Иван Андреевич Трещев

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЧАСТЬ ВТОРАЯ

для студентов технических специальностей

Иван Трещев

Программно-аппаратные средства обеспечения информационной безопасности. Часть вторая. Для студентов технических специальностей

«Издательские решения»

Трещев И. А.

Программно-аппаратные средства обеспечения информационной безопасности. Часть вторая. Для студентов технических специальностей / И. А. Трещев — «Издательские решения»,

ISBN 978-5-44-963210-4

В данной книге рассматриваются современные средства для обеспечения защиты от несанкционированного доступа к информации, приведены примеры настройки средств защиты для определенных классов автоматизированных систем.

ISBN 978-5-44-963210-4

Содержание

Программно-аппаратные средства обеспечения информационной безопасности. Часть вторая Для студентов технических специальностей

Иван Андреевич Трещев

Работа с программным обеспечением Анастасия Сергеевна Ватолина

ISBN 978-5-4496-3210-4 (т. 2)
ISBN 978-5-4496-3211-1
Создано в интеллектуальной издательской системе Ridero

Введение

Современные средства защиты от несанкционированного доступа предоставляют широкий спектр всевозможных настроек, но зачастую производители не уделяют должного внимания настройкам среды для конкретного класса государственной информационной системы, информационной системы персональных данных, автоматизированной системы.

В данной книге автор постарался сконцентрироваться на проблемах настройки средств защиты информации от несанкционированного доступа для конкретных классов объектов информатизации.

Так же в книге сделан акцент на использование средств создания и анализа моделей разграничения доступа, средств фиксации исходного состояния программных комплексов.

В настоящей книге автор в основном рассматривает продукты компании ЦБИ-Инфо и Код Безопасности, но уделяется внимание части продуктов компании Конфидент и Positive Tecnologies.

Средство сбора информации о программном и аппаратном обеспечении «Агент инвентаризации»

Назначение

Программное средство Агент инвентаризации предназначено для автоматизированного сбора информации об аппаратном и программном обеспечении АРМ и серверов, функционирующих под управлением операционных систем Windows 95, 98, Me, NT 4, 2000, XP и Server 2003.

Программа может запускаться автономно на отдельных АРМ или серверах или в составе других программных средств. В первом случае использование программы осуществляется через интуитивно понятный графический интерфейс. Во втором случае программа может быть запущена в режиме командной строки с широким набором параметров.

Полученная информация о составе программных и аппаратных средств, их свойствах, характеристиках и настройках в структурированном виде сохраняется в виде текстового файла, пригодного для дальнейшей обработки, а также может быть представлена в виде структурированного отчета в HTML-формате.

Имеется положительный опыт использования программного продукта в целях осуществления на регулярной основе процесса автоматизированной инвентаризации настроек АРМ и серверов крупных корпоративных сетей с сохранением актуальной информации в промышленной базе данных соответствующей информационной системы.

Программный продукт может быть также использован для автоматизированного формирования формуляров АРМ и серверов ЛВС, например, при проведении их аттестационных испытаний по требованиям безопасности информации.

Установка и настройка программы

Для установки «Агента инвентаризации» нужно скопировать файлы программы в любой каталог на жестком диске. Никаких дополнительных действий по установке не требуется.

Порядок выполнения зависит от поставленной задачи. Для запуска программы из командной строки нужно выполнить файл sysinfo. exe с указанием требуемых параметров работы. Для запуска программы с использованием графического интерфейса используется файл Agent. exe.

Выполнение с использованием графического интерфейса

Модуль графического интерфейса предназначен для упрощения взаимодействия между пользователем и основным исполняемым модулем. Основными функциями модуля графического интерфейса являются: запуск основного исполняемого модуля для сбора информации, просмотр результатов работы и генерация отчетов. Также он может быть использован для формирования командной строки запуска основного исполняемого модуля, если «Агент инвентаризации» применяется как часть программного комплекса.

Интерфейс программы

Главное окно программы имеет следующие элементы:

– Строка меню
– Панель инструментов
– Дерево объектов
– Список свойств текущего объекта
– Строка состояния

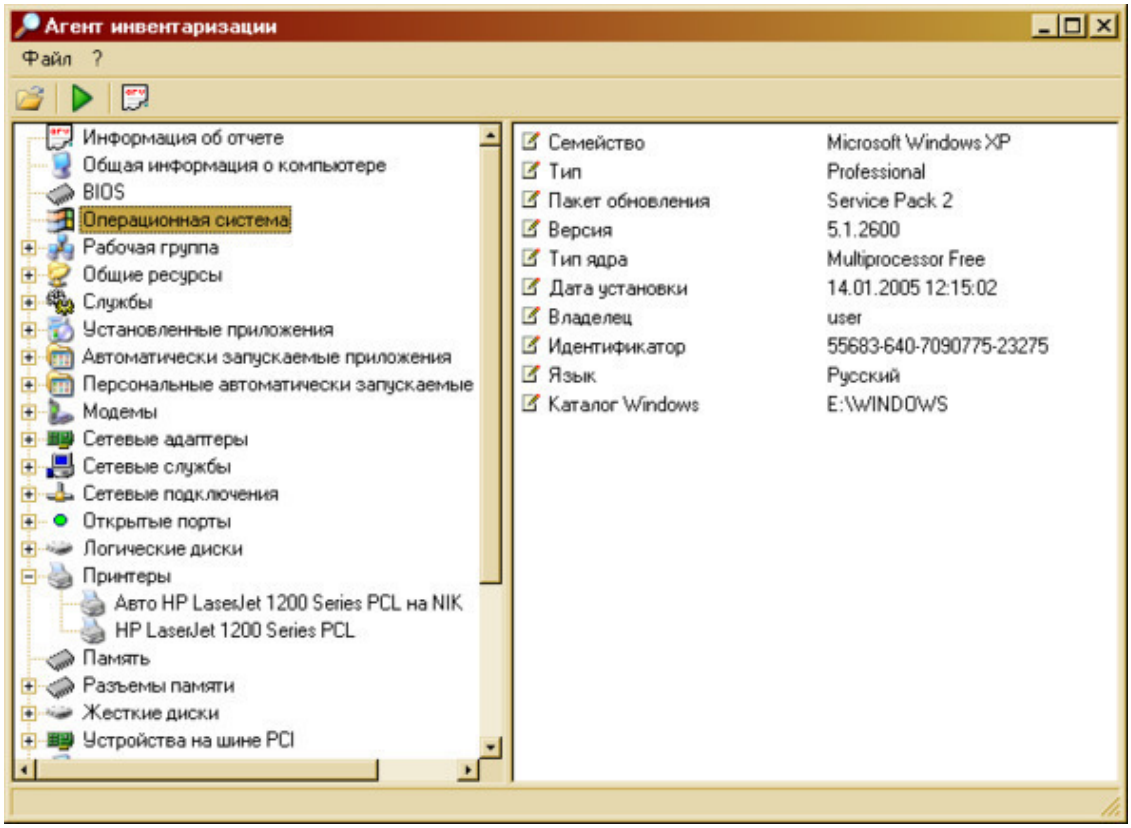


Рисунок 1 – Главное окно программы

Меню дублирует все функции, доступные с панели инструментов. На панели инструментов расположены следующие кнопки:

	Загрузка и просмотр результатов полученных при предыдущих запусках программы
	Сбор системной информации
	Создание отчета

Кнопки панели инструментов имеют всплывающие подсказки, появляющиеся при задержке курсора мыши над ними. Если команда, соответствующая кнопке, недоступна, кнопка также недоступна и отображается в сером цвете.

Вся полученная информация отображается в виде набора объектов, каждый из которых имеет собственный набор свойств. Перечень объектов отображается в дереве объектов (с разбиением по классам). Справа, в списке свойств, отображаются свойства текущего (выделенного в дереве) объекта.

Строка состояния отображает информацию о текущей выполняемой операции

Сбор информации

Для сбора информации о системе используется кнопка панели инструментов. После ее нажатия на экране появляется диалоговое окно, в котором можно за несколько шагов настроить параметры сбора информации.

Шаг 1. Настройка параметров работы программы

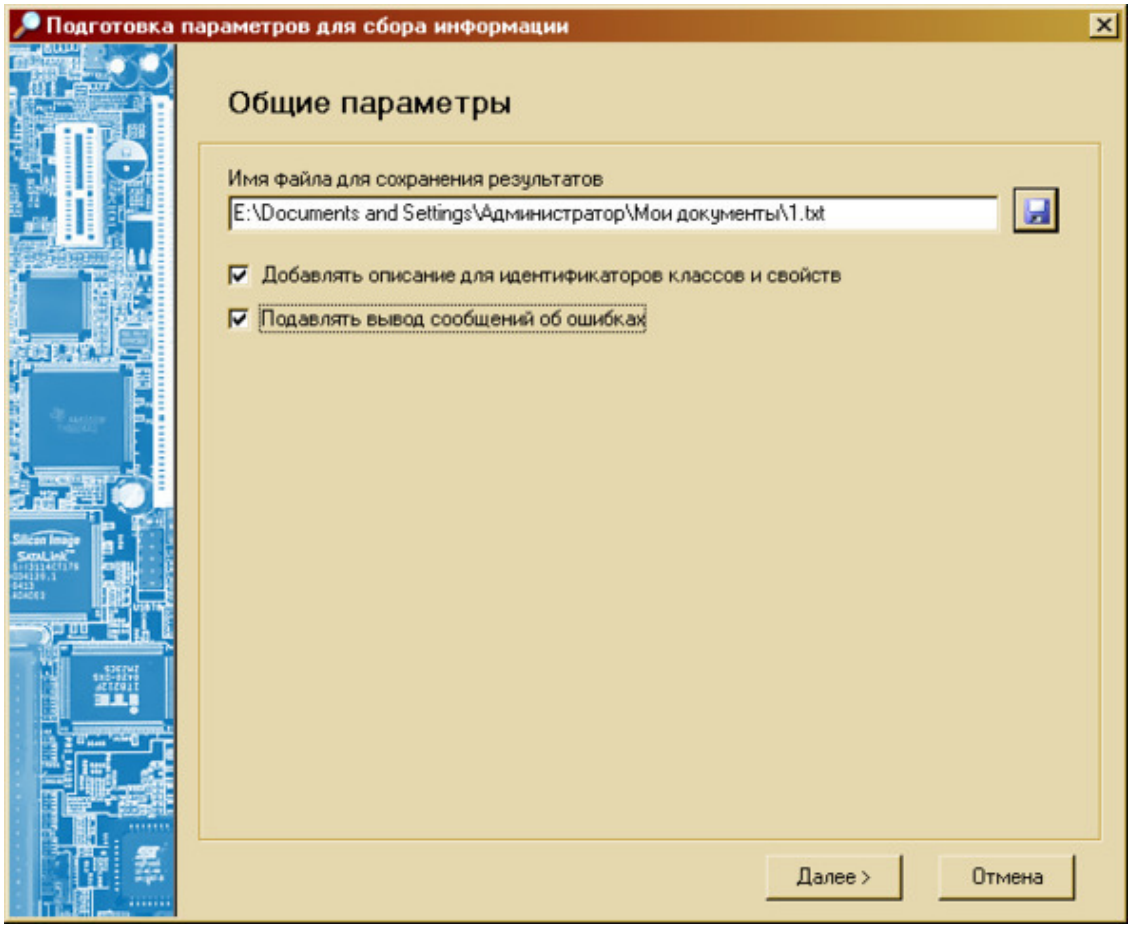


Рисунок 2- Настройка параметров работы программы

На этом шаге устанавливаются основные параметры, определяющие работу программы. Прежде всего, это имя файла для сохранения результатов (указывается с помощью кнопки). Также можно включить режимы «Добавлять описание для идентификаторов классов и свойств» (добавляет параметр /descr к строке запуска основного исполняемого модуля) и «Подавлять вывод сообщений об ошибках» (параметр /silent)

Шаг 2. Определение состава получаемой информации

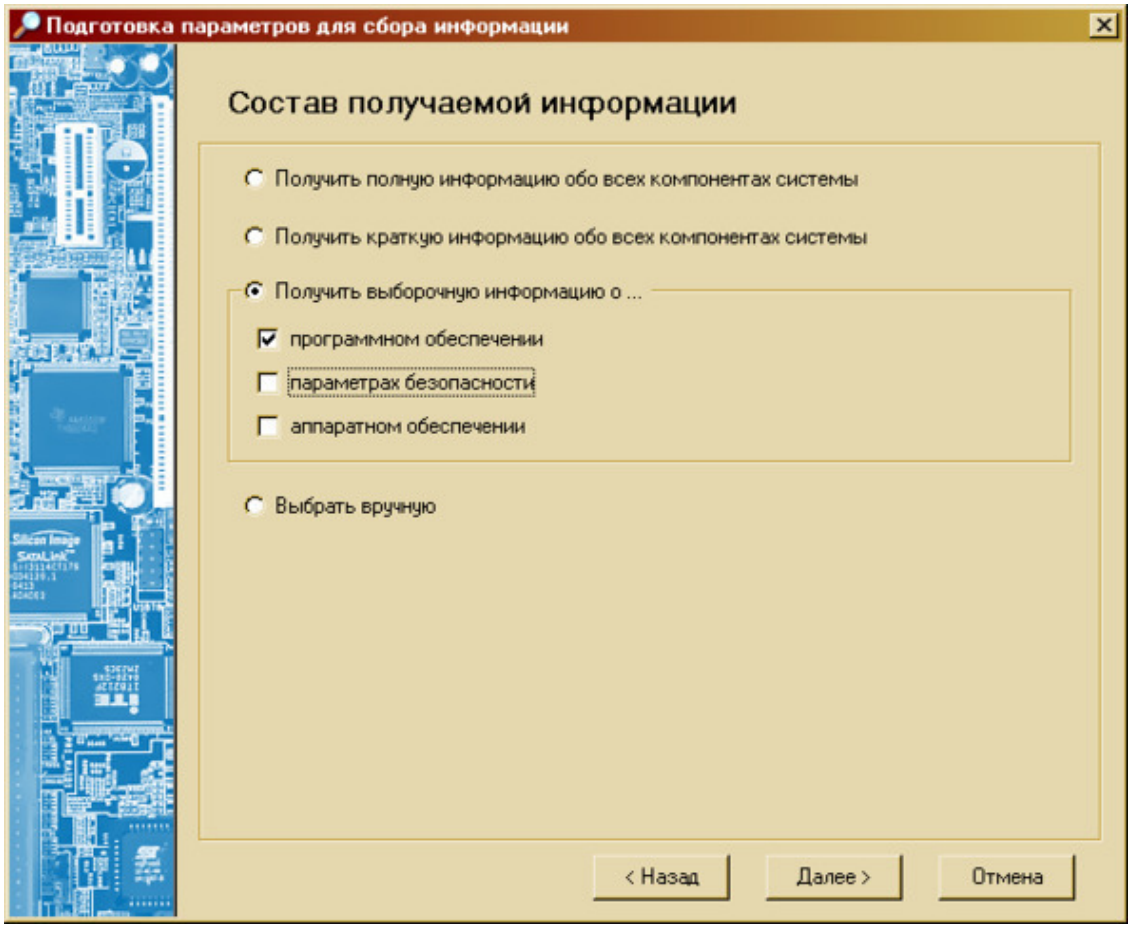


Рисунок 3 – Определение состава получаемой информации

На этом шаге определяется, какая информация должна быть получена в ходе работы программы. При этом используются групповые параметры. Если требуется детально определить состав получаемой информации, то нужно выделить вариант «Выбрать вручную».

Шаг 3. Определение состава получаемой информации (дополнительно)

Этот шаг выполняется только если был выбран вариант «Выбрать вручную» на предыдущем шаге. Пользователю предоставляется возможность более точно определить состав получаемой информации. Для удобства можно использовать функции «Выделить все» и «Снять все отметки», доступные через контекстное меню.

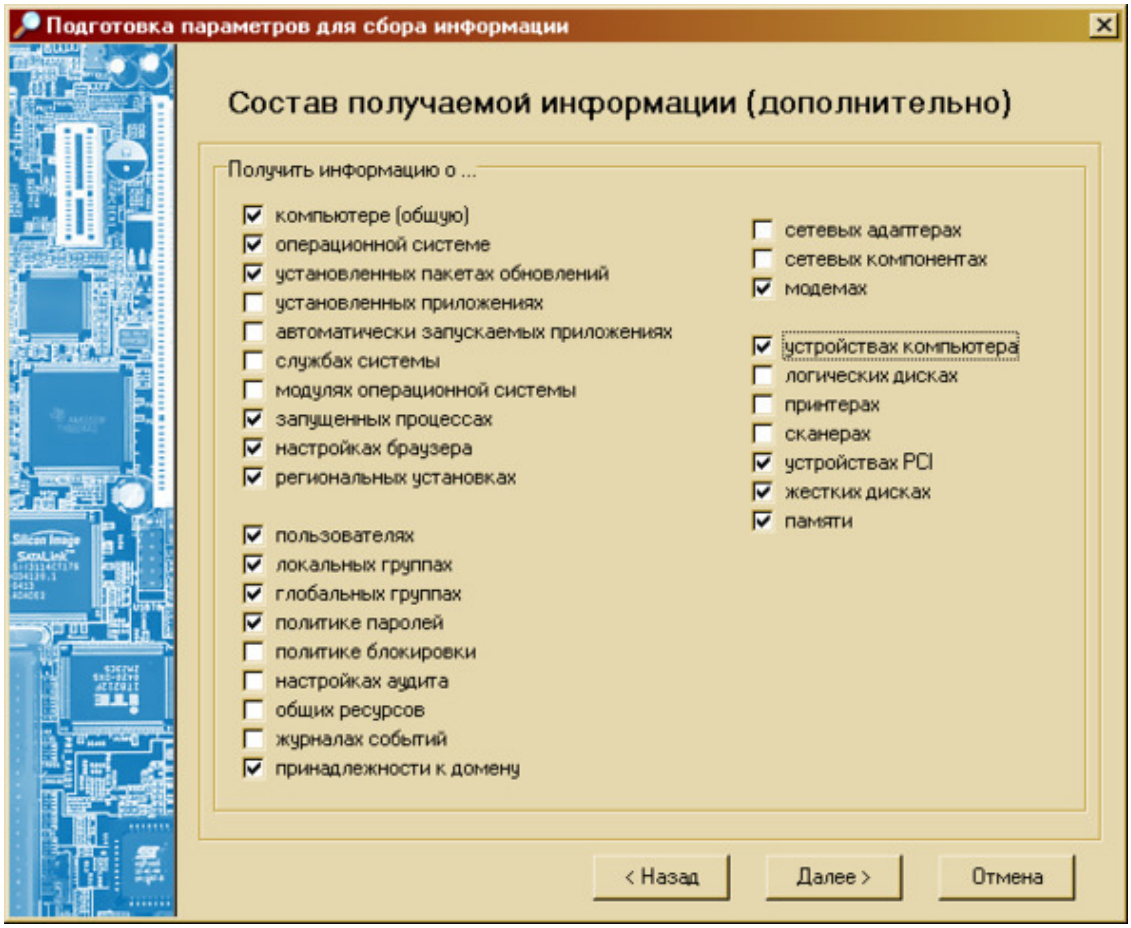


Рисунок 4 – Определение состава получаемой информации (дополнительно)

Шаг 4. Настройка параметров фильтрации журналов аудита

Этот шаг выполняется только в том случае, если в ходе работы программы должна быть получена информация из журналов аудита.

С целью сокращения объема выходных данных, в «Агенте инвентаризации» предусмотрена возможность фильтрации записей системных журналов событий.

Для добавления правила фильтрации нужно нажать кнопку «Добавить», после чего на экране появится окно настройки параметров создаваемого правила. В нем указывается, к какому из полей записи в журнале событий применяется правило, и требуемое значение поля. В дальнейшем правила фильтрации можно будет удалять и редактировать.

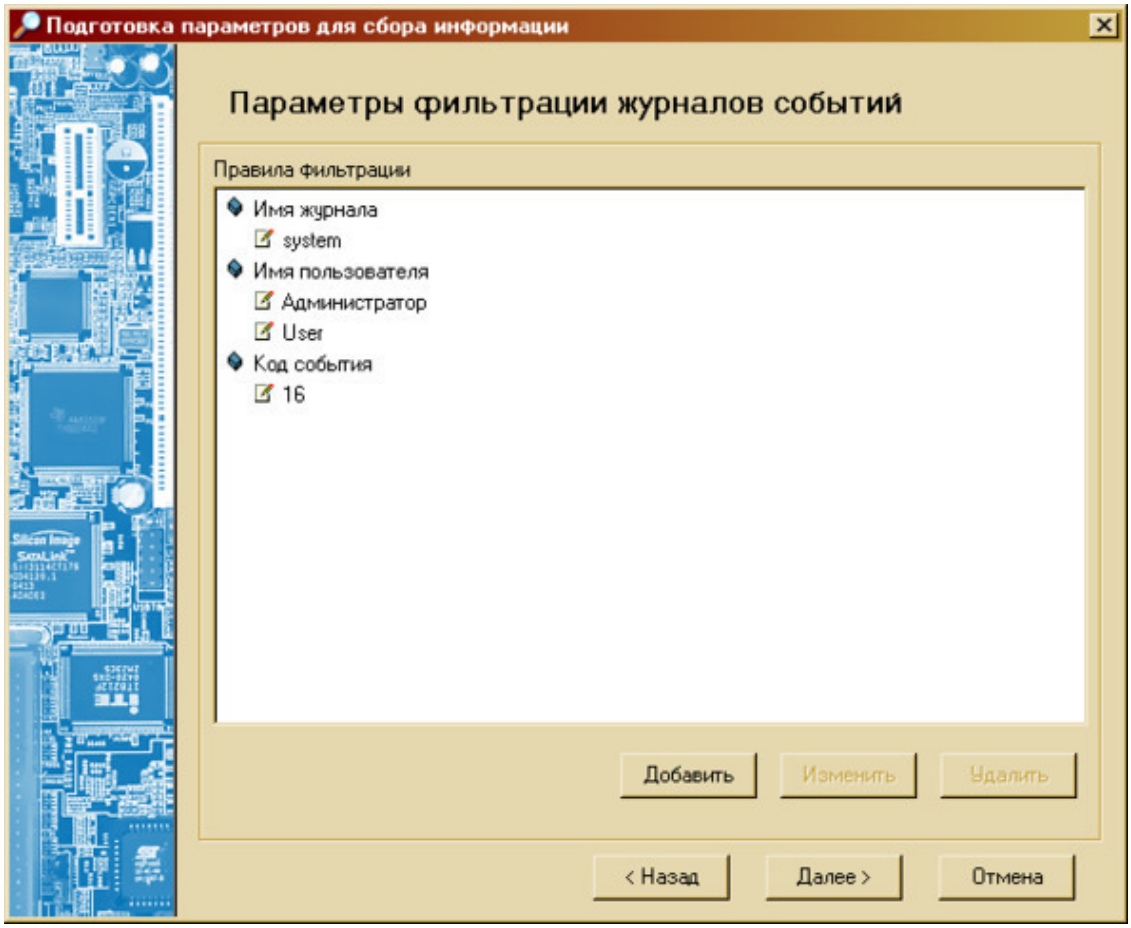


Рисунок 5 – Параметры фильтрации журналов событий.

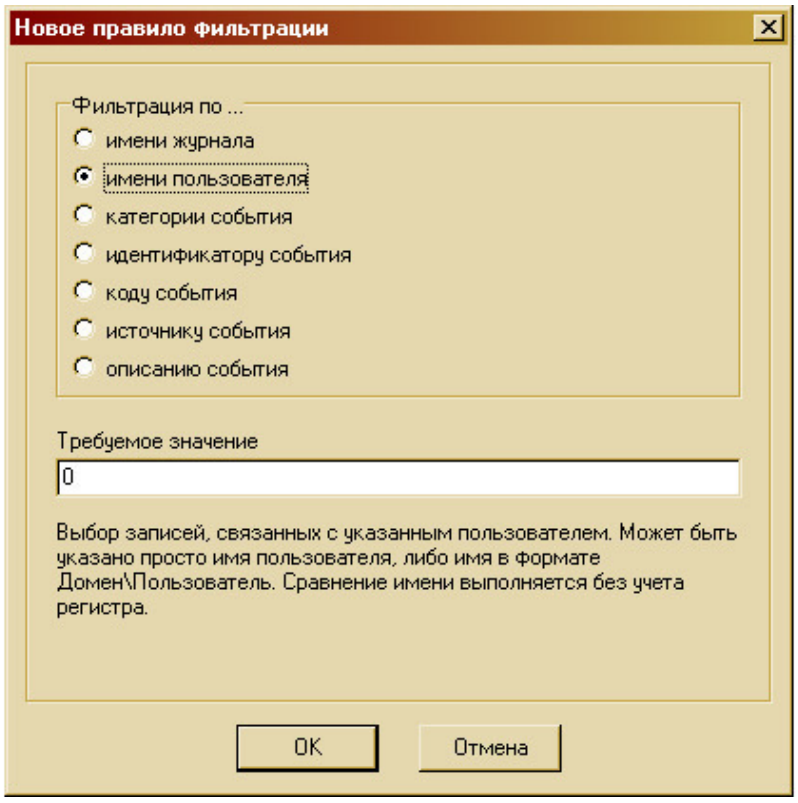


Рисунок 6 – Создание правила фильтрации журнала событий

Анализ полей «Категория», «Источник» и «Описание» проводится с помощью регулярных выражений. Это дает возможность гибко описывать требования к значению полей. В простейшем случае, если не используются управляющие символы, удовлетворяющими требованию считаются все строки, содержащие заданную подстроку. Если же требуется точное соответствие требуемому значению, то нужно указывать его в формате.

Если используются несколько условий, то они объединяются следующим образом: однотипные условия объединяются с помощью логического оператора ИЛИ, затем результаты объединения однотипных условий объединяются с помощью логического оператора И. Запись признается соответствующей требованиям, если она удовлетворяет хотя бы одному условию каждого типа.

Шаг 5. Завершение формирование параметров

На этом этапе формирование параметров уже завершено, и на экран выводится командная строка, которая будет использована при запуске основного исполняемого модуля. Эта строка может быть скопирована и использована в дальнейшем для запуска основного исполняемого модуля без использования графического интерфейса.

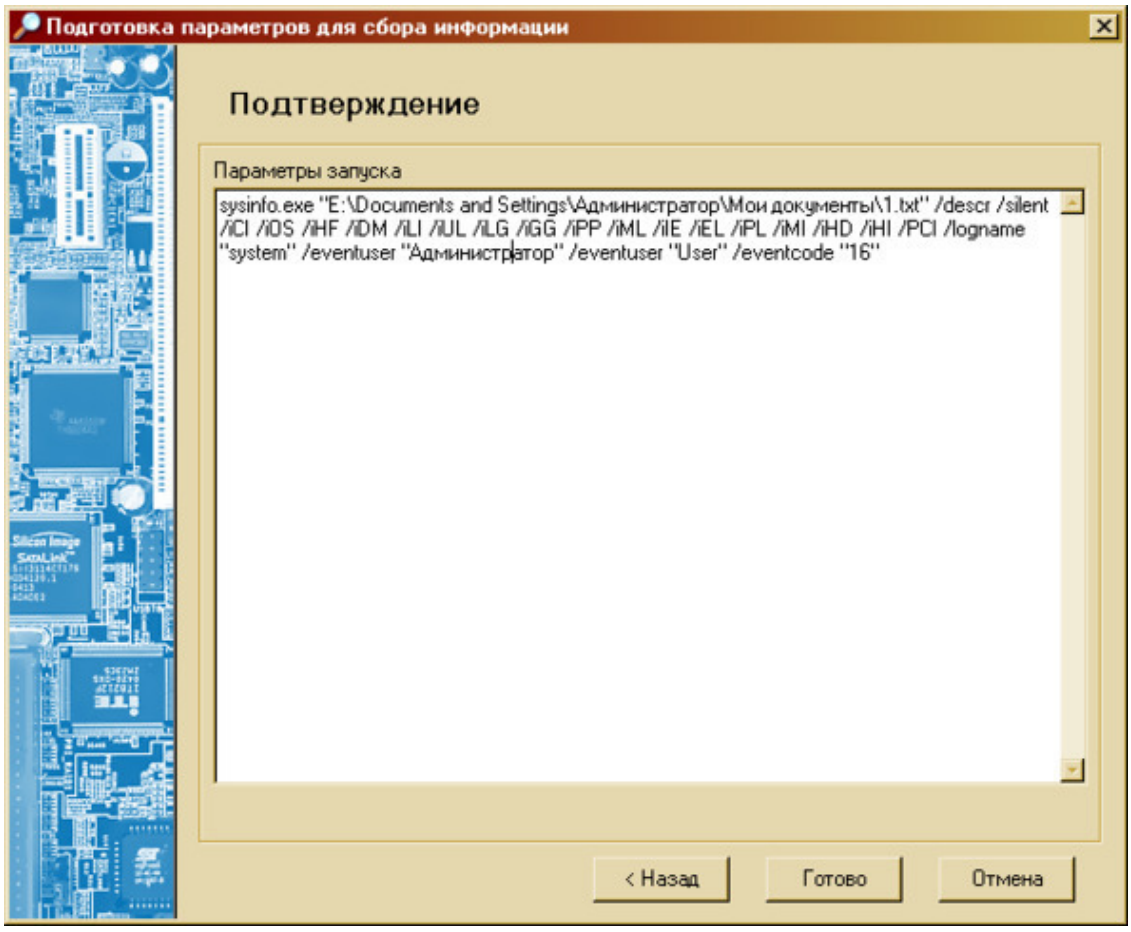
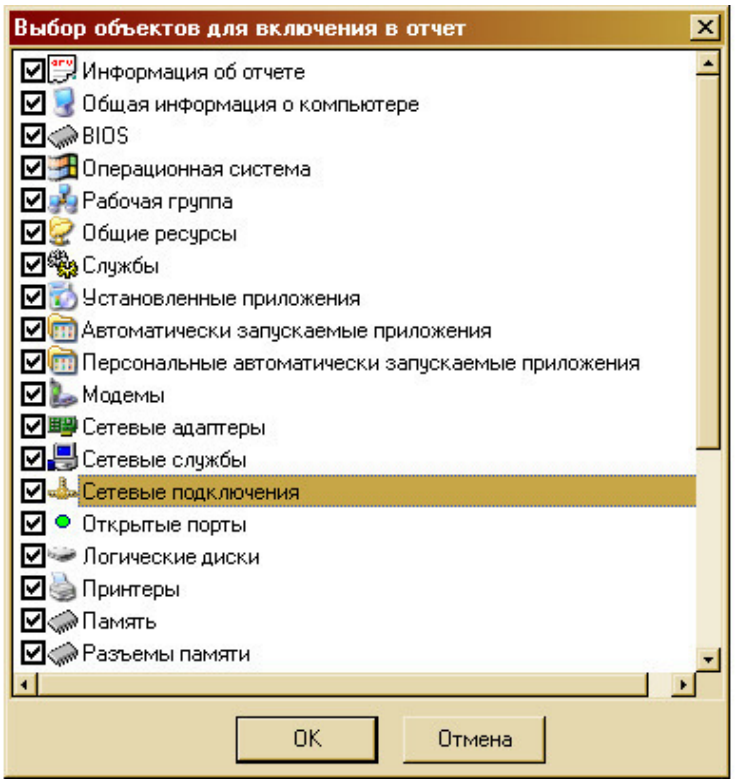


Рисунок 7 – Завершение подготовки параметров

По нажатию кнопки «Готово» выполняется запуск основного исполняемого модуля и ожидание завершения его работы. Все результаты сохраняются в файл. После завершения, результаты работы отображаются в главном окне программы.

Формирование отчетов

Создание отчета осуществляется с помощью кнопки. После нажатия этой кнопки, на экране появляется окно настройки состава формируемого отчета. Для удобства можно использовать функции «Выделить все» и «Снять все отметки», доступные через контекстное меню.



После завершения выбора и нажатия кнопки «ОК» будет запрошено имя файла для сохранения отчета, и, затем, создан отчет. Программа формирует отчет в формате HTML. Файлы в этом формате могут быть открыты любым веб-браузером (например, Internet Explorer) либо импортированы в офисные приложения, такие как Microsoft Word.

Порядок выполнения работы

Конец ознакомительного фрагмента.