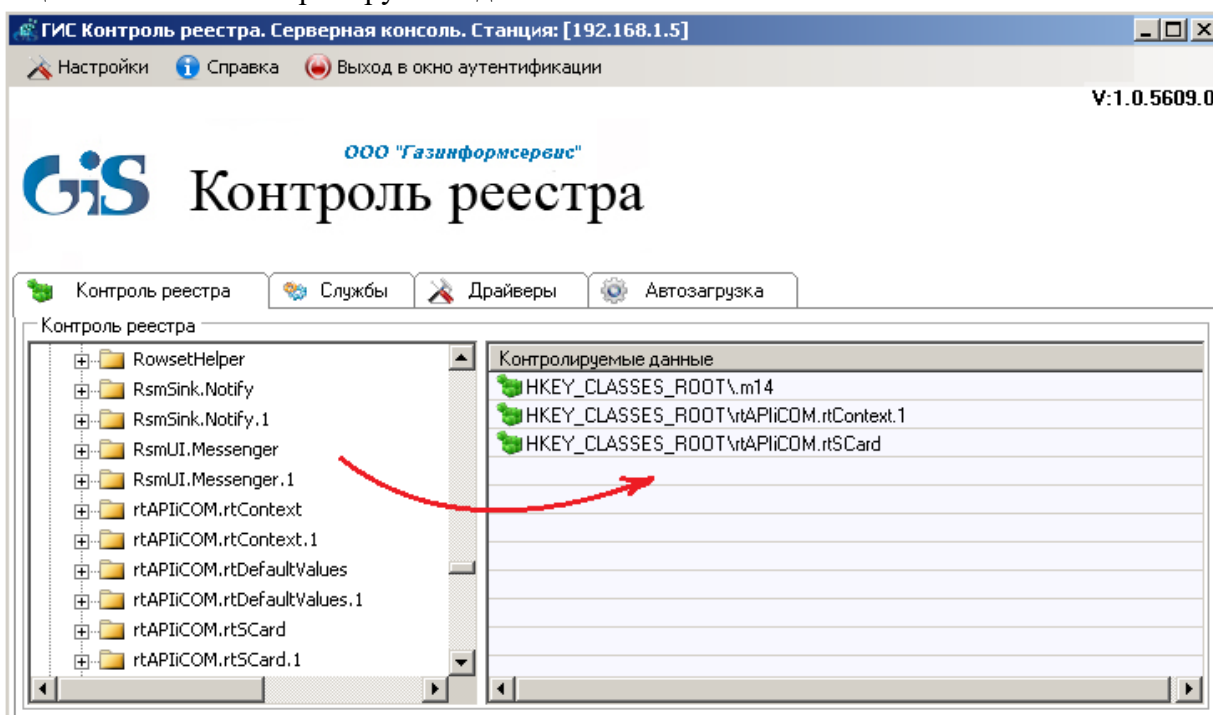


Рисунок 4.9. Серверный вариант консоли управления

После добавления объектов реестра на контроль над ними доступны следующие действия (рис. 4.10):

- *Удалить* – удаление из области контролируемых данных;
- *Обновить* – сохранение изменений в контролируемом разделе в качестве эталона;
- *Восстановить* – восстановление целостности нарушенных объектов;
- *Экспорт настроек* (сохранение настроек контроля целостности в текстовый файл).

Сохраненные настройки могут быть в дальнейшем импортированы в область контролируемых данных консоли управления модуля.

- **Импорт настроек** (импорт сохраненных в текстовом файле настроек в область контролируемых данных).

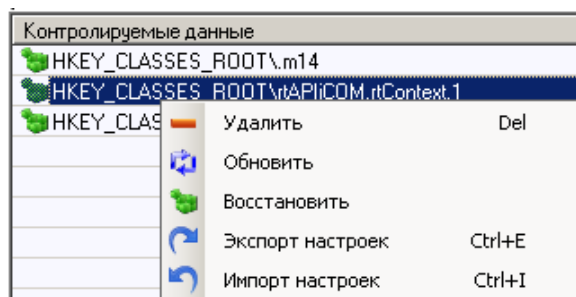


Рисунок 4.10. Контекстное меню

4.2.2.2 Управление службами удаленной рабочей станции

Вкладка «Службы» отображает список служб удаленной рабочей станции (рис. 4.11). Напротив служб, запускаемых при загрузке ОС, установлен указатель ☒. Контекстное меню, вызываемое по щелчку правой кнопкой мыши на службе, позволяет включать/отключать автозапуск служб при загрузке ОС. Для этого нужно воспользоваться пунктами контекстного меню «Включить» или «Выключить».

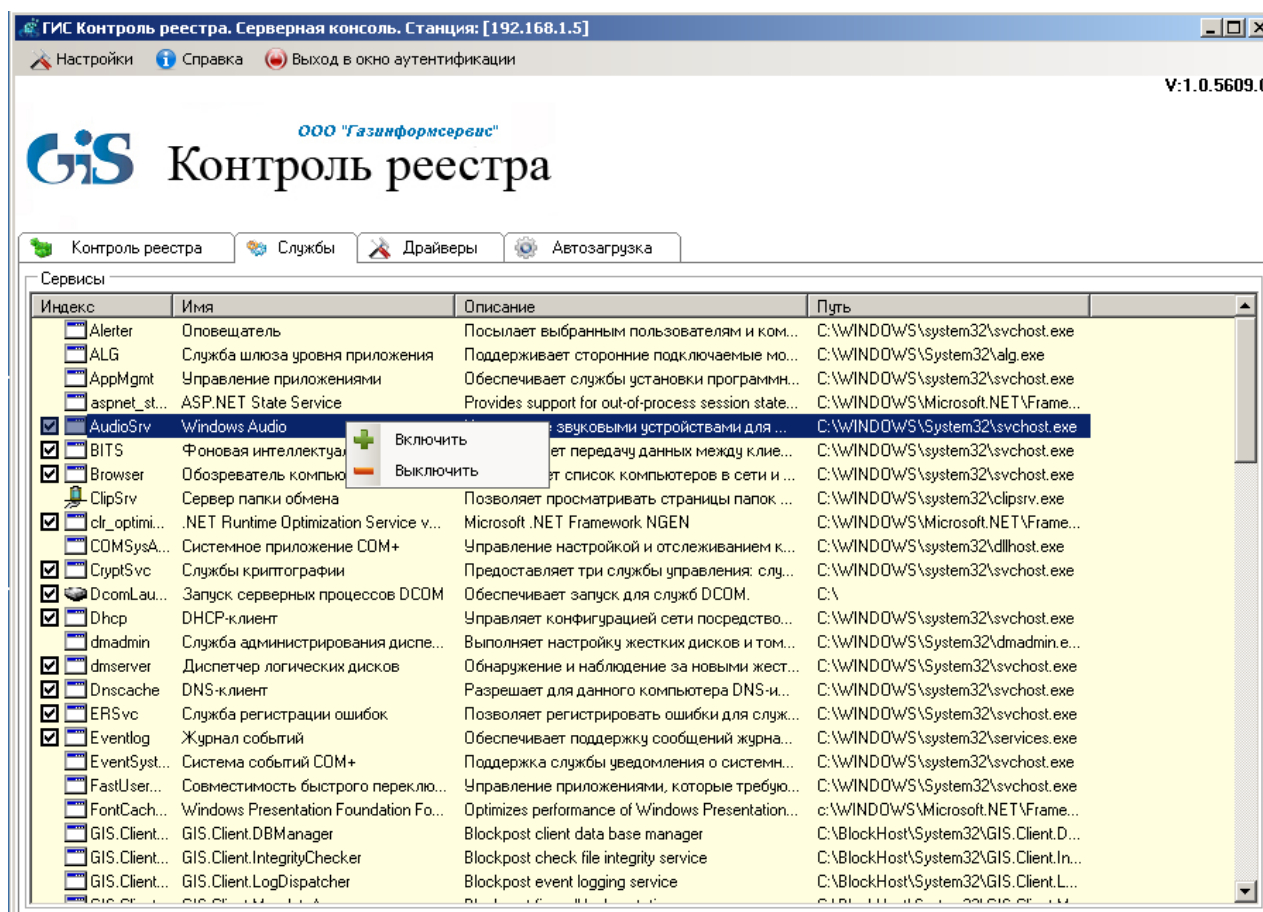


Рисунок 4.11. Вкладка служб удаленной рабочей станции

При выборе пункта «Включить» или «Выключить» появится сообщение, приведенное на рис. 4.12. При нажатии кнопки подтверждения автозапуск службы будет включен/отключен. В соответствующие ключи реестра Windows при этом будут внесены изменения. Применение настроек автозапуска системных служб произойдет при последующей загрузке ОС.

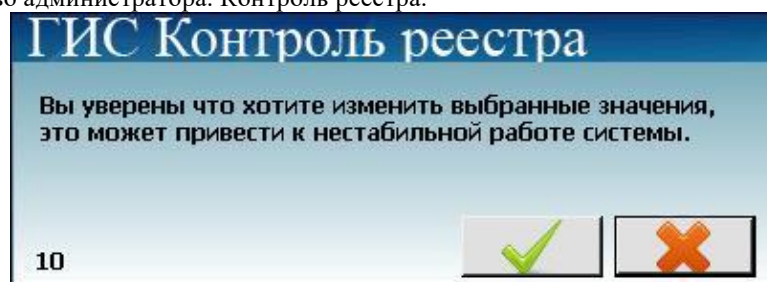


Рисунок 4.12. Подтверждения произведенных изменений

4.2.2.3 Управление драйверами удаленной рабочей станции

Вкладка «Драйверы» отображает список драйверов удаленной рабочей станции (рис. 4.13). Напротив драйверов, загружаемых при загрузке ОС, установлен указатель ☒. Контекстное меню, вызываемое по щелчку правой кнопкой мыши на драйвере, позволяет через соответствующие ключи реестра включать и отключать автозагрузку соответствующего драйвера.

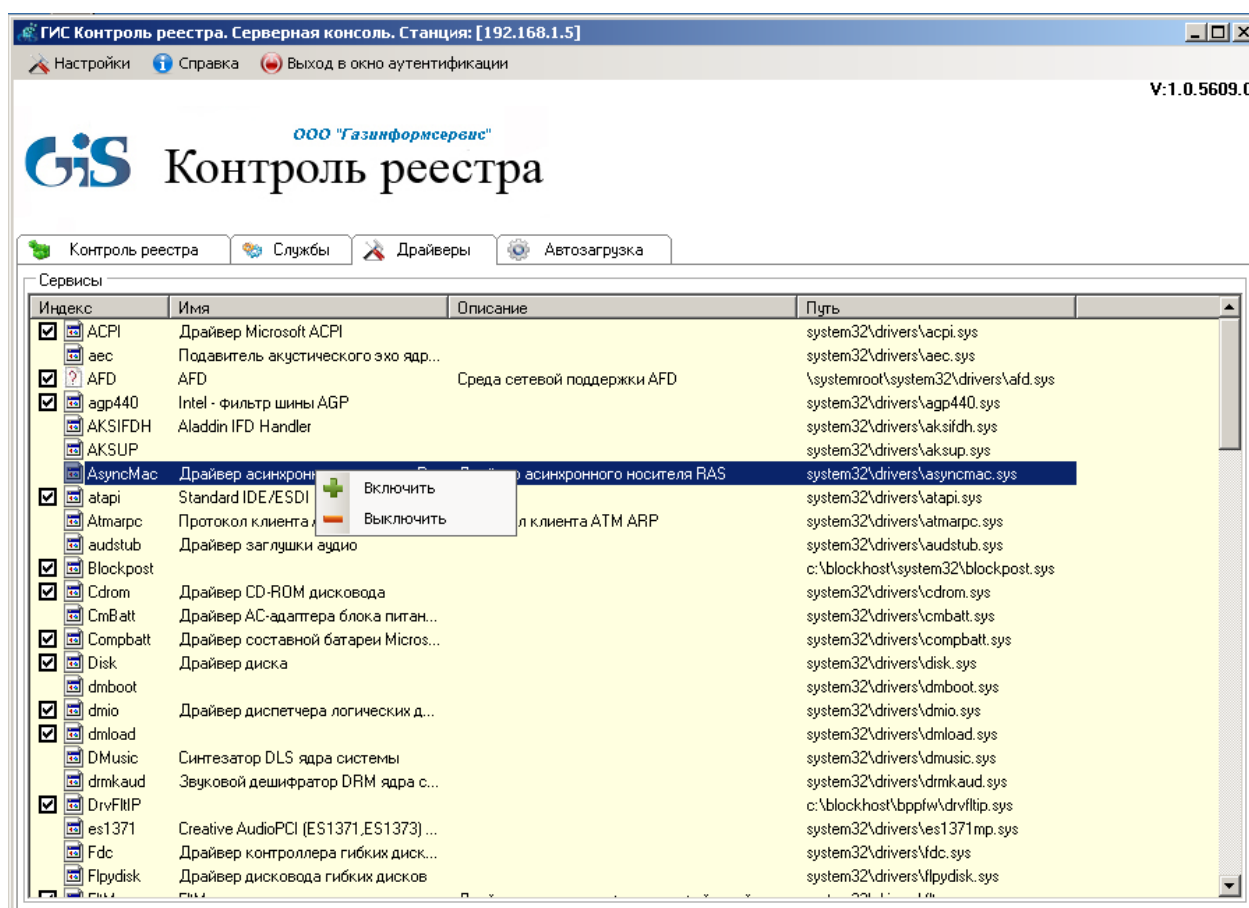


Рисунок 4.13. Вкладка драйверов удаленной рабочей станции

При выборе пункта «Включить» или «Выключить» контекстного меню появится сообщение, приведенное на рис. 4.14. После нажатии кнопки подтверждения автозагрузка драйвера будет включена/отключена, при этом в соответствующие ключи реестра Windows будут внесены изменения. Применение настроек автозагрузки драйверов произойдет при последующей загрузке ОС.

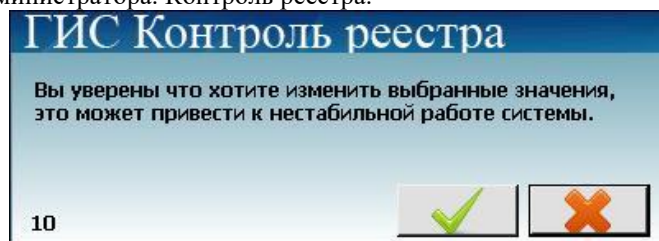


Рисунок 4.14. Подтверждения произведенных изменений

4.2.2.4 Управление списком автозагрузки программ удаленной рабочей станции

Вкладка «Автозагрузка» отображает список автозагрузки программ удаленной рабочей станции:

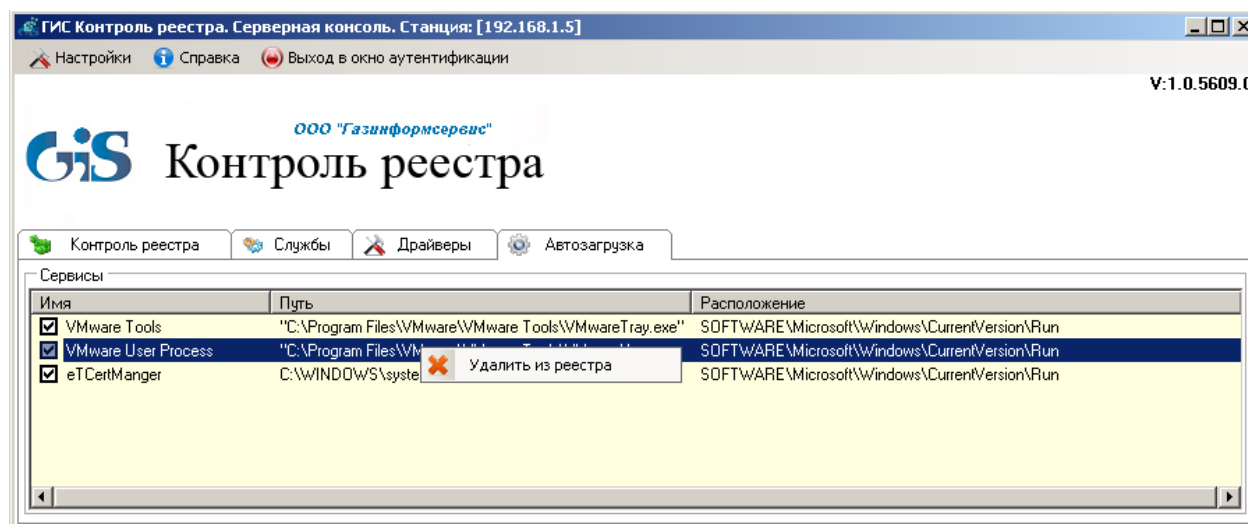


Рисунок 4.15. Вкладка «Автозагрузка»

Контекстное меню, вызываемое по щелчку правой кнопкой мыши на программе в списке автозагрузки, позволяет удалять соответствующие ей записи из реестра.

4.2.3 Редактор политик

Для формирования политик контроля целостности реестра рабочих станций в сети в окне аутентификации необходимо выбрать пункт «Редактор политик», ввести пароль и нажать кнопку подтверждения (рис. 4.16). По умолчанию для редактора политик установлен пароль «0987654321».

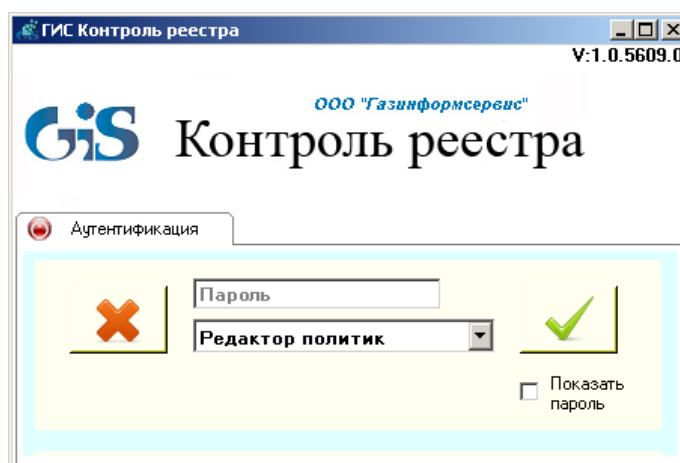


Рисунок 4.16. Редактор политик

После успешной аутентификации появится **консоль редактора политик** (рис. 4.17), которая состоит из 4 областей:

- 1 – Область IP-адресов контролируемых рабочих станций;
- 2 – Область контролируемых данных;
- 3 – Область отчета;
- 4 – Область ручного добавления контролируемых данных.

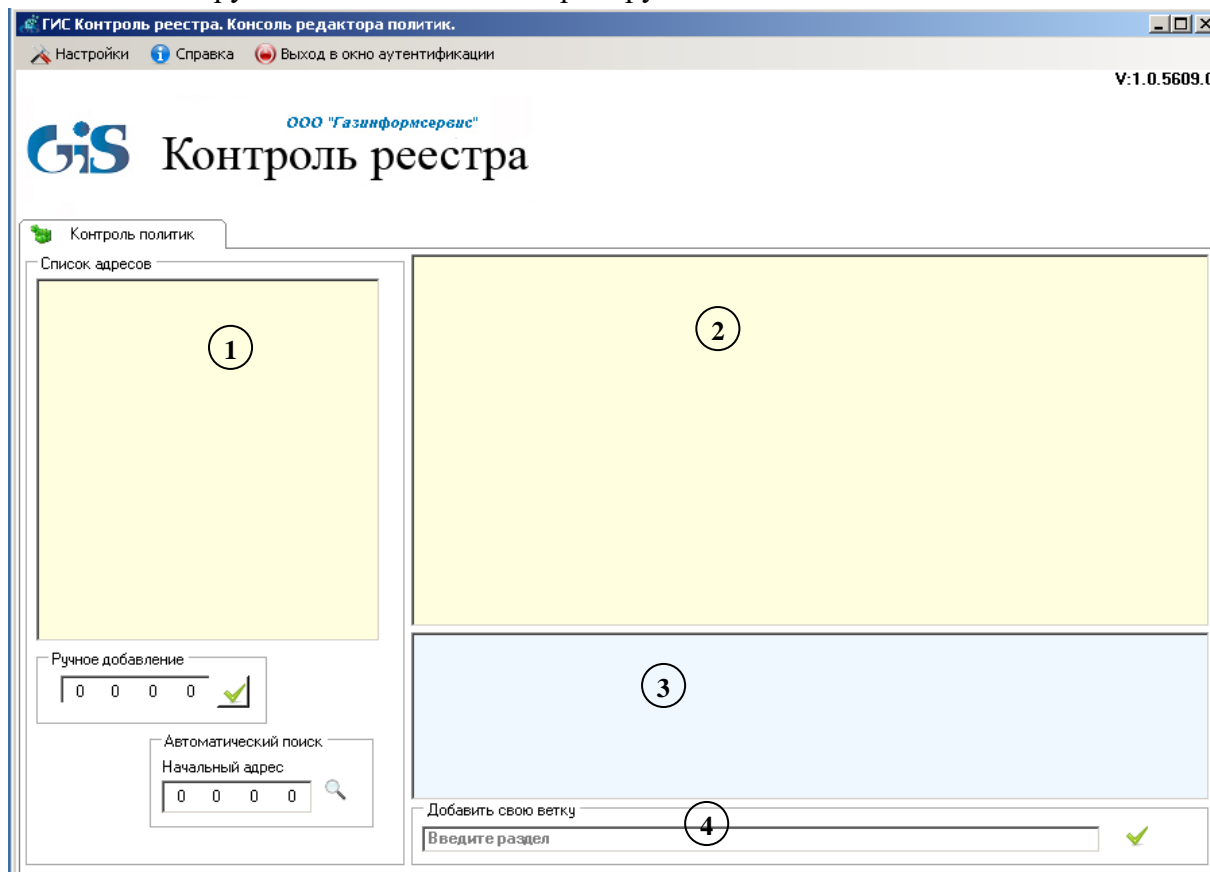


Рисунок 4.17. Редактор политик

Консоль управления редактора политик позволяет:

- формировать перечень рабочих станций, реестр которых будет контролироваться;
- формировать список контролируемых объектов реестра;
- формировать политики контроля целостности реестра выбранных рабочих станций.

4.2.3.1 Формирование перечня контролируемых рабочих станций

Область № 1 содержит IP-адреса набранных ранее рабочих станций. Для добавления новых адресов в список можно использовать «Ручное добавление» (ввод адреса вручную) или «Автоматический поиск» (поиск адресов по заданному начальному адресу).

По щелчку правой кнопкой мыши на адресе рабочей станции появляется контекстное меню, показанное на рисунке (рис. 4.18).

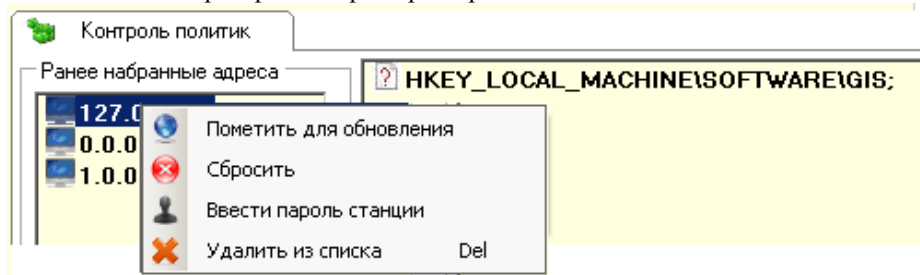


Рисунок 4.18. Контекстное меню выбранной рабочей станции

4.2.3.2 Формирование списка контролируемых объектов реестра

Для того, чтобы сформировать список контролируемых объектов реестра, необходимо добавить объект реестра (раздел/параметр/значение параметра реестра) в консоль редактора политик. Это можно сделать двумя способами:

- *Импорт объектов реестра из файла.* Для этого необходимо щелкнуть правой кнопкой мыши в области контролируемых данных (область № 2) и в появившемся меню выбрать пункт «Импорт»:

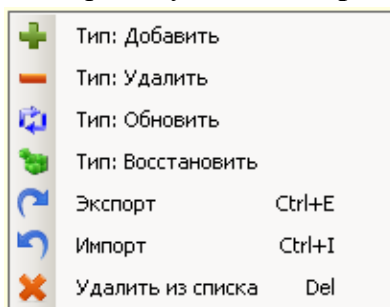


Рисунок 4.19. Контекстное меню консоли редактора политик

- *Ручное добавление объектов реестра.* Для этого необходимо в области № 4 ввести наименование контролируемого раздела/параметра/значения параметра реестра и нажать на кнопку подтверждения ✓.

Добавленные объекты реестра отображаются в консоли управления со значком :

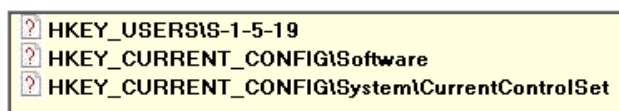


Рисунок 4.20. Добавленные объекты реестра

Для сохранения добавленных объектов реестра в текстовый файл нужно выделить объекты и выбрать в контекстном меню пункт «Экспорт» (рис. 4.19), вследствие чего будет сохранен файл со списком выбранных объектов.

Для удаления объектов реестра из списка в контекстном меню необходимо выбрать пункт «Удалить из списка» (рис. 4.19).

Если по добавленному в список объекту (рис. 4.20) еще раз щелкнуть левой кнопкой мыши, появится возможность отредактировать его вручную.

4.2.3.3 Создание политик контроля целостности объектов реестра

Для создания политик контроля целостности объектов реестра необходимо:

- 1) *Отметить рабочие станции, к которым будет применена политика контроля.* Для этого в консоли редактора политик необходимо вызвать контекстное меню рабочей

станции и в нем выбрать пункт «Пометить для обновления»:

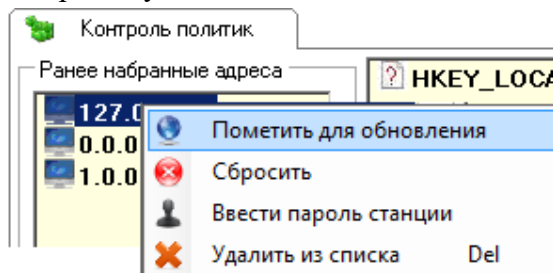


Рисунок 4.21. Пункт «Пометить для обновления»

Выбранная станция будет отмечена значком . Для того, чтобы отменить выбор, необходимо выбрать в контекстном меню пункт «Сбросить».

- 2) Выполнить аутентификацию на отмеченных рабочих станциях, для чего в контекстном меню (рис. 4.21) необходимо выбрать пункт «Ввести пароль станции» и в появившемся окне (рис. 4.22) ввести пароль удаленной рабочей станции.



Вводимый пароль должен совпадать с паролем сетевой аутентификации на удаленной рабочей станции, в противном случае применение политики контроля целостности реестра к данной станции будет невозможно.

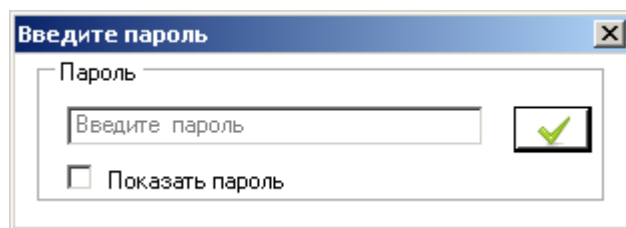


Рисунок 4.22. Окно аутентификации на удаленной рабочей станции

- 3) Применить политики контроля к рабочим станциям.

Сначала в списке добавленных объектов реестра необходимо отметить объекты реестра, которые должны контролироваться на рабочих станциях. Для этого надо щелкнуть по объекту правой кнопкой мыши и выбрать в контекстном меню пункт «Тип: Добавить» (рис. 4.23).

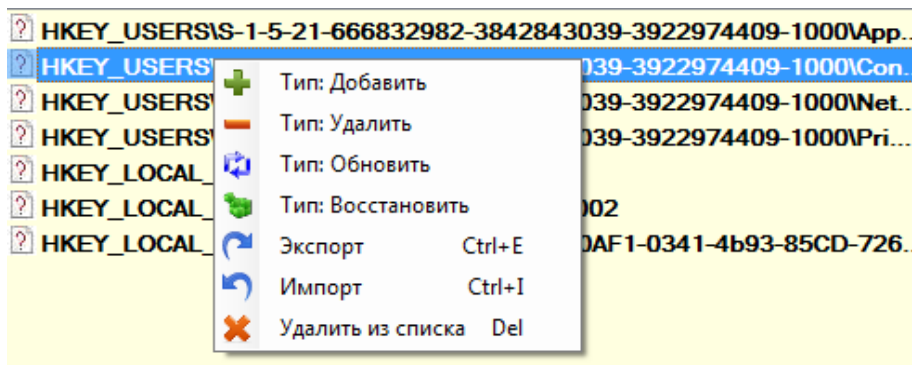


Рисунок 4.23. Контекстное меню добавленных объектов реестра

Объект реестра будет отмечен знаком плюс «». После этого надо перетащить объект реестра (или сразу несколько объектов) на отмеченную для обновления рабочую станцию (рис. 4.24) и подтвердить применение выбранных политик контроля целостности реестра к отмеченным рабочим станциям (рис. 4.25). Если перетащить объект реестра в пустую область поля «Список адресов», то его целостность будет контролироваться на всех отмеченных для обновления рабочих станциях.

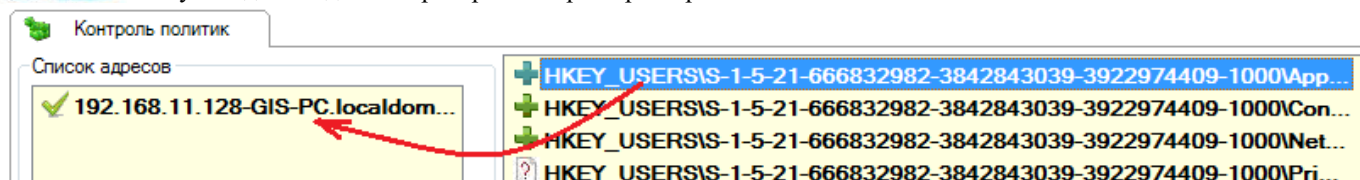


Рисунок 4.24. Применение выбранных политик контроля к отмеченным рабочим станциям

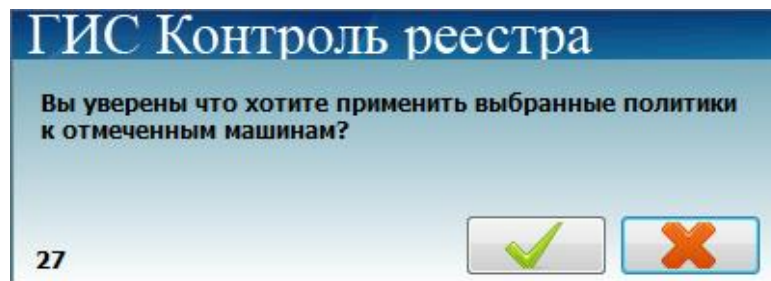


Рисунок 4.25. Подтверждение применение политики контроля

После применения политик в области отчета появится сообщение об успешном добавлении политик контроля целостности (рис. 4.26). Для очистки поля отчета необходимо щелкнуть правой кнопкой мыши по записи и выбрать пункт «Очистить».

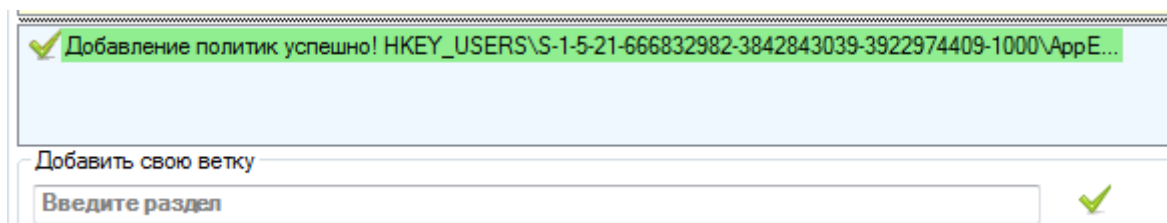


Рисунок 4.26. Сообщение об успешном добавлении политик контроля целостности реестра

Для отмены уже действующих на одной или нескольких рабочих станциях политик контроля необходимо щелкнуть по объекту правой кнопкой мыши и выбрать в контекстном меню пункт «Тип: Удалить» (рис. 4.27), при этом объект реестра будет отмечен знаком минус «-».

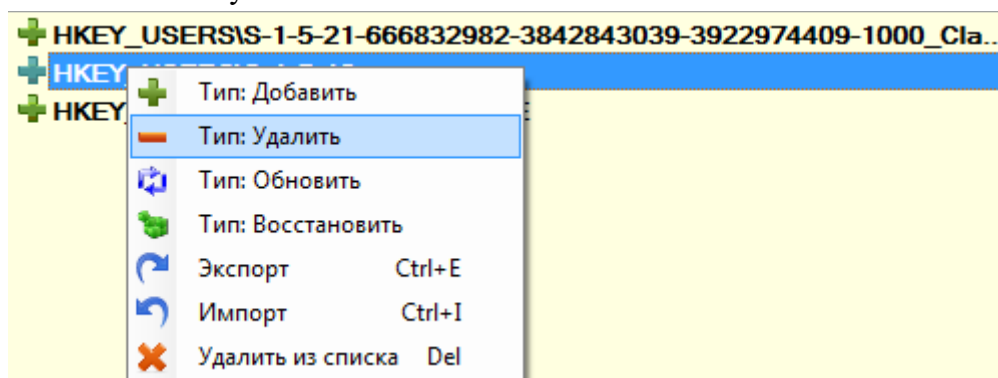


Рисунок 4.27. Пункт «Тип: Удалить» контекстного меню

После перетаскивания отмеченной знаком минус политики контроля на рабочую станцию эта политика контроля будет отменена, а в области отчета появится соответствующее сообщение:

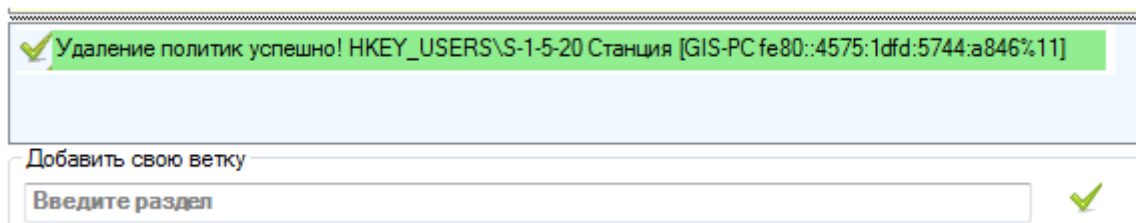


Рисунок 4.28. Сообщение об успешном удалении политик контроля целостности реестра

4.2.3.4 Сохранение изменений и/или восстановление целостности объектов реестра

При нарушении целостности объекта реестра возможно:

- *сохранить измененный объект реестра (принять его за эталон)*, щелкнув по объекту правой кнопкой мыши и выбрав в контекстном меню пункт «Тип: Обновить» (рис. 4.29);
- *восстановить целостность нарушенного объекта*, выбрав в контекстном меню пункт «Тип: Восстановить» (рис. 4.29).

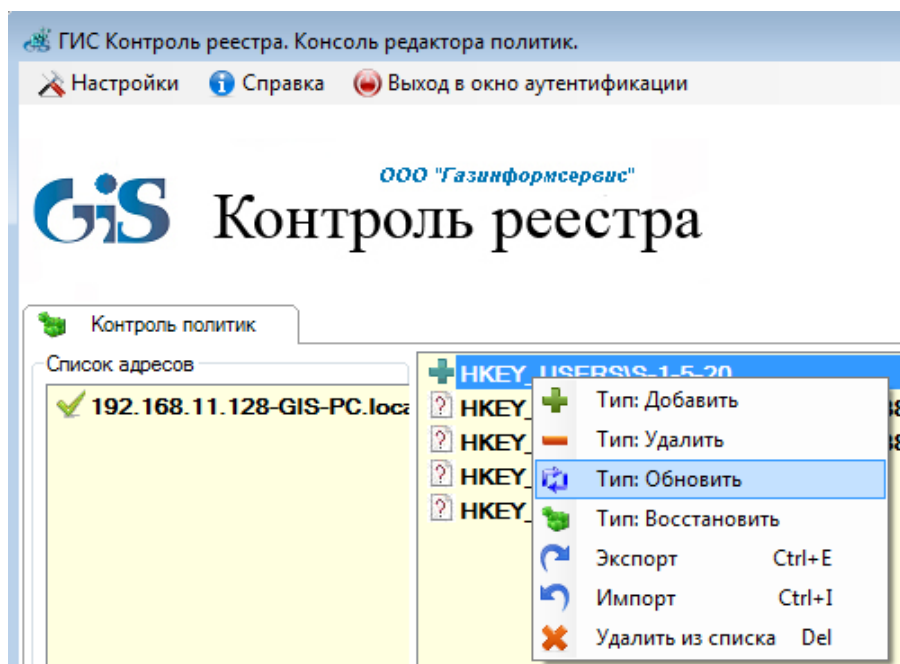


Рисунок 4.29. Сохранение изменений и/или восстановление целостности объектов реестра

5 Отображение и фиксация нарушений

5.1 Отображение нарушений

Отображение нарушений целостности объектов реестра происходит в области уведомлений:

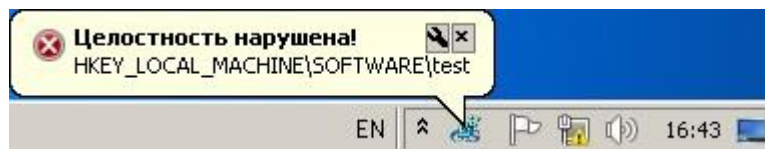


Рисунок 5.1. Сообщение о нарушении целостности реестра

5.2 Фиксация нарушений

Фиксация событий, связанных с нарушением целостности контролируемых объектов реестра, происходит в системном журнале Windows (*Управление компьютером → Служебные программы → Просмотр событий → Блокхост-сеть*).