УТВЕРЖДЕН
BY.ИАДВ.00138-02 31 01-ЛУ

КОМПЛЕКС VBA32 ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Защита персональных компьютеров и рабочих станций

от воздействия вредоносных программ

Описание применения
BY.ИАДВ.00138-02 31 01
Листов 75

2019

Литера

№ изм.	*Подп.*	*Дата*

Подп. и дата	
Инв. N дубл.	
Взам. инв. N	
Подп. и дата	
Инв.N подл.	

АННОТАЦИЯ

Настоящий документ содержит описание применения по использованию комплекса VBA32 программных средств защиты от воздействия вредоносных программ (далее – Комплекс).

Разработчик комплекса - ОДО «ВирусБлокАда».
220088, РБ, Минск, ул. Смоленская, 15 — 803б
телефон: (+375 17) 294-84-29 (коммерческий отдел)
телефон: (+375 17) 290-59-29 (технический отдел)
E-mail: info@anti-virus.by

Комплекс соответствует требованиям технического регламента Республики Беларусь ТР 2013/027/BY.

Комплекс устанавливается на ПК на базе архитектуры Intel x86 и требует наличия:

1) 32-разрядного (x86) или 64-разрядного (x64) процессора с тактовой частотой не ниже 2 ГГц;
2) не менее 1 ГБ оперативной памяти;
3) не менее 500 МБ свободного пространства на логическом диске ПК.

Комплекс функционирует под управлением ОС Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

Комплекс состоит из следующих модулей:

- Диспетчер Vba32;
- Сканер с графическим пользовательским интерфейсом;
- Файловый монитор с графическим пользовательским интерфейсом;
- Расширение контекстного меню «Проводника»;
- SendLogs;
- Почтовый фильтр;
- Скрипт-фильтр;
- Outlook-модуль;
- Карантин;
- Агент удаленного администрирования;
- Консольный сканер для Windows;
- Планировщик.

Диспетчер Vba32:

- осуществляет проверку целостности всех компонент Комплекса, обеспечивает автоматическое восстановление поврежденных компонент путем загрузки их с сервера локальной сети или Интернет;
- проверяет на наличие вредоносных программ оперативную память (системные области памяти и память всех процессов) и загрузочные сектора дисковых накопителей;

– выполняет автоматическое обновление антивирусных баз и всех исполнимых модулей Комплекса с сервера локальной сети или Интернет.

Сканер с графическим пользовательским интерфейсом:

– позволяет выполнять обработку выбранных объектов по запросу пользователя;
– имеет развитую систему настроек.

Файловый монитор с графическим пользовательским интерфейсом:

– обеспечивает надежную защиту рабочих станций, контролируя все функции работы с файлами в ОС;
– позволяет выполнять различные действия над инфицированными файлами, в том числе обезвреживание, «на лету».

Расширение контекстного меню «Проводника»:

– предоставляет возможность быстрой обработки объектов непосредственно из оболочки, привычной большому числу пользователей – «Проводника»;
– использует упрощенные настройки;
– позволяет обработать выбранные файлы или каталоги одним щелчком «мыши», используя ранее сохраненные настройки.

SendLogs:

– предназначена для сбора технической информации и файлов отчёта всех компонентов Vba32 с последующей их отправкой специалистам ОДО «ВирусБлокАда» либо сохранением на диск.

Почтовый фильтр Vba32:

– обрабатывает принимаемую с Интернет- или Интранет-серверов почту;
– не зависит от используемого почтового клиента;
– позволяет удалять или перемещать письма с вирусами;
– формирует сообщение об обнаружении вируса по заданному пользователем шаблону.

Скрипт-фильтр:

– осуществляет антивирусную защиту Microsoft Internet Explorer и Microsoft Outlook Express, а также любых других приложений, использующих технологию Microsoft Windows Scripting Host (MS WSH).

Outlook-модуль:

– выполняет проверку и обезвреживание почтовых сообщений перед их прочтением и отправкой с использованием Microsoft Outlook и Microsoft Exchange Client.

Карантин:

– обеспечивает хранение инфицированных и подозрительных файлов, помещенных в него антивирусными модулями Vba32.

Агент удаленного администрирования:

– Обеспечивает связь с центром управления (ЦУ) для удаленного управления.

Консольный сканер для Windows:

– позволяет выполнять обработку указанных объектов;

- позволяет управлять своими режимами с помощью параметров, вводимых в командной строке;
- позволяет использовать его в пакетном режиме.

Планировщик задач комплекса Vba32:

- позволяет запускать задачи (сторонние приложения, процесс сканирования, процесс обновления) в указанные временные ограничения на персональных компьютерах, рабочих станциях и серверах.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Комплекс предназначен для защиты рабочей станции от воздействия вредоносных программ и компьютерных вирусов.

Vba32 Диспетчер - Vba32 Диспетчер является главной контрольной панелью комплекса Vba32. Он позволяет отслеживать состояние антивирусных модулей, запускать Vba32 Сканер, а также предоставляет доступ к настройкам Vba32 Монитора.

Vba32 Монитор - обеспечивает непрерывную защиту на Вашем компьютере, как уже существующих, так и новых файлов, попадающих на Ваш компьютер из сети, с других носителей, скачиваемых из Internet или приходящих по электронной почте.

Vba32 Сканер - предоставляет возможность проводить антивирусную обработку дисков, каталогов и файлов по запросу. Имеет удобные средства просмотра результатов обработки.

Консольный сканер для Windows - консольный сканер Vba32 может использоваться для запуска антивирусной проверки дисков, каталогов и файлов из командной строки.

Расширение контекстного меню Проводника Windows - позволяет обрабатывать указанные файлы из контекстного меню Проводника Windows.

Антивирусный Почтовый фильтр - позволяет обрабатывать электронные почтовые сообщения до принятия их по протоколам POP3 и IMAPv4 почтовыми клиентами.

Антивирусный модуль для Microsoft Outlook - данный антивирусный модуль предназначен для защиты почтовых клиентов Microsoft Outlook и Microsoft Exchange Client.

Антивирусный скрипт-фильтр - позволяет осуществлять антивирусную защиту Microsoft Internet Explorer, Microsoft Outlook Express, а также любых других приложений, использующих технологию Microsoft Windows Scripting Host.

Антивирусный карантин - обеспечивает хранение инфицированных и подозрительных файлов, помещенных в него антивирусными модулями Vba32.

Модуль сбора информации о работе комплекса VBA32 (утилита SendLogs) - предназначен для сбора технической информации и файлов отчёта всех компонентов Vba32 с последующим их сохранением на диск или отправкой специалистам ОДО "ВирусБлокАда".

Агент удаленного администрирования – обеспечивает централизованное управление программными модулями в сети, сбор информации о состоянии программного комплекса Vba32.

Активация – позволяет перевести программы из демонстрационного режима в полнофункциональный.

Антируткит – позволяет обнаруживать аномалии операционных систем семейства Windows, вызванные присутствием в системе вредоносных программ, и восстанавливать целостность операционной системы путем их обезвреживания.

Планировщик задач комплекса Vba32 – позволяет запускать задачи (сторонние приложения, процесс сканирования, процесс обновления) в указанные временные ограничения на персональных компьютерах, рабочих станциях и серверах.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

Комплекс устанавливается на ПК на базе архитектуры Intel x86 и требует наличия:

1) 32-разрядного (x86) или 64-разрядного (x64) процессора с тактовой частотой не ниже 2 ГГц;
2) не менее 1 ГБ оперативной памяти;
3) не менее 500 МБ свободного пространства на логическом диске ПК.

2.2. Требования к программным средствам

Комплекс функционирует под управлением ОС Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

2.3. Общие характеристики входной и выходной информации

Входными данными для Комплекса являются команды, вводимые оператором с клавиатуры и «мыши». Входными данными также могут являться файлы конфигурации и сообщения (коды возврата) о результатах выполнения команд различными модулями. Выходными данными является информация, выводимая на дисплей, а также информация, необходимая для работы модулей.

2.4. Требования организационного характера

Персонал, использующий разработанное программное обеспечение, должен обладать соответствующими знаниями в данной предметной области.

3. ОПИСАНИЕ ЗАДАЧИ

Задача Комплекса – защитить рабочую станцию от воздействия вредоносных программ и компьютерных вирусов. Для этого необходимо установить и настроить все компоненты Комплекса.

3.1. Использование Комплекса

3.1.1. Диспетчер Vba32

Диспетчер Vba32 предназначен для:

- загрузки антивирусного ядра в оперативную память;
- введения пароля для защиты настроек от изменения пользователем;
- вызова модулей с графическим пользовательским интерфейсом;
- установки параметров запуска модулей;
- настроек режимов обработки оперативной памяти и загрузчиков;
- установки режима работы с файлом отчета работы общего загрузочного модуля и его просмотра;
- работы со звуковым оповещением;
- обновления базы данных известных вредоносных программ и исполнимых модулей Комплекса по сетевому пути или через Интернет.

Для запуска Диспетчера достаточно набрать в командной строке» Vba32Ldr.exe» и нажать клавишу «Enter» или дважды щелкнуть «мышью» на иконке Vba32. В этом случае параметрами работы являются параметры, записанные в реестр Windows при установке Комплекса или настройке в процессе работы.

При запуске Диспетчера из командной строки доступны следующие ключи:

/SL - загрузить сканер;

/SU - выгрузить сканер;

/MN - включить монитор;

/MF - выключить монитор;

/LU - выгрузить Диспетчер;

/BL - обновить компоненты.

Диспетчер может также загружаться автоматически (если это указано в его параметрах загрузки). Процесс загрузки, в зависимости от настроек, может отображаться в окне (рис. 1).

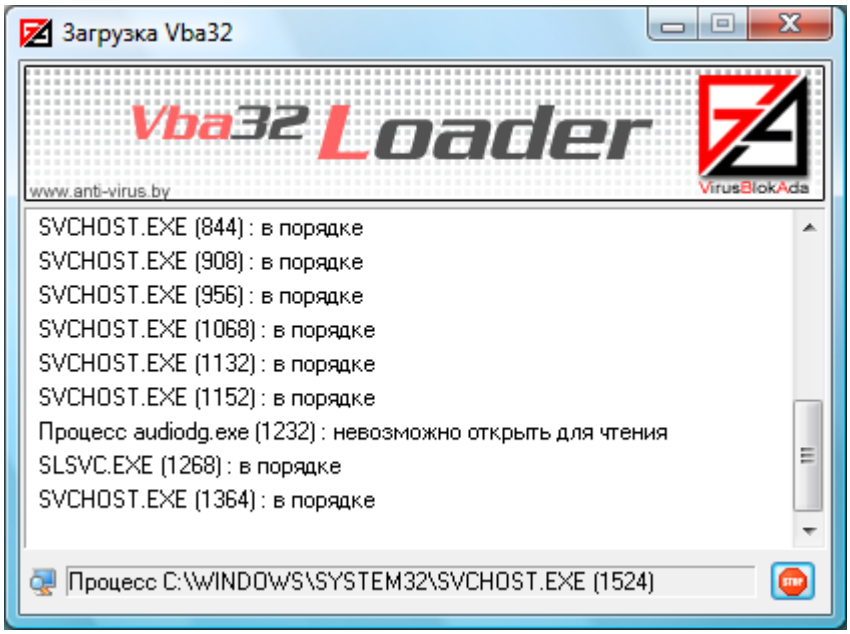

Рис. 1

При работе Диспетчера в панели задач появляется иконка с логотипом ОДО «ВирусБлокАда». При щелчке правой кнопкой «мыши» на иконке отображается контекстное меню Диспетчера (рис. 2), содержащее пункты:

- Настройки;
- Обновление;
- Карантин;
- Сканер;
- Монитор ВЫКЛючить (Монитор ВКЛючить);
- Поддержка;
- Выход.

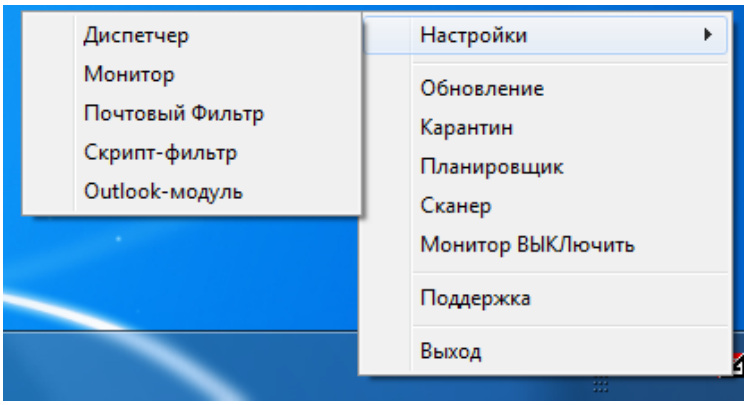

Рис. 2

Выбор пункта «Настройки» приводит к появлению выпадающего меню с пунктами, соответствующими установленным модулям Комплекса («Диспетчер», «Монитор», «Почтовый фильтр», «Скрипт-фильтр», «Outlook-модуль»). Выбор пункта «Обновление» приводит к попытке обновления программы по указанному в Диспетчере пути. Пункт «Карантин» запускает Карантин. Пункт «Сканер» запускает сканер. Пункт меню «Монитор ВЫКЛючить» («Монитор ВКЛючить»)

обеспечивает выключение (включение) монитора. Пункт «Поддержка» загружает окно с информацией о поддержке и возможностью запустить утилиту SendLogs. Пункт меню «Выход» позволяет выгрузить Комплекс из оперативной памяти.

Пункт меню «Настройки» - «Диспетчер» вызывает главное окно программы, которое имеет три закладки:

– «Общее»;

– «Инициализация»;

– «Дополнительно».

На закладке «Общее» (рис. 3) отображаются сведения об ОС, в среде которой работают компоненты, о лицензии и о программе. Здесь же присутствуют кнопки:

– «Пароль» - при нажатии на эту кнопку в появившемся диалоговом окне (рис. 4) можно изменить пароль;

– «Монитор» - при нажатии на эту кнопку на экране появляется графический интерфейс монитора;

– «Сканер» - при нажатии на эту кнопку на экране появляется графический интерфейс сканера;

– «Карантин» - при нажатии на эту кнопку на экране появляется графический интерфейс Карантина;

– «Выгрузить» - при нажатии на эту кнопку Комплекс выгружается из оперативной памяти ПК.

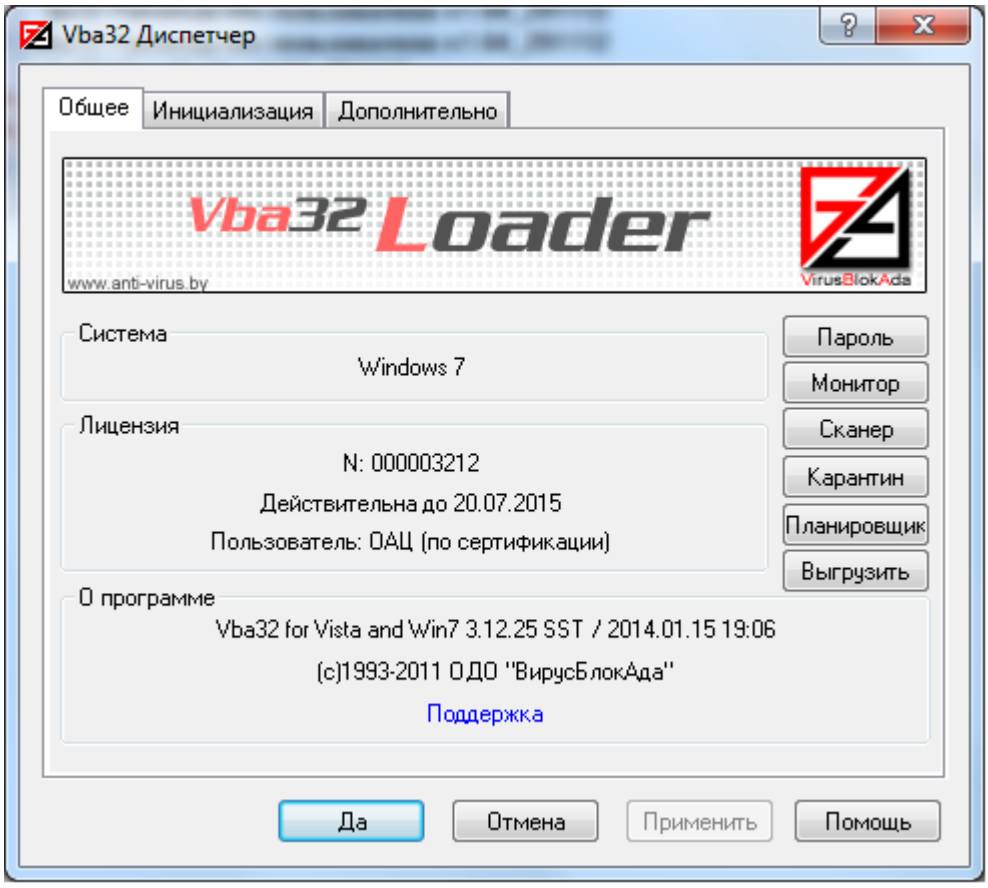

Рис. 3

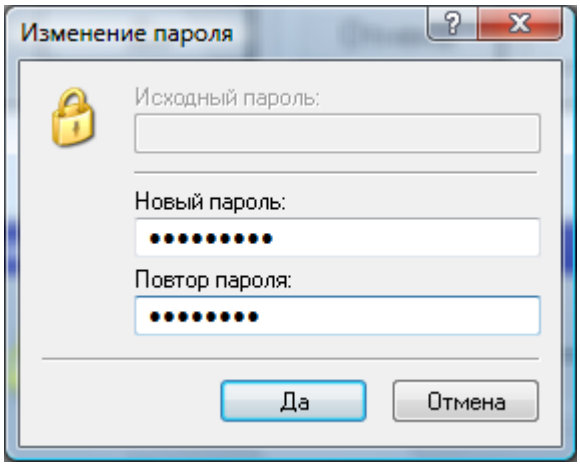

Рис. 4

Закладка «Инициализация» (рис. 5) служит для настройки параметров загрузки, а также обработки памяти и загрузчиков.

Пункт «Загружать Диспетчер при старте Windows» позволяет загружать Диспетчер при каждом включении или перезагрузке ПК.

Пункт «Включать Монитор при старте Диспетчера» разрешает автоматическую загрузку Монитора при каждом запуске Диспетчера.

Пункт «Защищать процесс Диспетчера» включает защиту процесса Диспетчера.

В нижней части окна имеются пункты, определяющие режимы работы Диспетчера при его запуске и режимы обработки объектов Диспетчером.

Пункт «Показывать процесс загрузки» позволяет отобразить на экране монитора загрузку Диспетчера. При этом в окне будут отображаться загрузка модулей Комплекса, результаты проверки оперативной памяти и загрузчиков.

Пункт «Обрабатывать память» включает обработку оперативной памяти при загрузке Диспетчера, при этом пункт «Быстрый режим» указывает на то, что будет производиться поиск наиболее опасных и наиболее распространенных вредоносных программ.

Пункт «Обрабатывать загрузчики» разрешает обработку загрузочных секторов жесткого диска, а пункт «Обрабатывать загрузчики дискет» - загрузчиков дискет.

Пункт «Поиск программ типа RootKit» включает режим обнаружения программ типа RootKit.

Пункт «Обрабатывать файлы, запускаемые при старте системы» включает проверку файлов, загружаемых при старте системы.

В нижней части окна выводится путь, по которому установлен Комплекс.

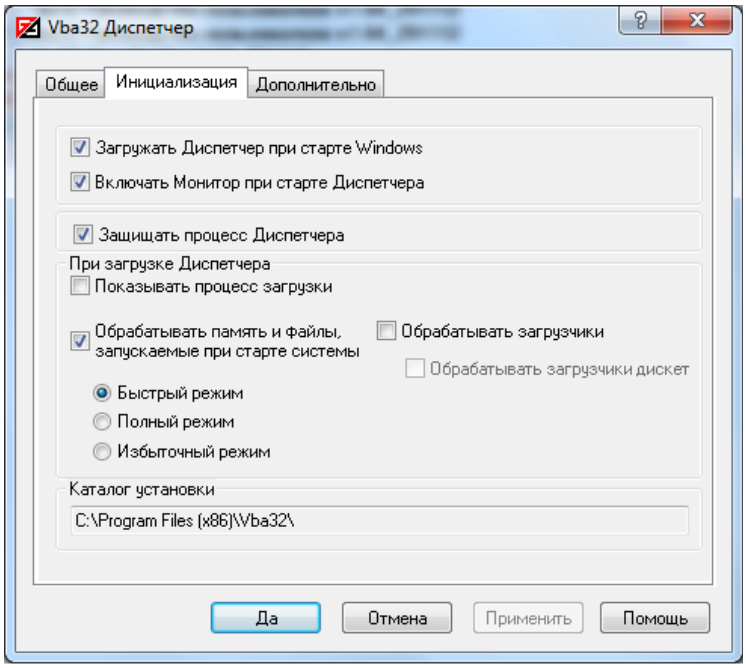

Рис. 5

На закладке «Дополнительно» (рис. 6) задаются параметры файла отчета о работе общего загрузочного модуля, включение звукового извещения, а также возможность обновления баз данных известных вредоносных программ по сетевому пути или через Интернет.

Необходимость ведения файла отчета о работе Диспетчера определяются пунктом «Вести». Имя файла отчета можно указать в строке ввода справа от данного пункта. Кнопка «Обзор» открывает диалоговое окно, в котором можно указать файл отчета.

Пункты «Дописывать» и «Максимальный размер, Кб» становятся активными, если выбран пункт «Вести». Выбор первого пункта приводит к тому, что информация о работе общего загрузочного модуля будет дописываться в файл отчета (иначе файл отчета будет создаваться заново при каждом запуске). Второй пункт позволяет задать максимальный размер файла отчета. При превышении данного размера старая информация (находящаяся в начале файла отчета) будет удаляться, а в файл отчета будет дописываться текущая информация.

Кнопка «Показать» позволяет просмотреть файл отчета о работе Диспетчера.

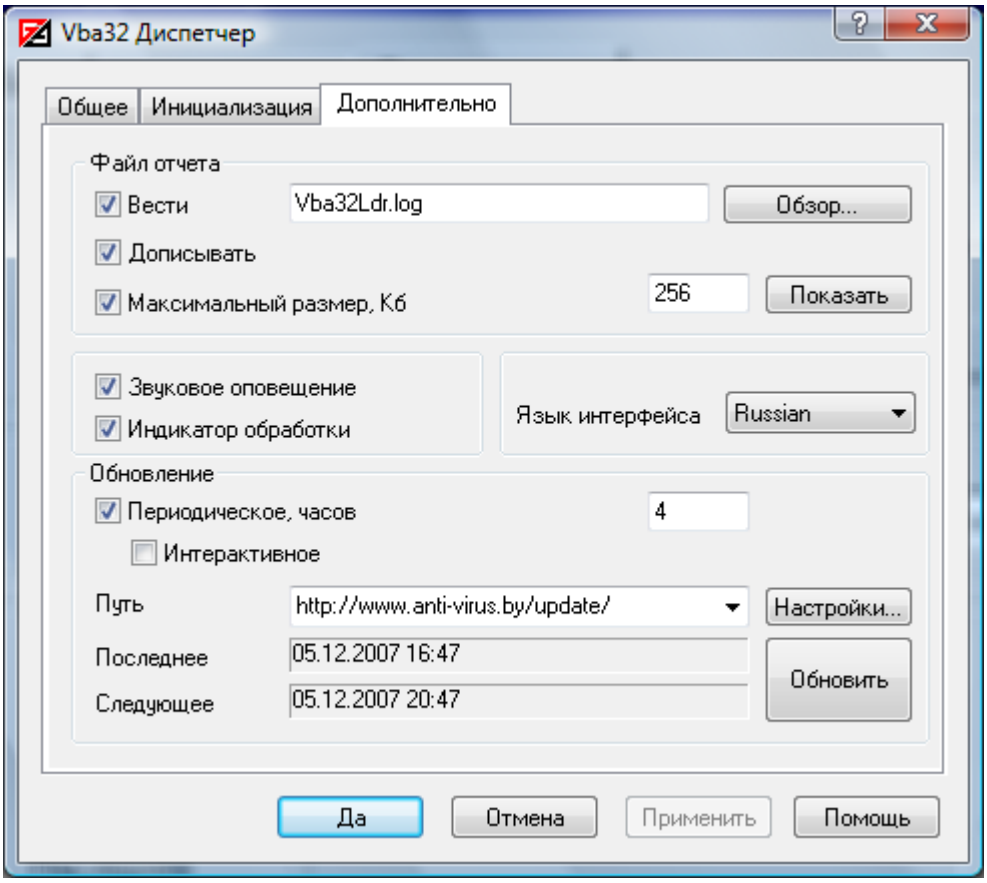

Рис. 6

Выбор пункта «Звуковое оповещение» включает подачу звукового сигнала в случае наступления определенных событий (в том числе обнаружения вредоносных программ) при работе общего загрузочного модуля, сканера и монитора.

Пункт «Язык интерфейса» позволяет выбрать один из установленных языков интерфейса (русский, английский, украинский и т.д.).

В нижней части закладки расположены настройки обновления Комплекса. Выбор пункта «Периодическое обновление» включает автоматическое обновление Комплекса через промежуток времени, указанный в строке ввода справа. Диалоговый режим в процессе обновления устанавливается с помощью пункта «Интерактивное обновление». Путь к пакету обновлений указывается в поле «Путь». По умолчанию предлагается выбрать адрес в Интернете http://www.anti-virus.by/update/. Путь к пакету обновлений можно указать в диалоговом окне, открывающемся по нажатию кнопки «Обзор». При обновлении с ПК в локальной сети достаточно создать на этом ПК копию папки обновлений, находящейся по адресу http://www.anti-virus.by/update/, и поддерживать ее в актуальном состоянии.

Кнопка «Настройки» служит для вывода окна «Настройки доступа к сети» (рис. 7).

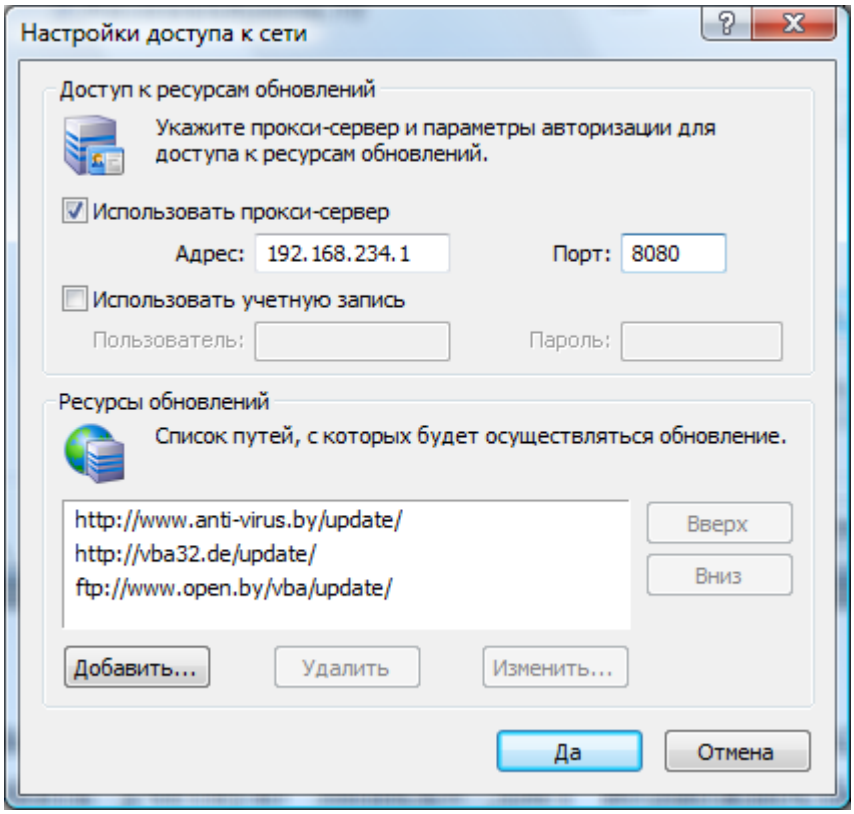

Рис. 7

Пункт «Использовать прокси-сервер» позволяет ввести адрес и порт proxy-сервера.

Пункт «Использовать учетную запись» дает возможность указать имя пользователя и пароль для proxy-сервера при обновлении через Internet или имя пользователя и пароль для доступа к сетевому ресурсу при обновлении по локальной сети.

В группе «ресурсы обновлений» отображается список путей, с которых будет осуществляться обновление. Первый используемый путь находится в верху списка. При помощи кнопок «вверх» и «вниз» можно соответственно перемещать выбранный путь вверх списка и вниз. Кнопки «Добавить…», «Удалить», «Изменить…» позволяют соответственно добавить новый ресурс обновления, удалить выбранный путь и изменить существующий путь для обновления.

Кнопка «Обновить» позволяет принудительно обновить Комплекс в данный момент времени.

Внизу окна в соответствующих полях автоматически выводятся дата и время последнего и следующего (в случае периодического) обновления.

При выбранном пункте «Интерактивное обновление» в процессе периодического обновления появляется диалоговое окно (рис. 8), в котором показаны модули, которые будут обновлены.

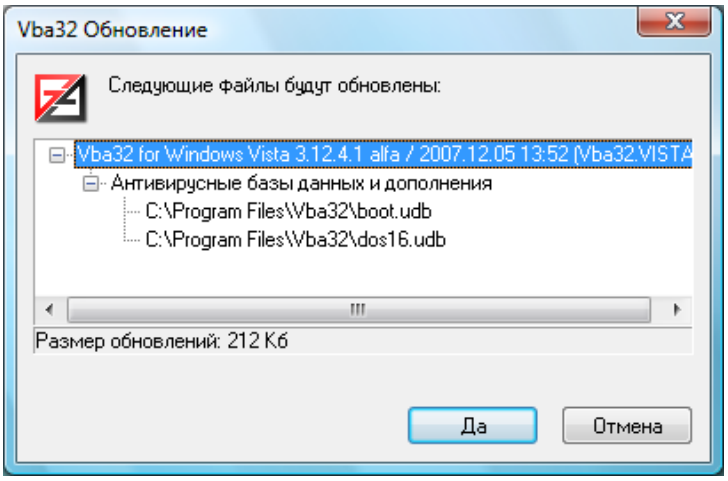

Рис. 8

Обновление завершается диалоговым окном с его результатами (рис. 9).

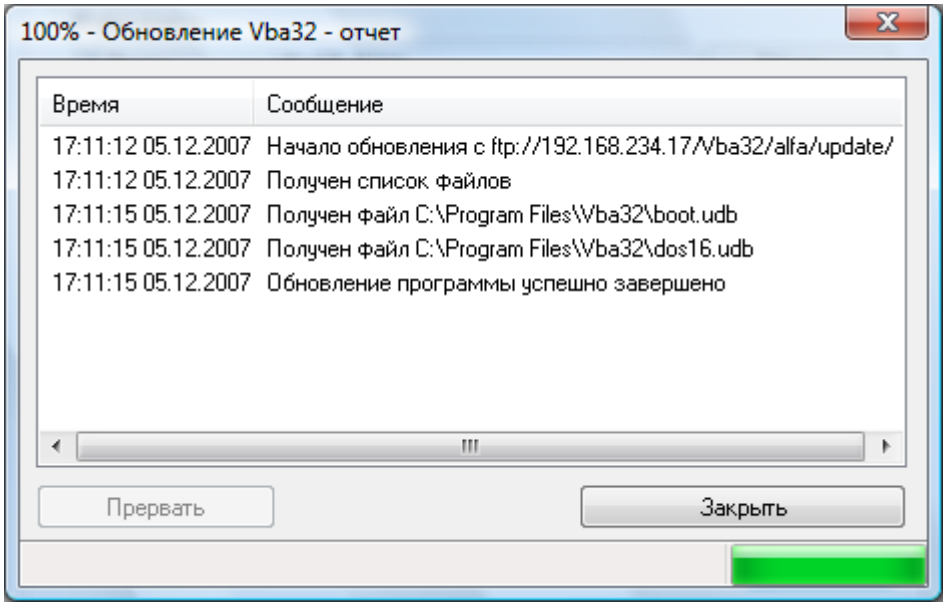

Рис. 9

3.1.2. Сканер

Сканер предназначен для антивирусной обработки оперативной памяти, загрузочных секторов дисков, выбранных пользователем папок и файлов на локальных и сетевых логических дисках.

Для запуска сканера в командной строке достаточно набрать «Vba32Ldr.exe /SL» и нажать клавишу «Enter». В этом случае параметрами работы являются параметры, записанные в реестре Windows при установке Комплекса или в файле конфигурации при его настройке в процессе работы. Сканер может также загружаться при помощи ярлыка в меню «Пуск», либо на «Рабочем столе» (при условии выбора данной возможности во время установки Комплекса). Кроме того, для запуска сканера можно щелкнуть правой кнопкой «мыши» по иконке с логотипом

ОДО «ВирусБлокАда» и в появившемся меню выбрать пункт «Сканер». После загрузки на экране появляется главное окно программы (рис. 10).

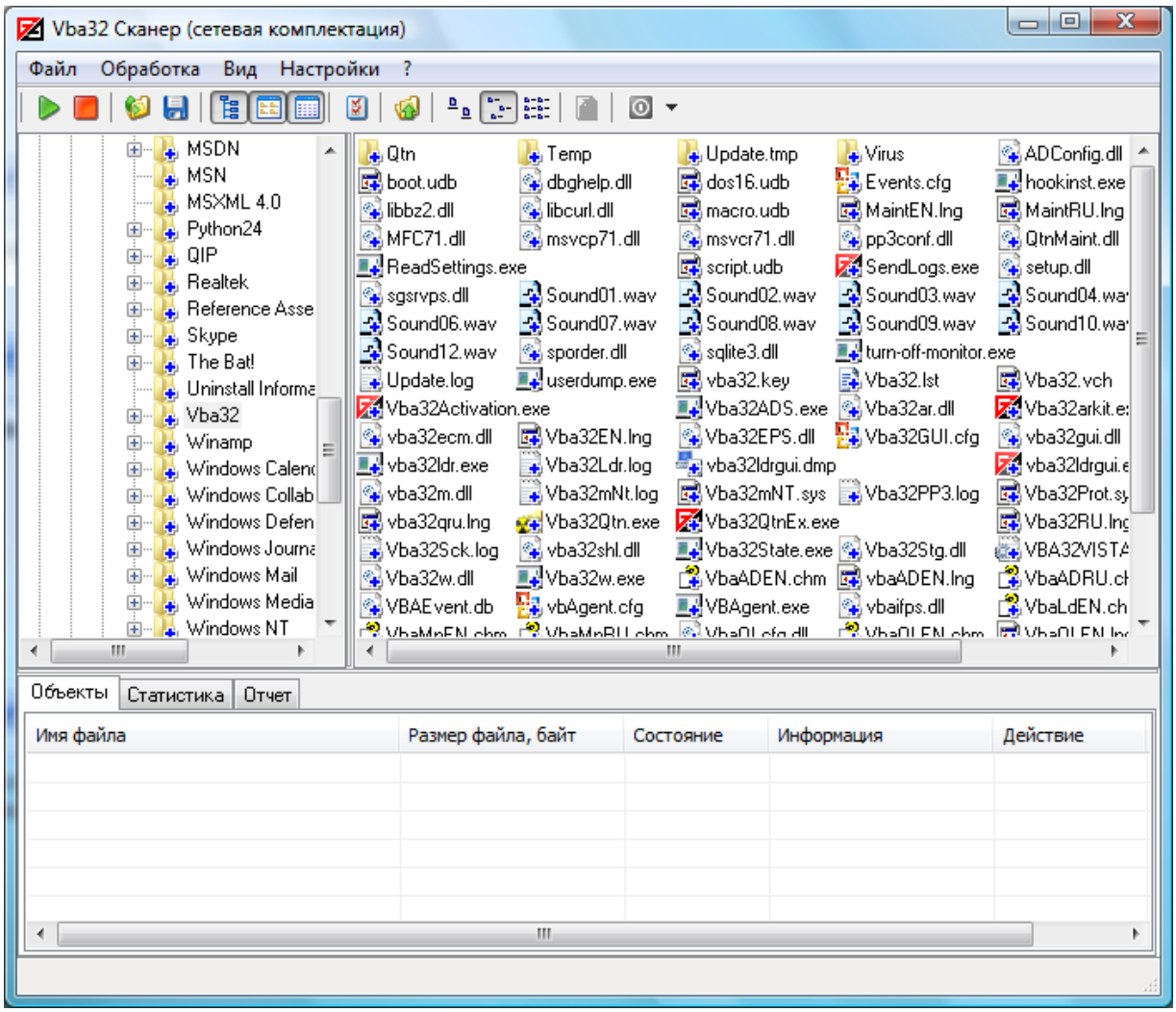

Рис. 10

3.1.2.1. Главное окно

В верхней части окна имеются строка меню и панель инструментов. В окне одновременно отображается как структура находящихся на ПК папок (слева), так и содержимое выделенной папки (справа). В нижней части окна располагаются три вкладки:

– Объекты;
– Статистика;
– Отчет.

Вкладка «Объекты» позволяет наблюдать за процессом обработки объектов и получить результаты сканирования в виде дерева объектов. В зависимости от настроек Сканера корневыми могут быть следующие элементы:

– Процессы;
– Загрузочные сектора;

– Автозапуск;

– Файловая система.

Информация о дереве организована в виде таблицы со следующими столбцами:

– Имя файла – содержит имя элемента дерева объектов. Это может быть имя процессов, идентификатор загрузочного сектора, путь к файлу, который находятся в автозагрузке, или путь к инфицированному или подозрительному файлу;

– Размер файла, байт – содержит размеров объектов, которые являются файлами;

– Состояние – состояние проверенного объекта;

– Информация - информация о вирусе или о подозрении на вирус;

– Действие – действие совершённое над объектом либо причина невозможности его выполнения;

– Копия – принимает значение «Да», если объект был помещён в Карантин. В противном случае – «Нет».

В зависимости от типа объекта над ним могут быть совершены некоторые действия. Чтобы получить к ним доступ, нужно щёлкнуть по объекту правой кнопкой мыши. Появившееся контекстное меню содержит следующие пункты:

– Показать файл - открывает в окне «Проводника» местонахождение объекта;

– Обезвредить - пытается обезвредить объект;

– Удалить - удаляет объект;

– Поместить в карантин - помещает объект в Карантин;

– Развернуть все - если объект является корневым элементов и свёрнут, то он разворачивается, отображая дочерние элементы;

– Свернуть все - если объект является корневым элементов и развёрнут, то он сворачивается, скрывая дочерние элементы;

– Выбрать все - выделяет все объекты в таблице;

– Копировать текст - копирует всю строку таблицы, содержащую объект, в буфер обмена;

– Завершить процесс - если объект является процессом, то пытается завершить его выполнение.

Во время сканирования на вкладке «Объекты» отображаются тип проверяемого объекта и статус его обработки. После завершения сканирования для корневых элементов «Процессы», «Автозагрузка» и «Загрузочные сектора» отображается информация о проверенных объектах. Записи об объектах файловой системы появляются лишь в том случае, если они инфицированы или подозрительные.

Вкладка «Статистика» содержит статистику работы Сканера при последнем его запуске:

– Обрабатываемый объект - показывает имя обрабатываемого в данный момент объекта;

– Процессы - показывает результат проверки процессов запущенных в системе;

– Загрузочные сектора - показывает результат проверки загрузочных секторов;

– Автозагрузка - показывает результат проверки файлов, находящихся в автозагрузке;

– Файловая система - показывает результат проверки объектов файловой системы;

– Найдено уникальных вредоносных программ - показывает количество найденных уникальных вредоносных программ;

– Найдено уникальных подозрений - показывает количество найденных уникальных подозрительных объектов;

– Время обработки - показывает продолжительность последнего сканирования;

– Файлов на дисках - показывает статистику по сканированию файлов на дисках.

Пункт «Файлов на дисках» содержит следующие параметры:

– обработано - показывает общее количество обработанных файлов;

– подозрительных - показывает количество обнаруженных подозрительных файлов;

– инфицированных - показывает количество обнаруженных инфицированных файлов;

– создано копий - показывает количество созданных копий инфицированных и подозрительных файлов;

– обезврежено - показывает количество обезвреженных файлов;

– удалено - показывает количество удаленных файлов.

Вкладка «Отчёт» содержит фрагмент файла отчёта с записями, которые касаются последнего процесса сканирования. В данной вкладке при работе программы выводится информация о работе и, после завершения обработки выбранных объектов, статистические данные. Кроме того, текущая информация и некоторые подсказки появляются в строке состояния.

При работе с окном, в котором изображается иерархия папок, используются приемы, аналогичные соответствующему окну «Проводника» Windows. В данном окне можно выделить только один объект в качестве целого и обработать его. Выделенный объект назначается для обработки с помощью «мыши» при одновременном нажатии клавиши «Ctrl». Кроме того, выделенный объект можно назначить для обработки нажатием клавиши «Пробел». Данные действия, совершенные повторно, отменяют назначение для обработки.

При нажатии на правую кнопку «мыши» на объекте в данном окне появляется меню, в котором можно открыть данный объект, т.е. показать его содержимое, и начать обработку объекта. Содержимое объекта в этом случае при обработке отображается в окне содержимого папок.

В процессе работы с окном, в котором отображается содержимое папки, используются те же приемы работы, что и в «Проводнике». Выделение одного объекта и назначение его для обработки происходит так же, как и в окне иерархии папок. Кроме того, в данном окне можно выделить группу объектов, используя клавишу «Shift» и левую кнопку «мыши». Назначить для обработки выделенную группу можно, поставив на нее курсор и одновременно нажав на клавишу «Ctrl» и левую кнопку «мыши» или нажав на клавишу «Пробел» или клавишу «+». Эти же действия, совершенные повторно, отменяют выделение и назначение для обработки.

Если курсор установлен на каком либо из объектов в левом окне, нажатие на правую кнопку «мыши» приводит к появлению меню, в котором можно открыть данный объект и обработать объект (выделенную группу объектов).

Если курсор установлен на каком либо из объектов в правом окне, нажатие на правую кнопку «мыши» приводит к появлению меню, в котором можно открыть данный объект (диск или папку), обновить содержимое окна, обработать объект или добавить объект, на который указывает курсор, в список для обработки или убрать из него, добавить в список обработки или удалить из него все изображенные в окне объекты, выделить в группу все изображенные в окне объекты.

При выделении группы объектов нажатие на правую кнопку «мыши» вызывает видоизмененное меню, в котором появляются пункты «Обработать группу элементов» и

«Добавить в список обработки группу элементов» или «Убрать из списка обработки группу элементов».

Пункты «Отображать большие значки», «Отображать маленькие значки», «Отображать список» изменяют вид области окна, в которой показано содержимое папки.

Назначенный в список обработки объект помечается специальным знаком синего цвета. Сплошной знак свидетельствует о том, что данный объект будет обрабатываться целиком. В противном случае будет обработано не все содержимое объекта, а только объекты, назначенные внутри него.

3.1.2.2. Строка меню

Строка меню позволяет настроить интерфейс программы, выбрать режимы антивирусной обработки различных объектов, получить справочную информацию.

Пункт меню «Файл» позволяет:

– выбрать сохраненные ранее настройки программы, загрузив соответствующий файл конфигурации;

– сохранить выбранные настройки программы в файле конфигурации;

– просмотреть созданный в данном сеансе работы файл отчета;

– осуществить выход из программы.

Пункт меню «Обработка» дает возможность начать, приостановить и прекратить антивирусную обработку выбранных объектов, а также обработать файлы по списку, хранящемуся в файлах с расширением «.lst». Данный пункт так же позволяет выбрать действие, которое будет совершено после окончания сканирования.

Пункт меню «Вид» позволяет настроить общий вид окна.

Пункт меню «Настройки» служит для выбора режимов антивирусной обработки объектов на логических дисках, а также общих режимов работы программы.

Пункт меню «?» предназначен для получения справочной информации. Кроме этого, в данном пункте меню можно найти информацию о программе, ее авторах и системе поддержки антивируса.

При выборе пункта меню «Файл» появляется выпадающее меню, содержащее строки:

– Загрузить файл конфигурации;

– Сохранить файл конфигурации;

– Просмотреть файл отчета;

– Выход.

Пункт «Загрузить файл конфигурации» позволяет выбрать конфигурацию сканера, сохраненную пользователем в предыдущих сеансах работы. После выбора данного пункта меню появляется диалоговое окно (внешний вид окна и работа с ним полностью совпадает с окном «Открыть» стандартных приложений Windows), с содержимым папки, в которую установлен Комплекс. Для выбора требуемой конфигурации достаточно пометить и открыть соответствующий конфигурационный файл (имеющий расширение «.cfg»). Кроме того, в данном окне имеются две строки ввода, в одной из которых можно вручную ввести имя загружаемого файла конфигурации, а во второй – выбрать расширение имен файлов, которые должны быть показаны в окне.

Пункт «Сохранить файл конфигурации» дает возможность сохранить текущие настройки сканера в соответствующем файле конфигурации. При выборе данного пункта меню появляется диалоговое окно (внешний вид окна и работа с ним полностью совпадает с окном «Сохранить как» стандартных приложений Windows), с содержимым папки, в которой находится программа – сканер.

В данном окне имеется возможность выбора папки, в которой будет сохранен конфигурационный файл с текущими настройками. Кроме того, здесь же можно указать требуемое имя сохраняемого конфигурационного файла, которому будет дано расширение «.cfg».

Пункт «Просмотреть файл отчета» позволяет с помощью Блокнота из стандартных приложений Windows просмотреть отчет о работе сканера.

Пункт «Выход» позволяет завершить работу с программой.

При выборе пункта меню «Обработка» появляется выпадающее меню, содержащее строки:

– Начать обработку;
– Приостановить обработку;
– Прекратить обработку;
– Обработать список.
– После завершения сканирования.

Выбор пункта «Начать обработку» приводит к выполнению заданных действий над выбранными объектами. Пункт меню «Приостановить обработку» дает возможность приостановить антивирусную обработку (при продолжении обрабатываются оставшиеся объекты). Пункт меню «Прекратить обработку» дает возможность завершить по желанию пользователя обработку выбранных объектов. Пункт меню «Обработать список» позволяет обработать список инфицированных объектов, созданных при работе сканера (см. пункт меню «Настройки», «Отчет»). Пункт «После завершения сканирования» в зависимости от аппаратной конфигурации компьютера может содержать некоторые из следующих пунктов:

– Ничего - никаких действий после завершения сканирования не производится;
– Выключить - компьютер будет выключен после завершения сканирования;
– Спящий режим - компьютер будет переведён в Спящий режим после завершения сканирования;
– Ждущий режим - компьютер будет переведён в Ждущий режим после завершения сканирования

При выборе пункта меню «Вид» появляется выпадающее меню, содержащее строки:

– Показывать инструменты;
– Показывать строку статуса;
– Показывать иерархию папок;
– Показывать область объектов;
– Показывать отчет;
– Отображать большие значки;
– Отображать маленькие значки;
– Отображать список.

Пункт меню «Показывать инструменты» позволяет показывать или прятать панель инструментов. Пункт меню «Показывать строку статуса» позволяет показывать или прятать

строку статуса, расположенную внизу главного окна. Следующие три пункта меню также позволяют изменять внешний вид окна. В зависимости от выбранных пунктов показывается или прячется область окна, содержащая иерархию папок, содержимое папки и отчет об антивирусной обработке объектов. Пункты меню «Отображать большие значки», «Отображать маленькие значки», «Отображать список» изменяют вид области окна, в которой показано содержимое папки.

При выборе пункта меню «Настройки» появляется выпадающее меню, содержащее строки:

– Объекты;
– Действия;
– Отчет;
– Дополнительно.

Пункт меню «Объекты» (рис. 11) позволяет выбрать объекты для антивирусной обработки и общие режимы антивирусной обработки.

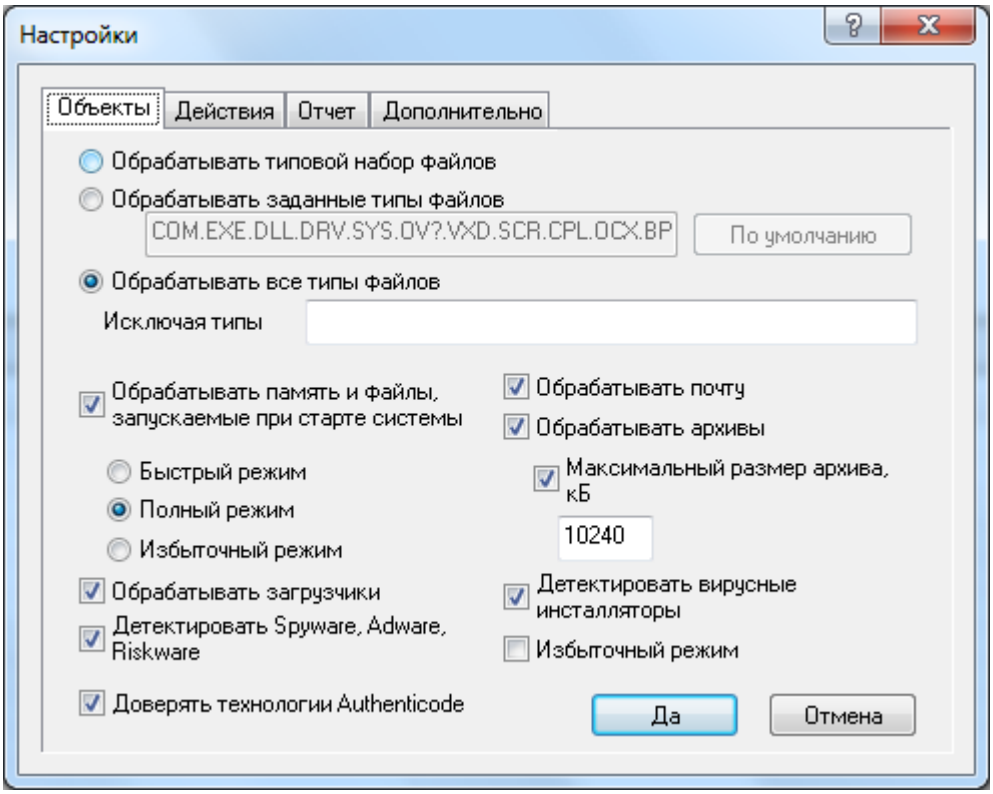

Рис. 11

Пункт «Обрабатывать типовой набор файлов» позволяет в качестве объектов для обработки выбрать файла с расширениями «.COM», «.EXE», «.DLL», «.DRV», «.SYS», «.OV?», «.VXD», «.SCR», «.CPL», «.OCX», «.BPL», «.AX», «.PIF», «.DO?», «.XL?», «.HLP», «.RTF», «.WI?», «.WZ?», «.MSI», «.MSC», «.HT*», «.VB*», «.JS», «.JSE», «.ASP*», «.CGI», «.PHP*», «.?HTML», «.BAT», «.CMD», «.EML», «.NWS», «.MSG».

Пункт «Обрабатывать заданные типы файлов» позволяет в качестве объектов для обработки указать файлы с расширениями, которые вводятся в строке, расположенной ниже данного пункта в диалоговом окне. По умолчанию в данной строке указаны расширения, соответствующие типовому набору файлов. После ввода нового списка расширений для ввода в данную строку списка типовых расширений служит кнопка «По умолчанию».

Пункт «Обрабатывать все типы файлов» в качестве объектов для обработки позволяет выбрать все типы файлов. В строке «Исключая типы» указываются расширения имен файлов, которые не должны обрабатываться.

Пункт «Обрабатывать память» позволяет в данном сеансе работы включить обработку памяти при антивирусной обработке объектов. «Быстрый режим» указывает на то, что обрабатываться будут только общие и системные области памяти, а обработка процессов будет исключена.

Пункт «Обрабатывать загрузчики» обеспечивает обработку загрузчиков.

Пункт «Обрабатывать файлы, запускаемые при старте системы» обеспечивает обработку файлов, запускаемых при старте системы.

Пункт «Поиск программ типа Rootkit» включает режим обнаружения программ.

Пункт «Детектировать Adware, Riskware» обеспечивает обнаружение Adware, Riskware.

Пункт «Обрабатывать почту» обеспечивает поиск компьютерных вирусов в присоединенных файлах и html-телах сообщений почтовых баз MS Outlook Express 4 и 5, The Bat! и MS Outlook.

Пункт «Обрабатывать архивы» дает возможность проверки файлов в архивах, созданных архиваторами RAR / ZIP / HA / ARJ / TAR / GZIP / BZIP2.

Пункт «Максимальный размер архива, кБ» включает ограничение на максимальный размер архивов, которые будут проверяться при сканировании.

Пункт «Детектировать вирусные инсталляторы» включает режим обнаружения вирусных инсталляторов.

Пункт «Избыточный режим» обеспечивает углубленную обработку файлов.

Пункт «Обрабатывать загрузчики» позволяют в данном сеансе работы включить обработку загрузчиков при антивирусной обработке объектов.

Пункт меню «Действия» (рис. 12) позволяет задать режимы антивирусной обработки инфицированных и подозрительных объектов, в том числе при невозможности их обезвреживания.

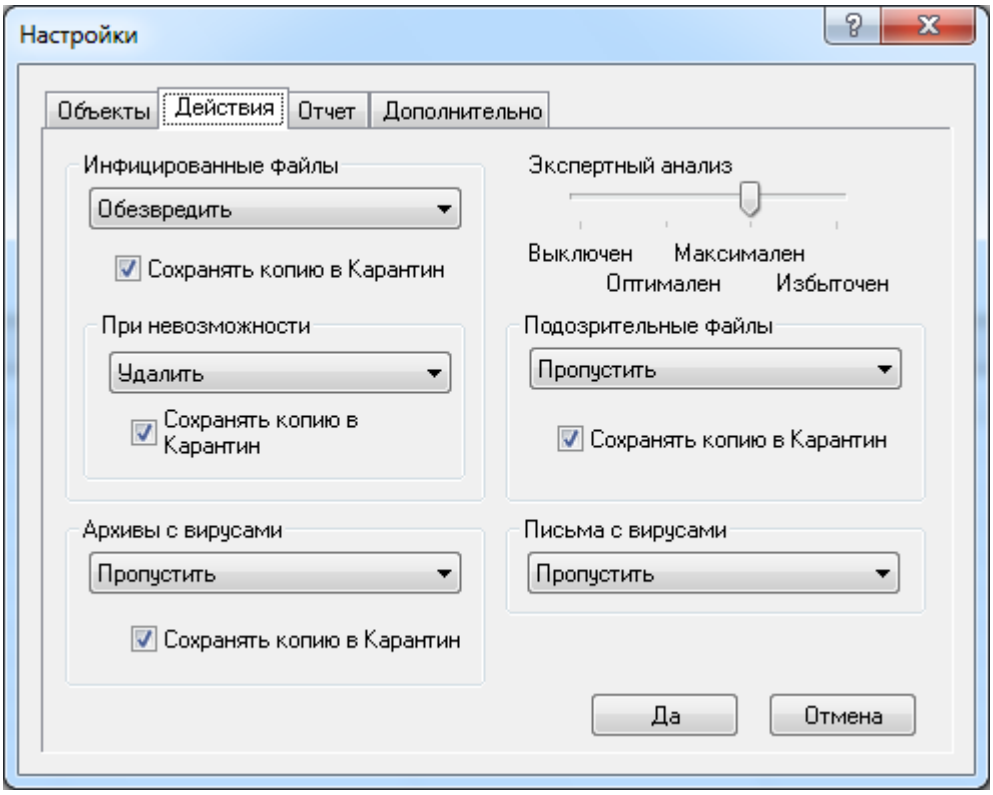

Рис. 12

Ползунок «Экспертный анализ» позволяет включить поиск неизвестных вирусов при обработке объектов. Положение «Оптимален» (рекомендуется при обработке объектов) позволяет обнаружить неизвестные вирусы, принадлежащие к известным семействам. Положение «Максимален» позволяет обнаружить неизвестные вирусы, использующие разновидности известных вирусных алгоритмов. Положение «Избыточен» позволяет обнаруживать максимальное число неизвестных вредоносных программ при большей вероятности ложных срабатываний.

Пункт «Пропустить» устанавливает режим поиска вирусов в выбранных для обработки объектах. Пункт «Обезвредить» вызывает режим обезвреживания вирусов в выбранных для обработки объектах. В том случае, когда имеются не зараженные резервные копии, инфицированные файлы целесообразно автоматически удалить, для чего необходимо выбрать «Удалить» в описываемом диалоговом окне. В некоторых случаях может являться целесообразным изменение режима обработки в процессе лечения. Для этого используется пункт «Дополнительный запрос». Пункт «Письма с вирусами» дает возможность пропустить письма, содержащие инфицированные объекты, обезвредить сообщения в почтовых базах MS Outlook или удалить инфицированные сообщения из почтовых баз MS Outlook Express / The Bat! Кроме того, данный пункт позволяет выводить дополнительный запрос на действия с инфицированными сообщениями. Пункт «Архивы с вирусами» позволяет пропустить архивы, содержащие внутри себя инфицированные объекты, включить режим удаления архивов, в которых хотя бы один файл инфицирован или является вредоносной программой, и вывести дополнительный запрос на действия над инфицированным архивом. Пункт «Сохранять копию в Карантин» включает сохранение копий инфицированных (подозрительных) файлов в Карантин.

Пункт меню «Отчет» (рис. 13) позволяет управлять окном отчета, вести список инфицированных файлов и назначить параметры файла отчета, его имя.

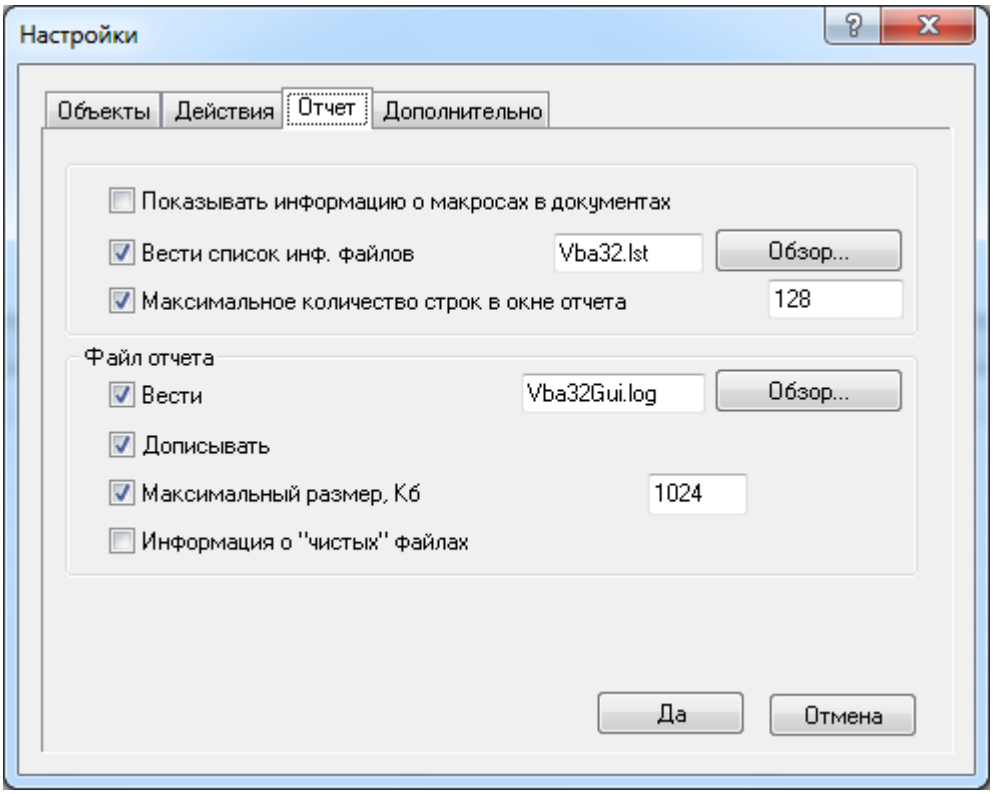

Рис. 13

Пункт «Показывать информацию о макросах в документах» позволяет выводить в окне отчета специальное обозначение, имя макроса и его параметры.

Обозначения:

[ ] - активный макрос;

[!] - макрос входит в состав какого-то вируса, возможно, это модификация макровируса;

[X] - в документе удаленный макрос (только в документах Word6);

[-] - макрос с пустым кодом (например, только комментарии);

[=] - макрос встречается в стандартных документах MS Office.

Пункт «Вести список инф. файлов» позволяет создать файл, содержащий список имен инфицированных файлов для последующей обработки по данному списку. Имя файла указывается в расположенной рядом строке ввода. Кнопка «Обзор» вызывает окно, аналогичное окну «Открыть» Windows.

Пункт «Максимальное количество строк в окне отчета» определяет количество строк (число строк указывается в расположенном рядом окне), которые можно просмотреть в окне отчета программы.

Пункт «Вести» задают режим, при котором результаты антивирусной обработки сохраняются в виде файла на диске. Имя файла указывается в расположенной рядом строке ввода. Кнопка «Обзор» вызывает окно, аналогичное окну «Открыть» Windows.

В обычном режиме работы файл отчета переписывается в каждом сеансе обработки. Пункт «Дописывать» позволяет продолжать файл отчета при следующих сеансах антивирусной обработки объектов.

В окне, расположенном рядом с пунктом «Максимальный размер, Кб», указывается наибольший размер файла, содержащего отчет об антивирусной обработке объектов.

Пункт «Информация о чистых файлах» позволяет включать в файл отчета информацию о чистых файлах.

Пункт меню «Дополнительно» (рис. 14) позволяет автоматизировать настройку программы при запуске и указать приоритет выполнения антивирусной обработки объектов.

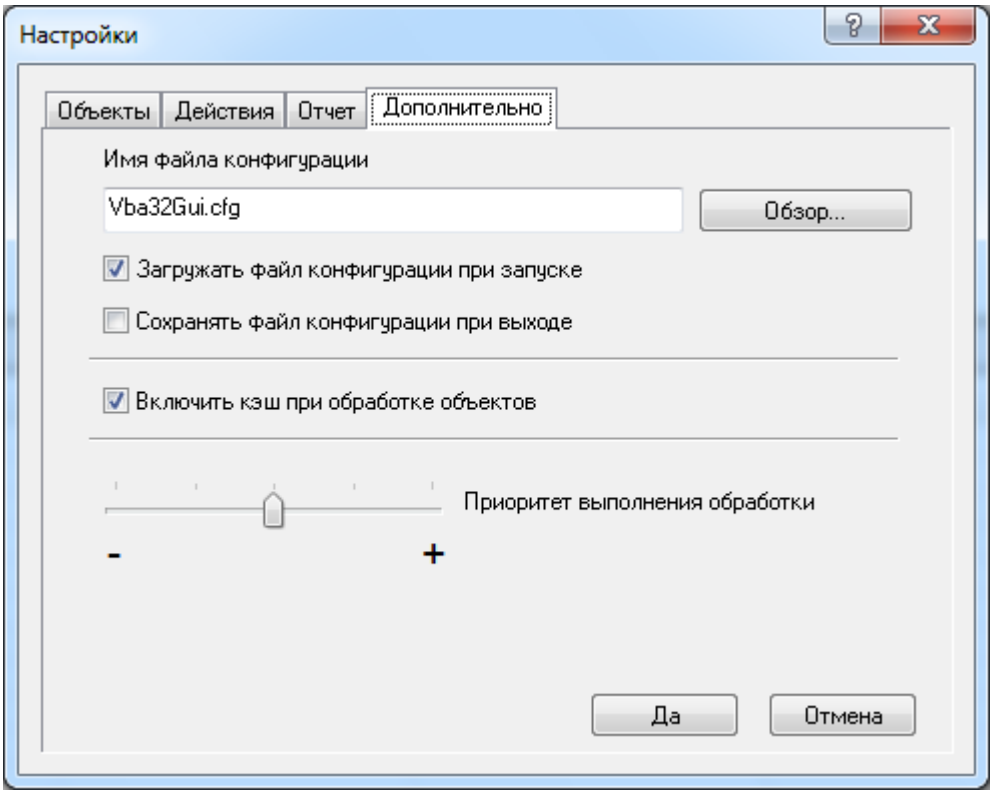

Рис. 14

Имя файла конфигурации по умолчанию указано в строке ввода. Кнопка «Обзор» вызывает окно, аналогичное стандартному окну «Сохранить как». В данном окне можно выбрать диск и папку, в которых сохранится файл конфигурации.

Пункт «Загружать файл конфигурации при запуске» позволяет запустить программу с параметрами, выбранными в предыдущем сеансе работы.

Пункт «Сохранять файл конфигурации при выходе» автоматически сохраняет в файле конфигурации текущие настройки программы.

Пункт «Включить кэш при обработке объектов» позволяет создавать библиотеку контрольных сумм обрабатываемых файлов и, в дальнейшем, проводить обработку файлов по контрольным суммам. В том случае, если контрольная сумма файла между обработками не изменилась, то его обработка в данном сеансе прекращается. Следует отметить, что созданная библиотека контрольных сумм используются также монитором и консольными сканерами при их функционировании.

Шкала «Приоритет выполнения обработки» задает приоритет проверки в многозадачной среде Windows.

Пункт меню «?» позволяет получить информацию о программе, о ее поддержке и помощь по работе с программой.

3.1.2.3. Панель инструментов

В панели инструментов (рис. 15) присутствуют следующие кнопки:

– Начать обработку – приступить к обработке назначенных объектов. В процессе обработки данная кнопка приостанавливает и возобновляет обработку.

– Остановить обработку – Остановить обработку назначенных объектов.

– Загрузить конфигурацию – соответствует пункту меню «Файл - Загрузить файл конфигурации».

– Сохранить конфигурацию - соответствует пункту меню «Файл - Сохранить файл конфигурации».

– Показать/скрыть иерархию папок - соответствует пункту меню «Вид – Показывать иерархию папок».

– Показать/скрыть папку - соответствует пункту меню «Вид – Показывать папку».

– Показать/скрыть отчет - соответствует пункту меню «Вид – Показывать отчет».

– Настройки - соответствует пункту меню «Настройки».

– Переход на уровень вверх – позволяет перейти на один уровень вверх в окне папок.

– Отображать крупные значки - соответствует пункту меню «Вид – Отображать большие значки».

– Отображать мелкие значки - соответствует пункту меню «Вид – Отображать маленькие значки».

– Отображать список - соответствует пункту меню «Вид – Отображать список».

– Просмотреть файл отчета - соответствует пункту меню «Файл - Показать файл отчета».

– Действие после завершения сканирования - соответствует пункту меню «Обработка – После завершения сканирования».

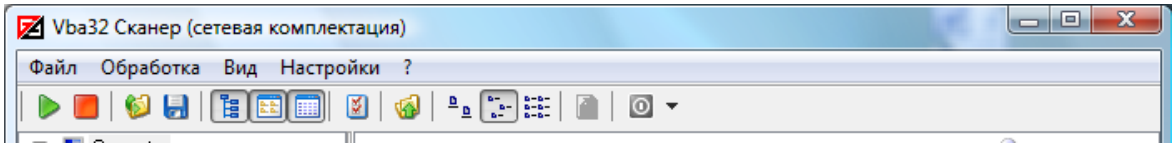

Рис. 15

3.1.3. Монитор

Программа-монитор постоянно находится в оперативной памяти ПК и осуществляет поиск компьютерных вирусов в файлах при открытии, запуске на выполнение и закрытии.

Для включения монитора в командной строке достаточно набрать «Vba32Ldr.exe /MN» (для выключения монитора используется ключ MF) и нажать клавишу Enter или щелкнуть правой кнопки «мыши» на иконке с логотипом ОДО «ВирусБлокАда» и выбрать соответственно «Монитор ВКЛючить» (или «Монитор ВЫКЛючить»). В этом случае параметрами работы являются параметры, записанные в реестре Windows при установке Комплекса или настройке в

процессе работы. Монитор может также загружаться автоматически (если это указано в его параметрах загрузки).

После загрузки на экране появляется главное окно программы, на котором показаны пункты «Общее», «Объекты», «Действия», «Отчет», «Статистика» и кнопки «Включить» («Выключить»), «Да», «Отмена», «Применить», «Помощь».

Содержимое вкладки «Общее» (рис. 16) позволяет получить информацию о лицензии и программе. Кнопка «ВКЛючить» («ВЫКЛючить») позволяет включить (выключить) монитор.

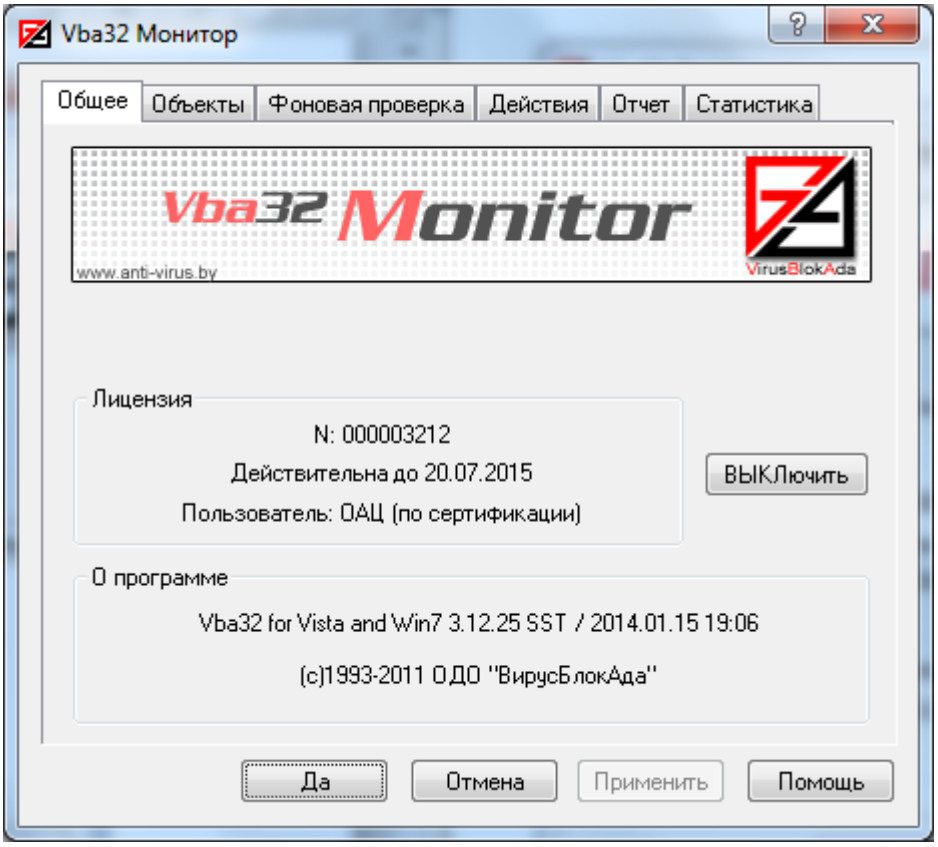

Рис. 16

Вкладка «Объекты» (рис. 17) позволяет выбрать объекты для антивирусной обработки и общие режимы антивирусной обработки.

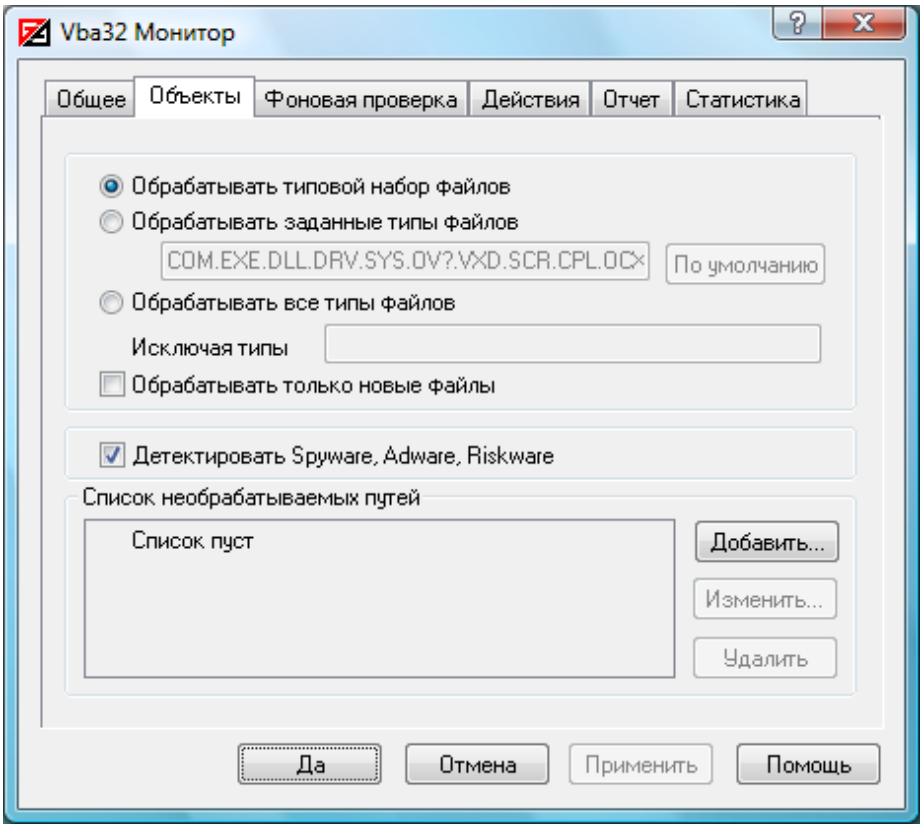

Рис. 17

Пункт «Обрабатывать типовой набор файлов» позволяет в качестве объектов для обработки выбрать файла с расширениями «.COM», «.EXE», «.DLL», «.DRV», «.SYS», «.OV?», «.VXD», «.SCR», «.CPL», «.OCX», «.BPL», «.AX», «.PIF», «.DO?», «.XL?», «.HLP», «.RTF», «.WI?», «.WZ?», «.MSI», «.MSC», «.HT*», «.VB*», «.JS», «.JSE», «.ASP*», «.CGI», «.PHP*», «.?HTML», «.BAT», «.CMD», «.EML», «.NWS», «.MSG».

Пункт «Обрабатывать заданные типы файлов» позволяет в качестве объектов для обработки указать файлы с расширениями, которые вводятся в строке, расположенной ниже данного пункта в диалоговом окне. По умолчанию в данной строке указаны расширения, соответствующие типовому набору файлов. После ввода нового списка расширений для ввода в данную строку списка типовых расширений служит кнопка «По умолчанию».

Пункт «Обрабатывать все типы файлов» в качестве объектов для обработки позволяет выбрать все типы файлов. В строке «Исключая типы» указываются расширения имен файлов, которые не должны обрабатываться.

Пункт «обрабатывать только новые файлы» включает режим, при котором обрабатываются только вновь созданные и измененные файлы заданных типов, что значительно уменьшает задержки, вызванные работой Vba32 Монитором, за счет снижения надежности защиты. При использовании данного режима необходимо периодически выполнять проверку компьютера Сканером.

Пункт «Детектировать Adware, Riskware» позволяет включить (выключить) обнаружение Adware, Riskware.

Область «Список необрабатываемых путей» позволяет задать (изменить, удалить) пути файловой системы, которые не будут обрабатываться монитором.

Вкладка «Фоновая проверка» (рис. 18) позволяет осуществлять фоновую проверку файлов Монитором.

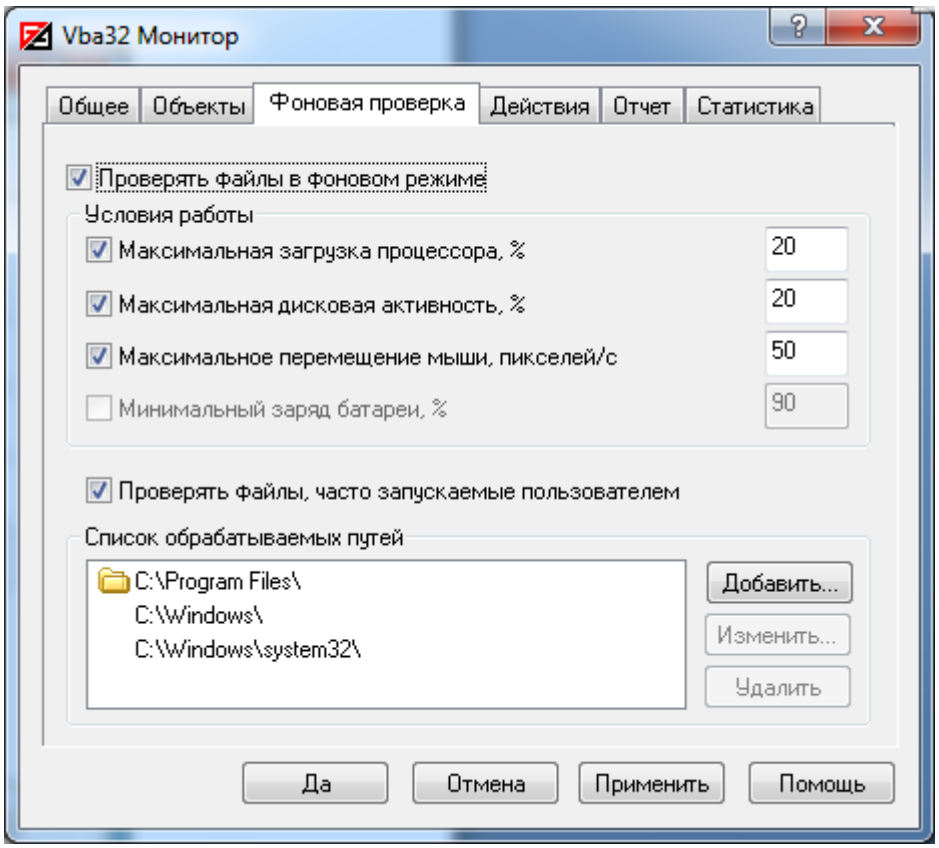

Рис. 18

Пункт «Проверять файлы в фоновом режиме» включает фоновую обработку файлов Монитором. Проверка осуществляется только при выполнении условий работы.

Пункт «Условия работы» позволяет задать условия, при которых Монитор осуществляет фоновую проверку.

Пункт «Максимальная загрузка процессора, %» определяет максимальную загрузку процессора в процентах, не считая загрузки, при которой производится фоновая проверка файлов. Загрузка процессора Диспетчером при этом не учитывается.

Пункт «Максимальная дисковая активность, %» определяет максимальную дисковую активность в процентах, при которой производится фоновая проверка файлов.

Пункт «Максимальное перемещение мыши, пикселей/с» определяет максимальное перемещение указателя мыши, при котором Монитор не прекращает фоновую проверку файлов.

Пункт «Минимальный заряд батареи, %» определяет минимальный заряд батареи в процентах, при котором производится фоновая проверка файлов. Если заряд батареи меньше указанного, то проверка приостанавливается.

Пункт «Проверять файлы, запускаемые при старте системы» определяет обработку файлов, автоматически запускаемых при старте системы во время фоновой проверки.

Пункт «Проверять файлы, часто запускаемые пользователем» определяет обработку файлов, часто запускаемых пользователем во время фоновой проверки.

Пункт «Список обрабатываемых путей» - список путей, которые будут обработаны Монитором во время фоновой проверки. Кнопки «Добавить», «Изменить» и «Удалить» предназначены для редактирования списка.

Вкладка «Действия» (рис. 19) позволяет задать режимы антивирусной обработки инфицированных и подозрительных файлов.

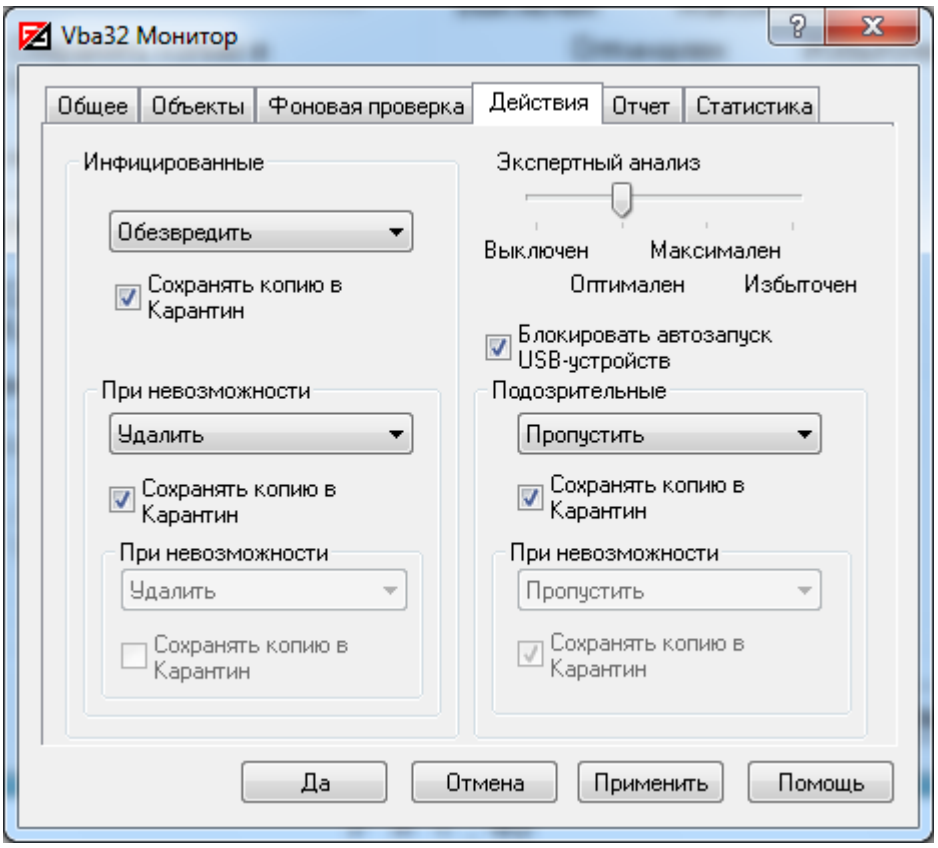

Рис. 19

Пункт «Блокировать» запрещает доступ к инфицированному объекту. «Обезвредить» вызывает режим обезвреживания вирусов в обрабатываемом файле. Для автоматического удаления инфицированных файлов необходимо выбрать «Удалить» в описываемом диалоговом окне. В некоторых случаях может являться целесообразным изменение режима обработки при работе монитора. Для этого используется пункт «Дополнительный запрос». Пункт «Сохранять копию в Карантин» включает сохранение копий инфицированных (подозрительный) файлов в Карантин. Ползунок «Экспертный анализ» позволяет включить поиск неизвестных вирусов при обработке объектов. Положение «Оптимален» (рекомендуется при обработке объектов) позволяет обнаружить неизвестные вирусы, принадлежащие к известным семействам. Положение «Максимален» позволяет обнаружить неизвестные вирусы, использующие разновидности известных вирусных алгоритмов. Положение «Избыточен» позволяет обнаруживать максимальное число неизвестных вредоносных программ при большей вероятности ложных срабатываний.

Вкладка «Отчет» (рис. 20) позволяет назначить параметры файла отчета и его имя.

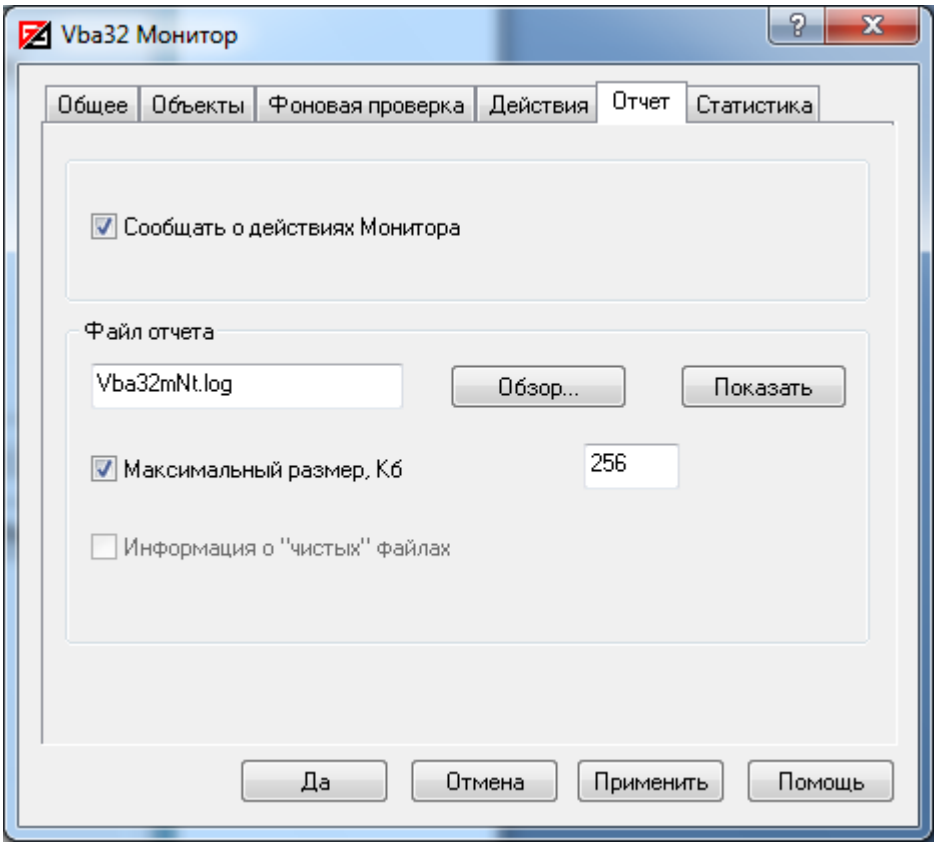

Рис. 20

Пункт «Сообщать о действиях монитора» позволяет выводить окно (рис. 21) с сообщениями о действиях монитора при обнаружении инфицированных объектов.

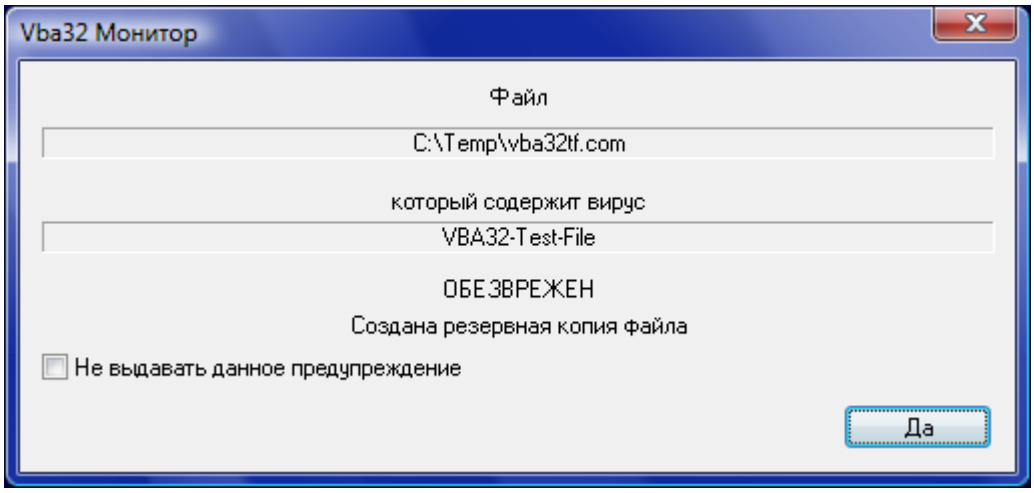

Рис. 21

Пункт «Вести» задает режим, при котором результаты антивирусной обработки сохраняются в виде файла на диске. Имя файла указывается в расположенной рядом строке ввода. Кнопка «Обзор» вызывает окно, аналогичное окну «Открыть» Windows. В обычном режиме работы файл отчета переписывается в каждом сеансе обработки. Пункт «Дописывать» позволяет продолжать файл отчета при следующих сеансах антивирусной обработки объектов. В окне,

расположенном рядом с пунктом «Максимальный размер, Кб», указывается наибольший размер файла, содержащего отчет об антивирусной обработке объектов. Пункт «Информация о «чистых» файлах» позволяет включать в файл отчета информацию о чистых файлах.

Вкладка «Статистика» (рис. 22) позволяет просмотреть результаты работы программы. В нем отображается количество обработанных, подозрительных, инфицированных, обезвреженных, удаленных, перемещенных и заблокированных файлов. Кроме того, выводится имя последнего обработанного и последнего инфицированного файлов, а также имя вируса, которым заражен последний инфицированный файл. Вышеупомянутые имена можно скопировать в буфер обмена для дальнейшего использования. В последней строке выводится информация о времени начала работы монитора. Кнопка «Сбросить» позволяет начать сбор статистики заново.

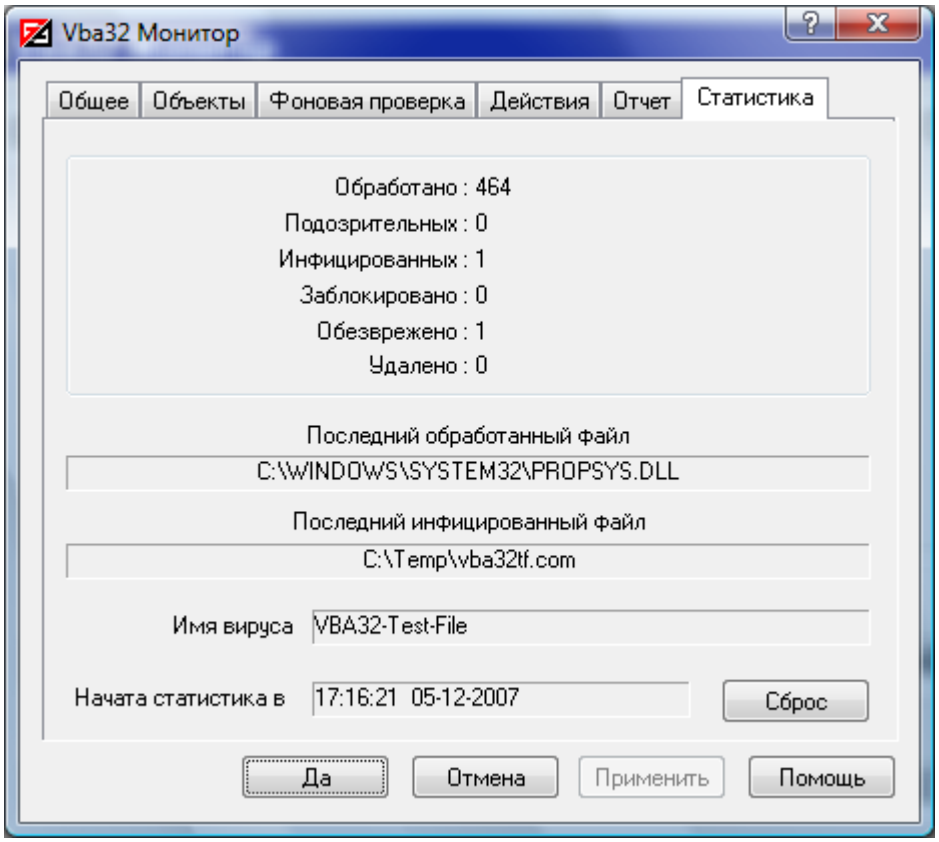

Рис. 22

3.1.4. SendLogs

Утилита SendLogs предназначена для сбора технической информации и файлов отчёта всех компонентов Vba32 с последующей их отправкой специалистам ОДО «ВирусБлокАда» либо сохранением на диск.

Утилита Send Logs поставляется со всеми комплектациями программы.

Она может быть запущена одним из следующих способов:

1. Перейдите в папку, куда установлен комплекс, и запустите файл SendLogs.exe;

2. Открыть главное окно Диспетчера, На закладке «Общее» нажать на ссылку «Поддержка». Затем в появившемся диалоговом окне «Поддержка» (рис. 23) нажать кнопку «Обратиться за поддержкой».

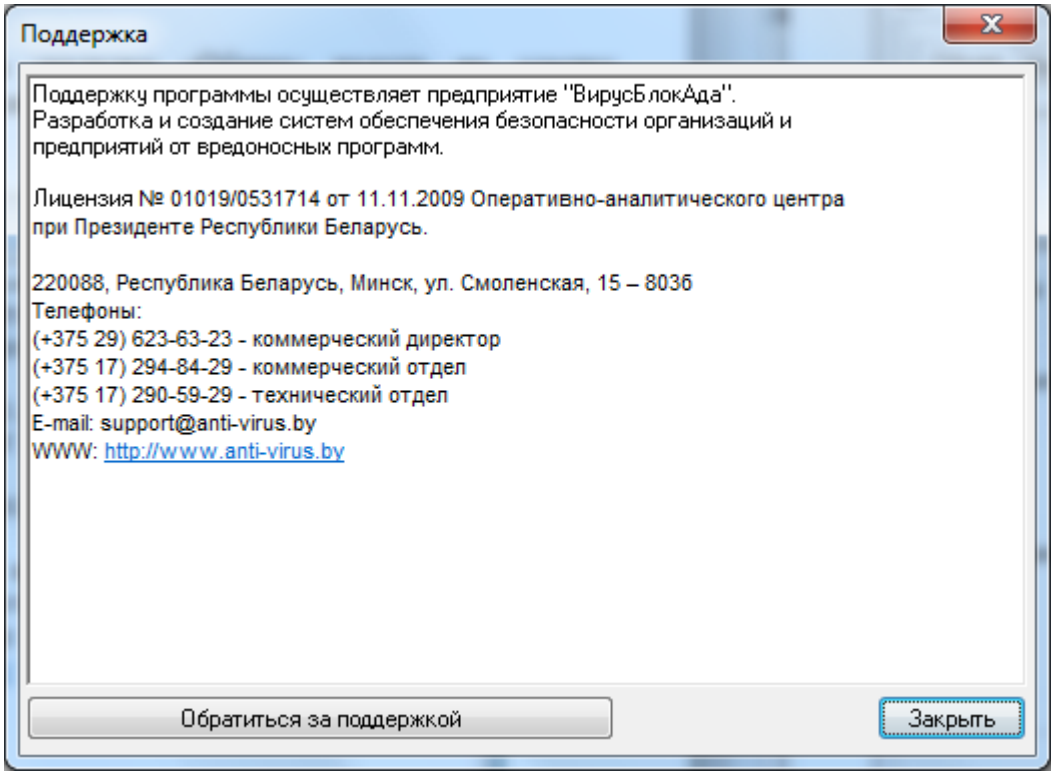

Рис. 23

После этого запустится главное окно SendLogs (рис. 24).

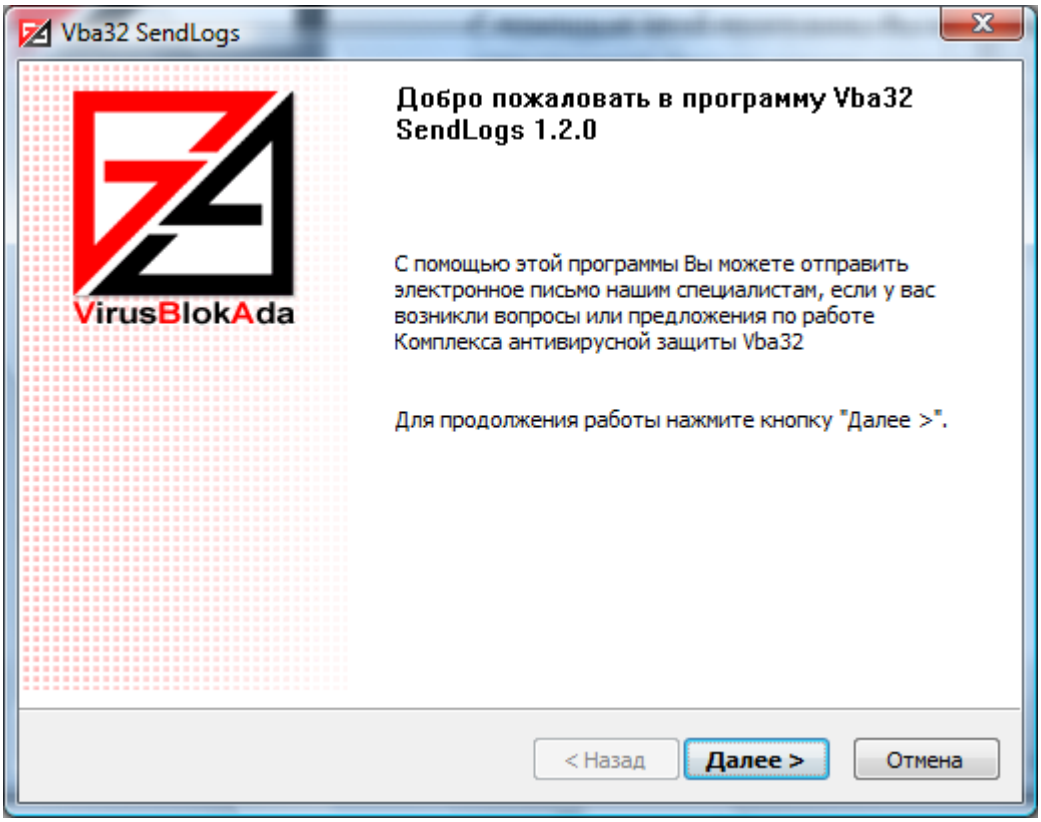

Рис. 24

3. Вызвать в панели задач контекстное меню Диспетчера. Выбрать пункт «Поддержка». Затем в появившемся диалоговом окне «Поддержка» (рис. 23) нажать кнопку «Обратиться за поддержкой». После этого запустится главное окно SendLogs.

Главное окно SendLogs содержит ее краткое описание. Для продолжения работы необходимо нажать «Далее». Для завершения работы – «Отмена».

После нажатия кнопки «Далее» загружается окно «Сбор файлов отчета» (рис. 25).

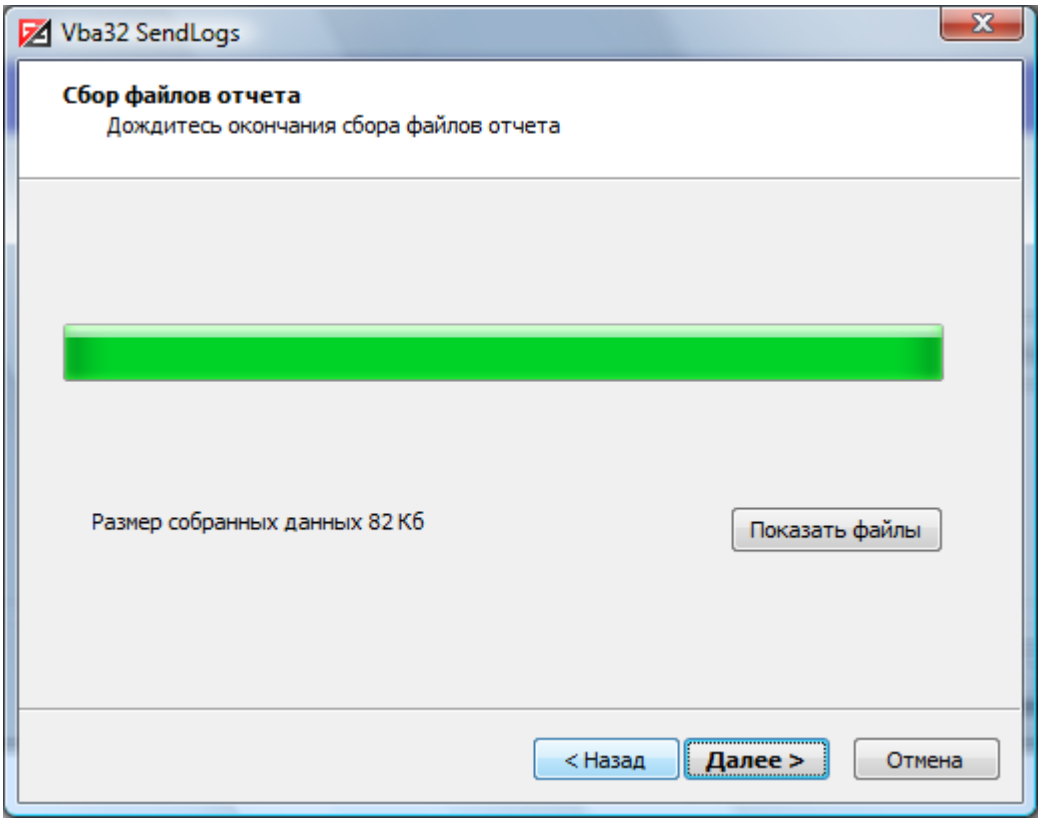

Рис. 25

Диалоговое окно «Сбор файлов отчёта» содержит индикатор состояния процесса сбора файлов, кнопку «Показать файлы», нажатие на которой открывает диалоговое окно со списком файлов, подготовленных к отправке, а также размер отсылаемого вложения.

Нажатие на кнопку «Назад» возвращает на предыдущий шаг. Нажатие на кнопку «Далее» переходит к выполнению выбранного метода отправки (рис. 26). Кнопка «Отмена» служит для завершения работы утилиты.

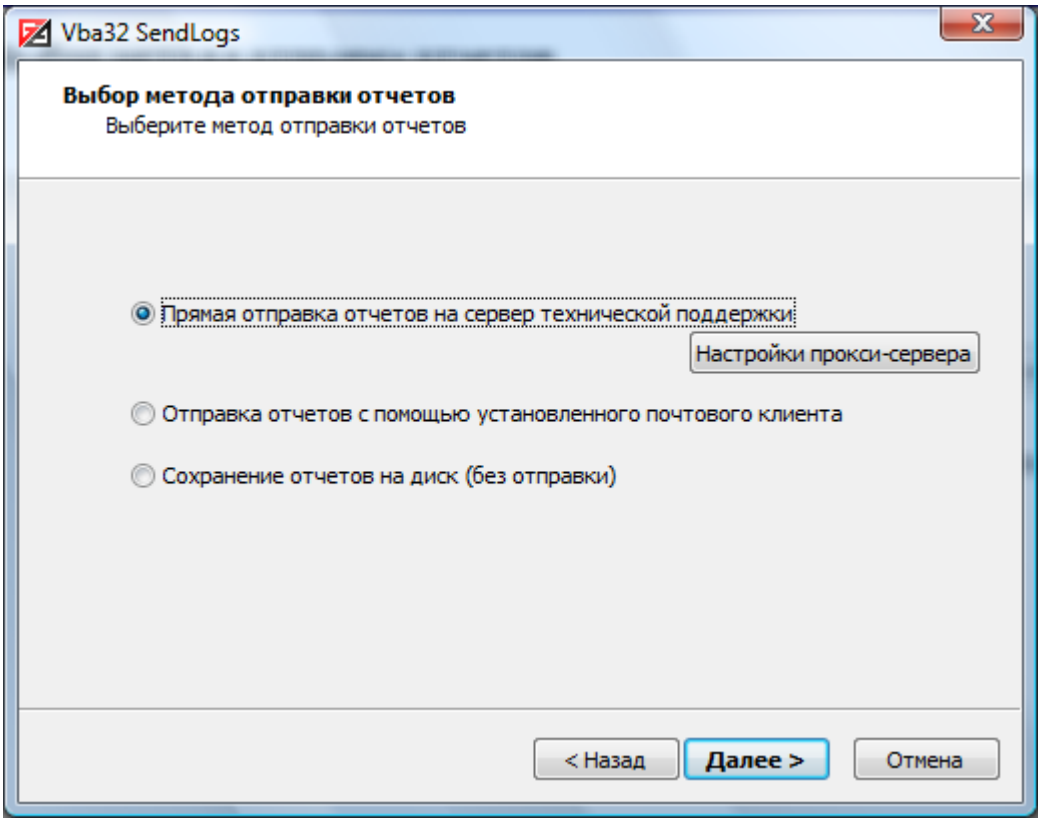

Рис. 26

Диалоговое окно «Выбор метода отправки» отчёта предлагает три варианта дальнейших действий:

– прямая отправка отчетов на сервер технической поддержки;
– отправка отчетов с помощью установленного почтового клиента;
– сохранение отчетов на диск (без отправки).

Пункт «Прямая отправка отчетов на сервер технической поддержки» предназначен для отправки файлов в службу технической поддержки прямо из утилиты SendLogs с использованием протокола SMTP. Если выбран данный способ отправки, то появляется диалоговое окно «Ввод данных» (рис. 27), содержащее текстовые поля для ввода адреса, на который будет прислан ответ на пользовательский запрос, темы письма и сути вопроса, который возник у пользователя. Также диалоговое окно поддерживает технологию «drag and drop», что позволяет добавлять файлы, которые будут присоединены к письму, путём их перетаскивания на диалоговое окно (по умолчанию единственным вложением является архив с файлами отчёта Vba32Logs.zip).

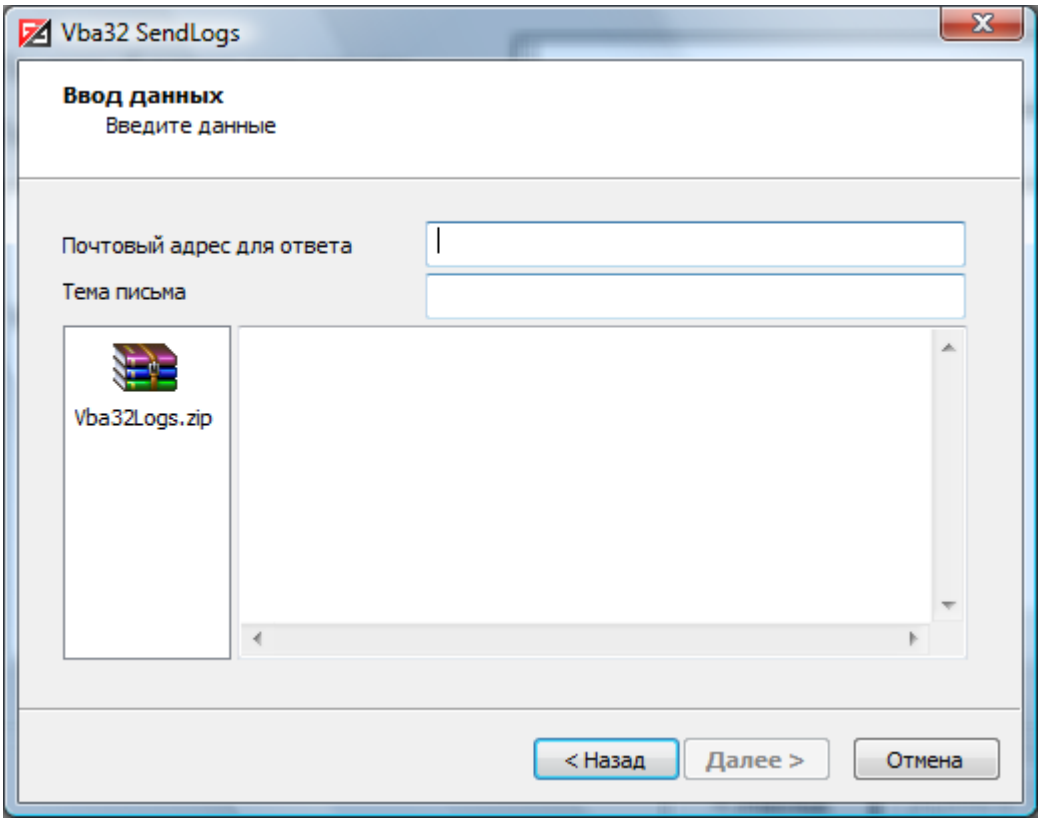

Рис. 27

Пункт «Отправка отчетов с помощью установленного почтового клиента» создаст электронное письмо и вызовет установленный почтовый клиент для отправки архива с файлами отчёта Vba32Logs.zip.

Пункт «Сохранение отчетов на диск (без отправки)» предназначен для помещения файлов в архив и сохранения на диск во временный каталог пользователя. После этого откроется окно Проводника Windows с папкой, содержащей архив Vba32Logs.zip.

Для выполнения одного из описанных выше действий необходимо выбрать один из этих пунктов и нажать на кнопку «Далее». Нажатие на кнопку «Назад» возвращает на предыдущий шаг. Кнопка «Отмена» служит для завершения работы утилиты.

После завершения метода отправки загружается диалоговое окно «Выполнение успешно завершено» (рис. 28). Для закрытия данного окна необходимо нажать кнопку «Готово».

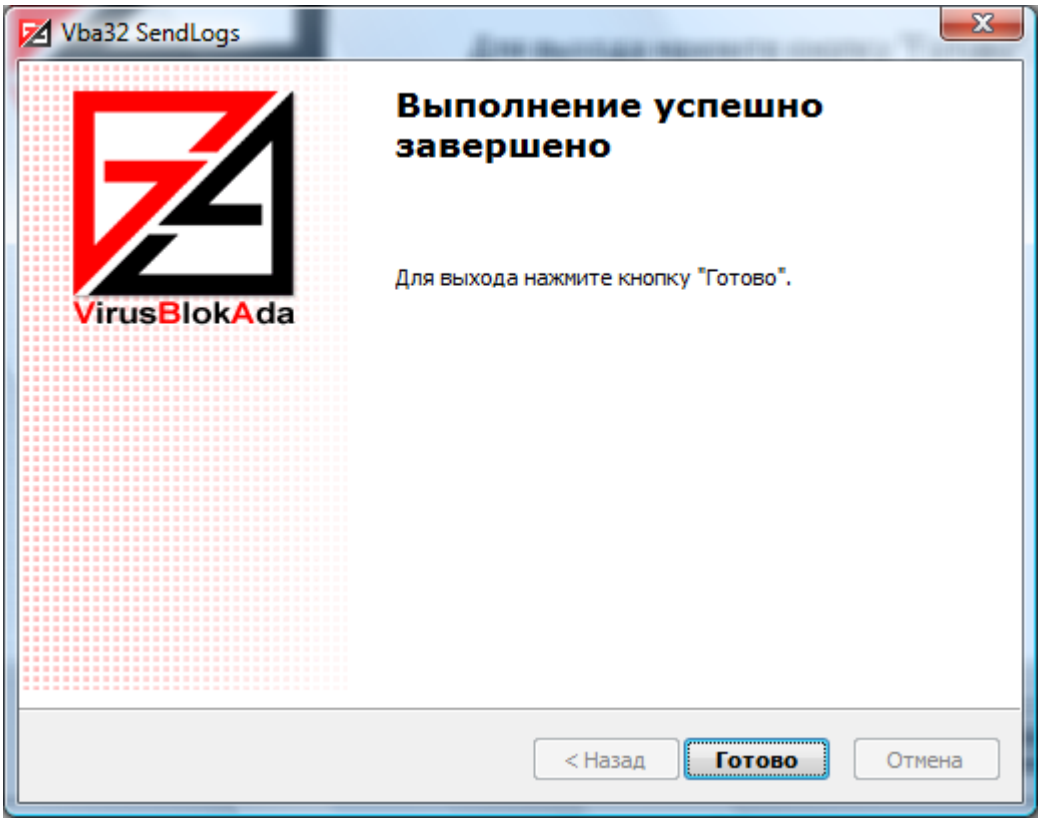

Рис. 28

3.1.5. Карантин

Карантин является компонентом комплекса Vba32 и обеспечивает хранение инфицированных и подозрительных файлов, помещенных в него антивирусными модулями.

При обнаружении инфицированных или подозрительных файлов антивирусом Vba32 выполняются действия, указанные в настройках программы. Если в настройках указана опция «Сохранять копию в Карантин», то перед каждым выполняемым действием копия файла будет помещаться в Карантин, а над файлом будут выполняться указанные действия. Также существует возможность добавить любой файл в Карантин вручную.

Карантин организует специальный каталог на Вашем компьютере, предназначенный для изоляции помещенных в него инфицированных и подозрительных файлов от остальной системы. Местоположение данного каталога можно изменить в настройках Карантина.

Карантин позволяет:

- добавлять в хранилище любой файл на компьютере;
- проводить неограниченное число повторных проверок хранимых файлов;
- удалять файлы из хранилища;
- отправлять файлы на антивирусный сервер Vba32 для детального анализа;
- извлекать файлы по указанному пути;
- восстанавливать файлы на прежнее место.

Чтобы открыть главное окно Карантина необходимо выбрать соответствующий пункт в контекстном меню иконки Диспетчера в панели задач (рис. 29).

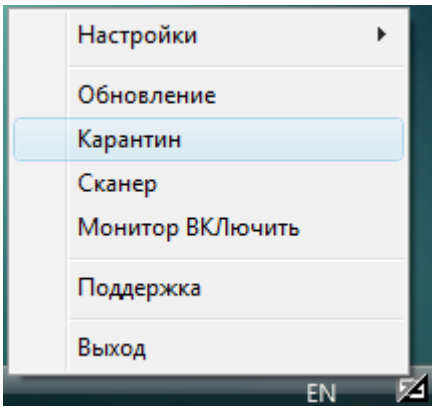

Рис. 29

Главное окно Карантина содержит две закладки:

– файловый карантин;

– почтовый карантин.

В файловый карантин (рис. 30) объекты помещаются пользователем, Монитором и Сканером.

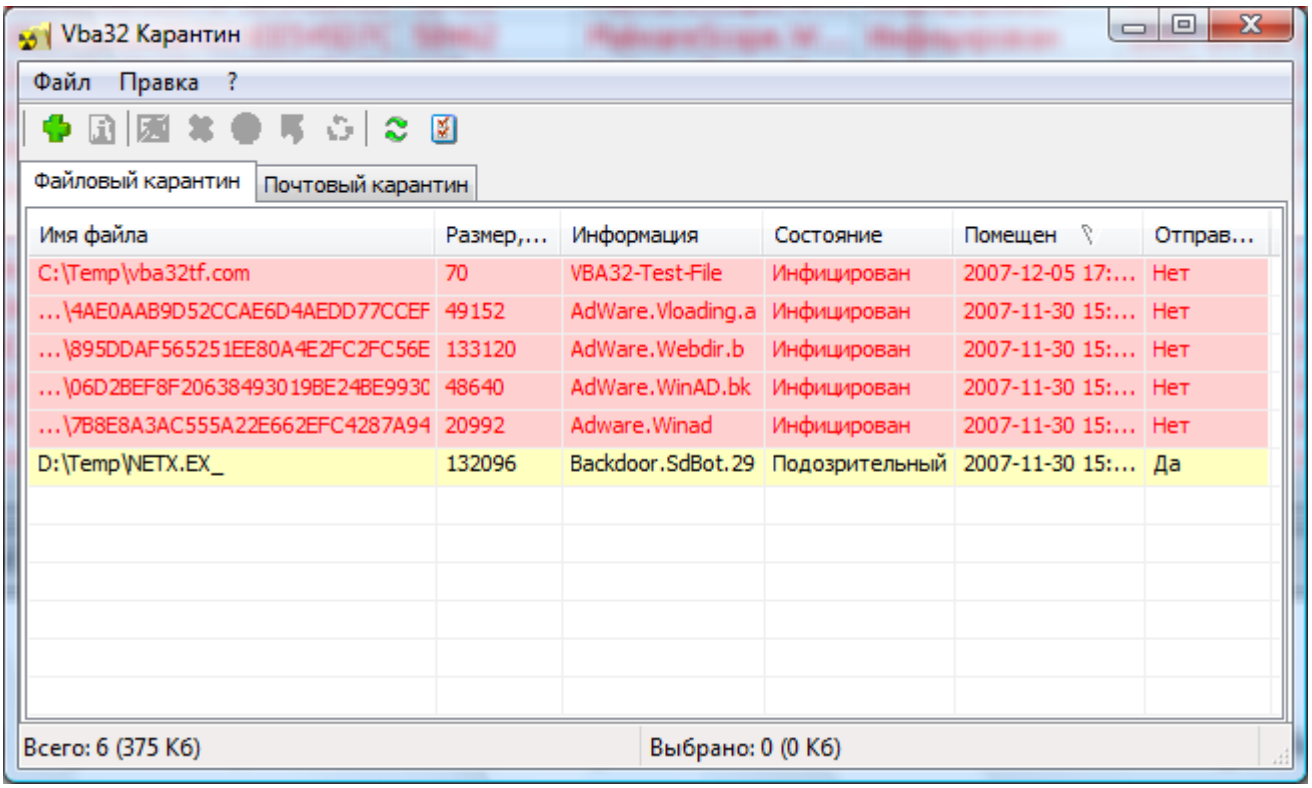

Рис. 30

Почтовый карантин (рис. 31) получает объекты от Почтового фильтра и Outlook-модуля.

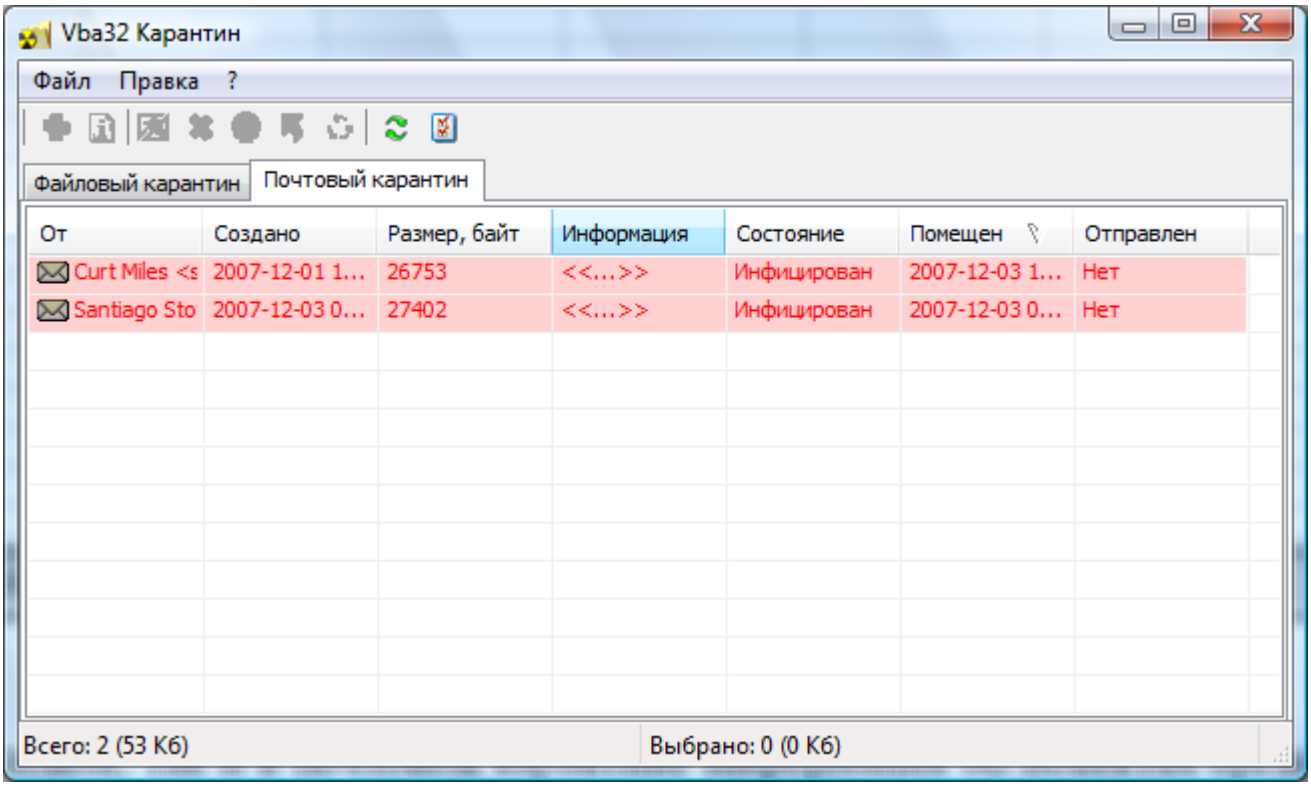

Рис. 31

Как в файловом, так и в почтовом карантине информация об объектах организована в виде таблицы со следующими столбцами:

– «Имя файла» - полное имя файла, помещенного в Карантин;

– «Размер, байт» - оригинальный размер файла;

– «Информация» - различные сведения о файле;

– «Состояние» - информация о текущем состоянии файла в Карантине. Файл может быть «Инфицирован», «Подозрительный» или «Чистый». Состояние файла может быть «Неопределено», если файл был добавлен вручную и его проверка ранее не проводилась;

– «Дата/время» - дата и время помещения файла в Карантин;

– «Отправлен» - статус отправки файла для детального анализа на сервер компании ОДО «ВирусБлокАда».

Настройки Карантина (рис. 32) позволяют определить путь для хранения файлов Карантина на компьютере, выбрать один из серверов компании ОДО «ВирусБлокАда» для отправки файлов на анализ, указать прокси-сервер, используемый для доступа в Internet, установить параметры и период автоматического обслуживания Карантина.

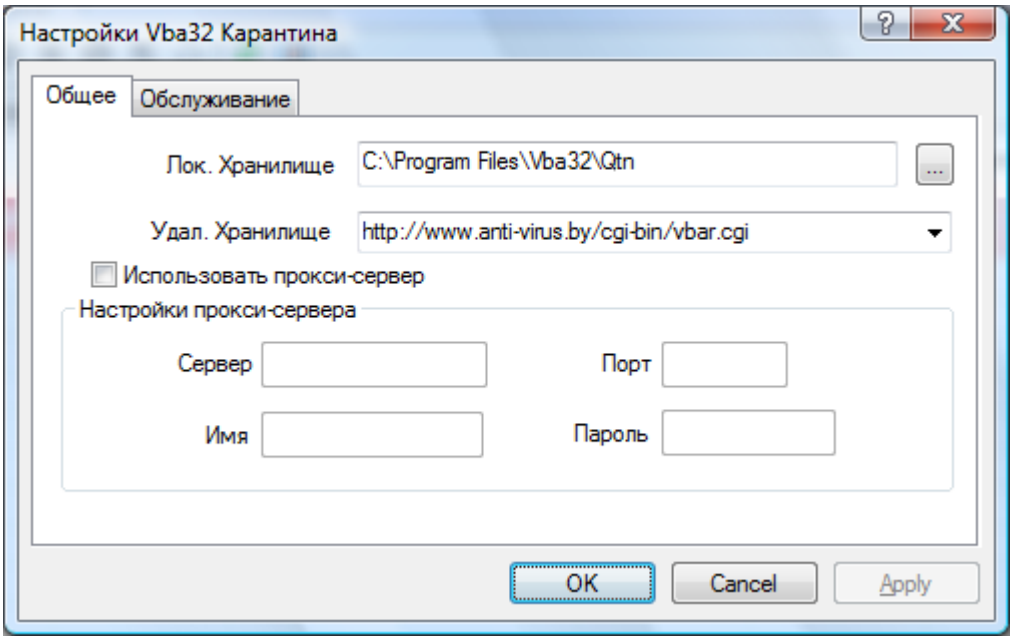

Рис. 32

Чтобы открыть окно настроек Карантина нужно:

– открыть главное окно Карантина;

– выбрать пункт меню «Правка»;

– в открывшемся меню выбирать пункт «Настройки...» или нажать кнопку «Настройки» на панели инструментов.

Окно настроек Карантина содержит следующие закладки:

– «Общее»;

– «Обслуживание».

На закладке «Общее» окна настроек Карантина выполняется выбор пути для хранения файлов в Карантине, пути для отправки файлов на анализ, а также настройки использования прокси-сервера.

Пункт «Локальное хранилище» представляет собой путь для хранения файлов в Карантине на компьютере.

Пункт «Удаленное хранилище» представляет собой путь к серверу компании ОДО «ВирусБлокАда» для отправки файлов на анализ.

Пункт «Использовать прокси-сервер» включает использование прокси-сервера для доступа к удаленному хранилищу.

Пункт «Сервер» представляет собой адрес прокси-сервера.

Пункт «Порт» - порт прокси-сервера.

Пункт «Имя» - имя пользователя для доступа к прокси-серверу.

Пункт «Пароль» - пароль пользователя для доступа к прокси-серверу.

Кнопка «Применить» предназначена для сохранения настроек. Кнопка «Да» предназначена для сохранения внесенных изменений и закрытия окна настроек. Кнопка «Отмена» предназначена для закрытия окна настроек без сохранения внесенных изменений.

На закладке «Обслуживание» (рис. 33) окна настроек Карантина выполняется настройка параметров хранения и обслуживания файлов в Карантине.

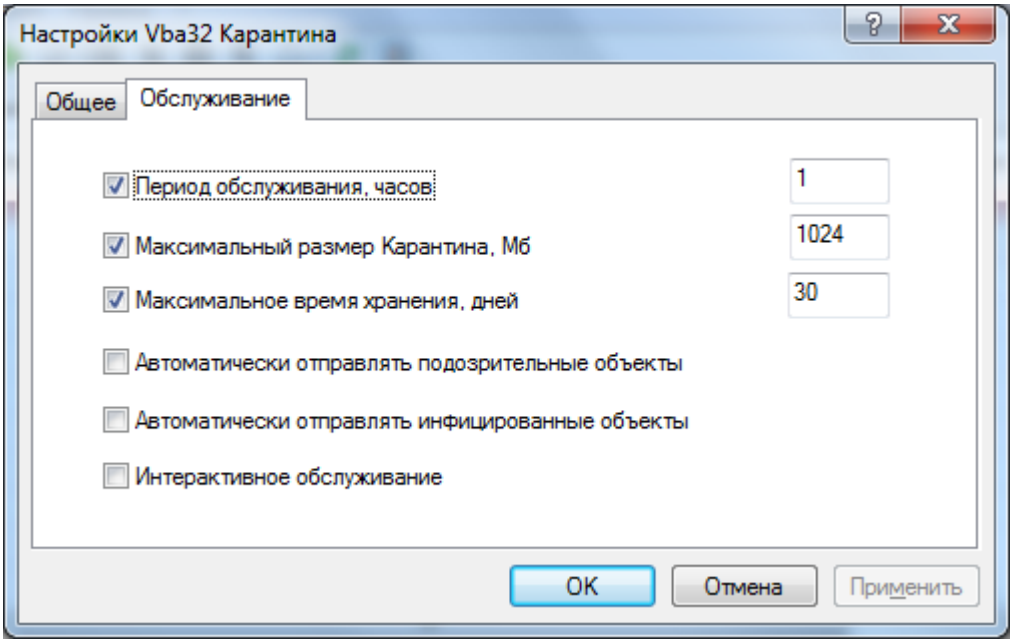

Рис. 33

Пункт «Период обслуживания, часов» устанавливает режим автоматического обслуживания файлов в Карантине. Сеансы обслуживания будут проводиться через указанные промежутки времени.

Пункт «Максимальный размер Карантина, Мб» включает ограничение максимального размера дискового пространства, используемого для хранения файлов в Карантине. После превышения указанного максимального размера в каждом сеансе обслуживания будет происходить удаления наиболее ранних файлов, пока размер Карантина не уменьшится до установленного максимального размера.

Пункт «Максимальное время хранения, дней» устанавливает максимальное время хранения файлов в Карантине. В каждом сеансе обслуживания все файлы, хранящиеся в Карантине дольше указанного времени, будут автоматически удаляться.

Пункт «Автоматически отправлять подозрительные объекты» включает автоматическую отправку подозрительных файлов для детального анализа на сервер компании ОДО «ВирусБлокАда», указанный на закладке «Общее».

Пункт «Интерактивное обслуживание» включает отображение во время обслуживания значка. Нажатие на ней вызывает диалоговое окно «Обслуживание карантина», которое показывает статус выполняемых в данный момент действий по обслуживанию Карантина.

Кнопка «Применить» предназначена для сохранения настроек. Кнопка «Да» предназначена для сохранения внесенных изменений и закрытия окна настроек. Кнопка «Отмена» предназначена для закрытия окна настроек без сохранения внесенных изменений.

Вы можете выполнять различные действия над файлами, хранящимися в Карантине. Для этого выделите файлы в списке и выберите необходимое действие. Действия можно выбирать

либо на панели инструментов, либо из контекстного меню (щелкнув правой кнопкой мыши по выбранным файлам). Действия применяются ко всем выделенным файлам.

Для работы с файлами в Карантине предназначены следующие действия:

– «Добавить» - позволяет добавлять в хранилище любой файл на компьютере;

– «Проверить» - позволяет проводить повторную проверку хранимых файлов;

– «Удалить» - позволяет удалять файлы из хранилища;

– «Отправить» - позволяет отправлять файлы на антивирусный сервер Vba32 для детального анализа;

– «Извлечь» - позволяет извлекать файлы по указанному пути;

– «Восстановить» - позволяет восстанавливать файлы на прежнее место;

Чтобы добавить один или несколько файлов в Карантин необходимо:

– Открыть Главное окно Карантина;

– Выбрать пункт меню «Файл»;

– В открывшемся меню выбирать пункт «Добавить...»;

– В открывшемся стандартном диалоге открытия файлов нужно выделить требуемые файлы и нажать кнопку «Открыть»;

– Затем нужно дождаться завершения процесса добавления.

Карантин позволяет проводить повторные проверки файлов, хранящихся в нем. Например, после обновления комплекса Vba32 некоторые ложные срабатывания могут быть исправлены, поэтому файлы, помещенные в Карантин как подозрительные, могут быть безопасно восстановлены.

Чтобы проверить один или несколько файлов в Карантине необходимо проделать следующие действия:

– открыть Главное окно Карантина;

– выделить файлы, предназначенные для проверки;

– выбрать пункт меню «Проверить...» в контекстном меню главного окна Карантина или нажать кнопку «Проверить» на панели инструментов;

– в открывшемся диалоге «Проверка» (рис. 34) отображаются выбранные для проверки файлы. Для открытия диалога «Настройки проверки» необходимо нажать кнопку «Настройки» (рис. 35). Для запуска процесса проверки выбранных файлов необходимо нажать кнопку «Проверить»;

– необходимо дождаться завершения процесса проверки;

– нажать «Закрыть» для закрытия диалога проверки файлов.

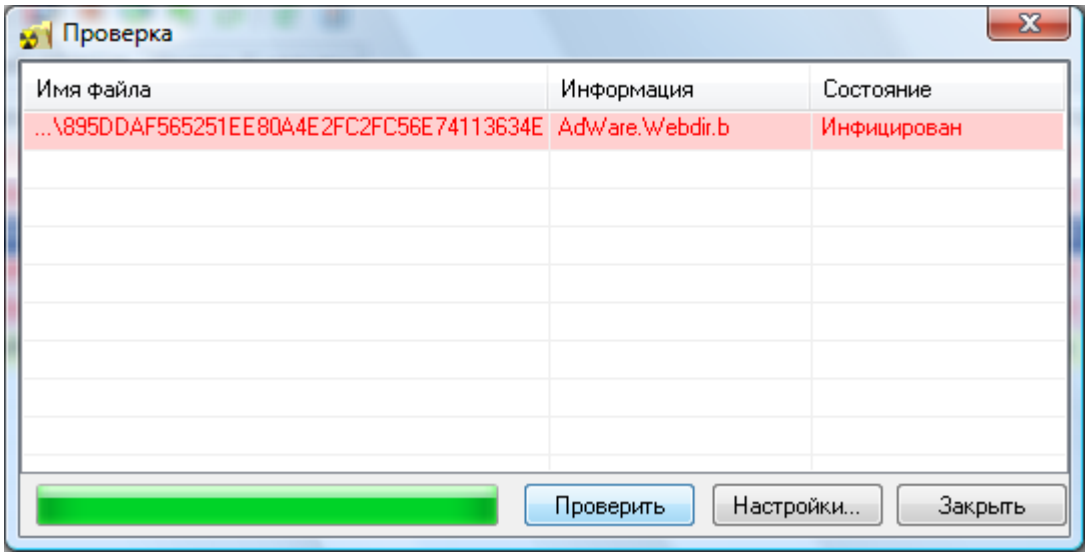

Рис. 34

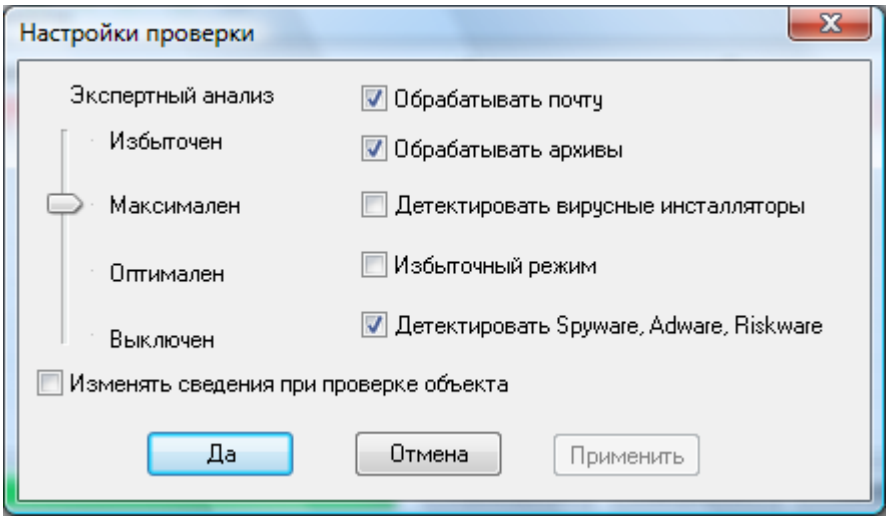

Рис. 35

Настройки проверки позволяют изменить параметры обработки файлов, выбранных для проверки.

Пункт «Экспертный анализ» позволяет обнаруживать неизвестные вредоносные программы и модификации известных вредоносных программ, что позволяет обеспечить более надежную защиту компьютера. Можно выбрать различный уровень экспертного анализа:

– «Выключен» - при выключенном экспертном анализе неизвестные вредоносные программы обнаружены не будут;

– «Оптимален» - данный уровень экспертного анализа оптимально подобран разработчиками. Он позволяет осуществлять детектирование неизвестных вредоносных программ и практически не снижает скорость обработки;

– «Максимален» - обеспечивает максимальный уровень детектирования неизвестных вредоносных программ при минимальном количестве ложных срабатываний, но несколько снижает скорость обработки;

– «Избыточен» - обнаруживает максимальное количество неизвестных вредоносных программ при большей вероятности ложных срабатываний. Рекомендуется только для опытных пользователей.

Пункт «Обрабатывать почту» устанавливает режим, при котором будут обрабатываться все файлы почтовых форматов.

Пункт «Детектировать вирусные инсталляторы» устанавливает режим детектирования инсталляторов вредоносных программ.

Пункт «Обрабатывать архивы» устанавливает режим, при котором будут обрабатываться все заархивированные файлы.

Пункт «Избыточный режим» устанавливает избыточный режим обработки файлов.

Пункт «Детектировать Spyware, Adware, Riskware» устанавливает дополнительный режим, при котором перестанут игнорироваться приложения класса Adware и Riskware. Они будут расцениваться как инфицированные.

Пункт «Изменять сведения при проверке объекта» разрешает изменение сведений о файле в колонке «Сведения» главного окна Карантина.

Для сохранения настроек в окне «Настройки проверки» необходимо нажать на кнопку «Применить». Для сохранения внесенных изменений и закрытия окна настроек необходимо нажать кнопку «Да». Для закрытия окна настроек без сохранения внесенных изменений необходимо нажать кнопку «Отмена».

Существует возможность удалять файлы из Карантина.

Чтобы удалить один или несколько файлов из Карантина необходимо проделать следующие действия:

– Открыть Главное окно Карантина;

– Выделить файлы, предназначенные для удаления;

– Выбрать пункт меню «Удалить...» из контекстного меню главного окна Карантина или нажать кнопку «Удалить» на панели инструментов;

– Нажать «Да» для подтверждения удаления файлов;

– Дождаться завершения процесса удаления.

При помощи Карантина можно отправить избранные файлы (рис. 36) из него на специальный сервер компании ОДО «ВирусБлокАда» для детального анализа. Эту возможность нужно использовать только при необходимости, например:

– Инфицированный файл был помещен в Карантин Сканером или Монитором, потому что не удалось его обезвредить;

– Неизвестный файл был получен по электронной почте и помещен в Карантин;

– Файл был помещен в Карантин в результате ложного срабатывания.

При отправке необходимо указать точный адрес электронной почты для обратной связи. В поле для примечаний нужно внести как можно больше полезной информации: версию операционной системы, установленные сервисные пакеты, версию антивирусного комплекса Vba32, дату последнего обновления, причину отправки файлов.

Чтобы отправить один или несколько файлов из Карантина для детального анализа необходимо проделать следующие действия:

– открыть Главное окно Карантина;

– выделить файлы, предназначенные для отправки;

– выбрать пункт меню «Отправить...» из контекстного меню главного окна Карантина или нажать кнопку «Отправить» на панели инструментов;

– в открывшемся диалоге «Отправка объекта» (рис. 36) можно видеть выбранные для отправки файлы;

– указать адрес электронной почты для обратной связи;

– в поле «Примечание» ввести детальное описание отправляемых данных;

– нажать «Отправить» для запуска процесса отправки файлов;

– дождаться завершения процесса отправки;

– нажать «Закрыть» для отмены отправки и закрытия диалога.

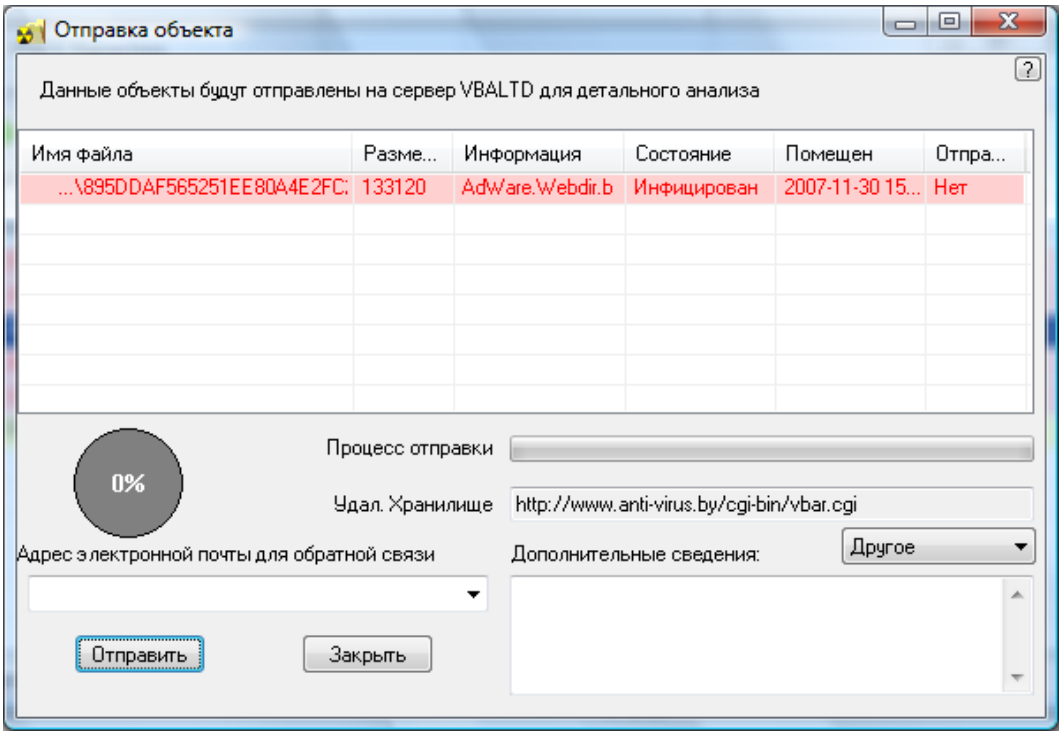

Рис. 36

Чтобы извлечь один или несколько файлов из Карантина:

– открыть Главное окно Карантина;

– выделить файлы, предназначенные для извлечения;

– выбрать пункт меню «Извлечь в...» в контекстном меню главного окна Карантина или нажать кнопку «Извлечь» на панели инструментов;

– в открывшемся стандартном диалоге «Обзор папок» (рис. 37) необходимо выбрать требуемую папку, либо создать новую и нажать кнопку ОК;

– дождаться завершения процесса извлечения.

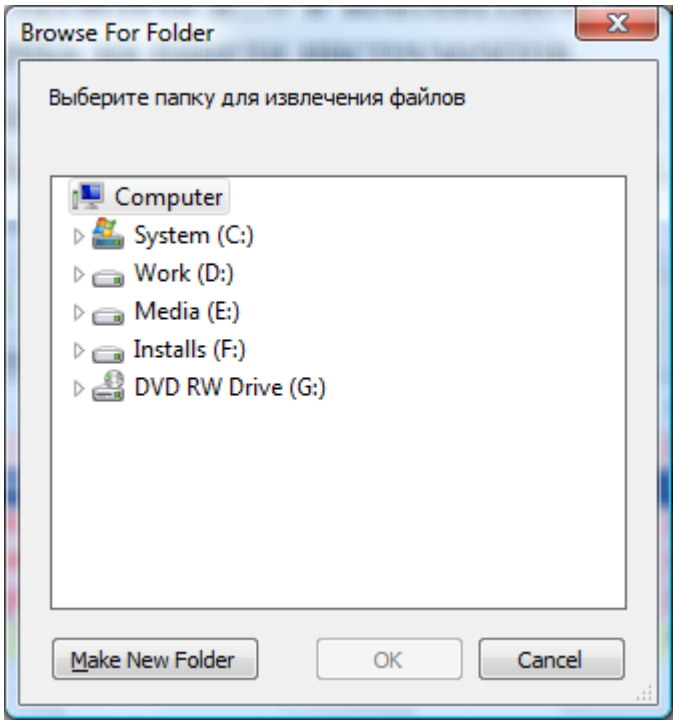

Рис. 37

Восстановление файлов позволяет возвращать файлы, ранее помещенные в Карантин, на прежнее место в системе.

Чтобы восстановить один или несколько файлов из Карантина необходимо проделать следующие действия:

– открыть Главное окно Карантина;

– выделить файлы, предназначенные для восстановления;

– выбрать пункт меню «Восстановить...» в контекстном меню главного окна Карантина или нажать кнопку «Восстановить» на панели инструментов;

– нажать «Да» для подтверждения восстановления файлов;

– дождаться завершения процесса восстановления. Для отмены процесса восстановления файлов нажать «Прервать».

3.1.6. Расширение контекстного меню «Проводника»

Расширение контекстного меню «Проводника» позволяет проводить обработку отдельных файлов и каталогов без запуска Сканера. Для запуска обработки необходимо установить курсор мыши на имени выбранного объекта, щелкнуть правой кнопкой мыши и в открывшемся контекстном меню Windows выбрать пункт «Scan by Vba32» (рис. 38).

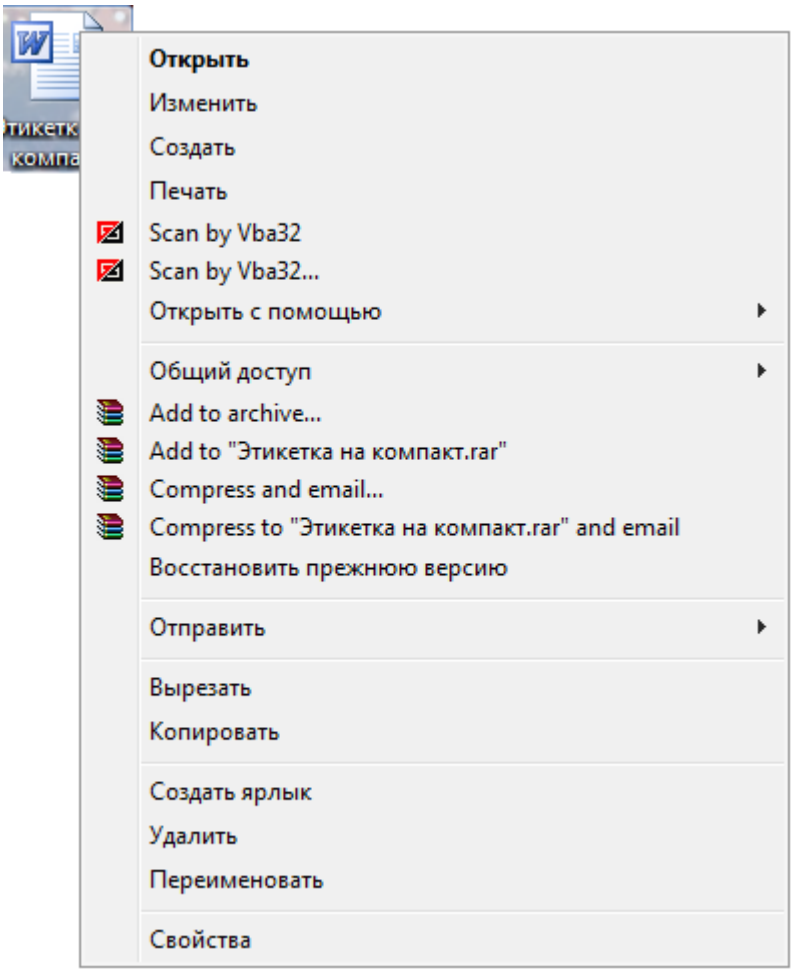

Рис. 38

В появившемся окне результатов обработки (рис. 39) будет отображаться процесс выполнения обработки.

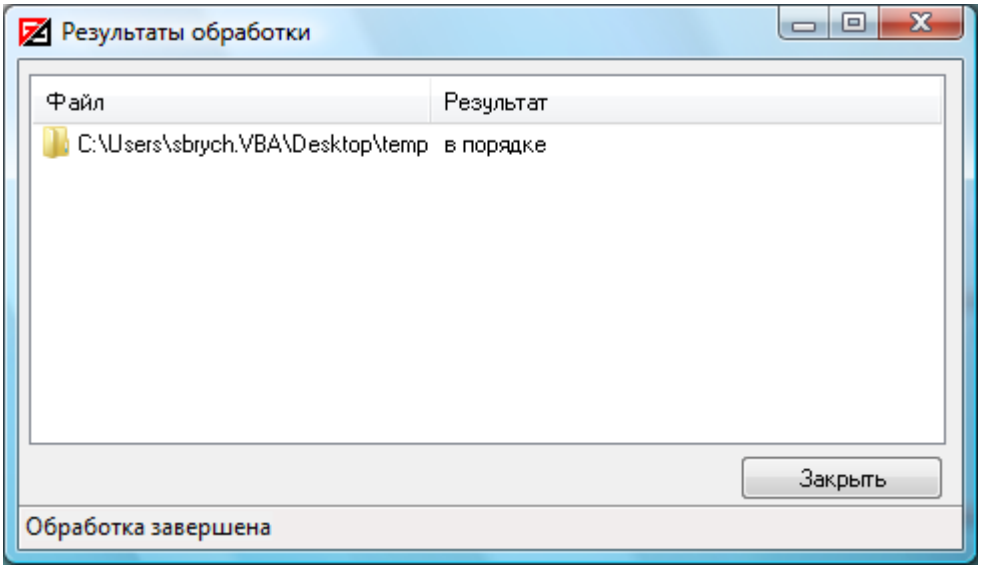

Рис. 39

Обработка в данном случае будет выполняться с настройками по умолчанию.

Для запуска обработки с параметрами необходимо установить курсор мыши на имени выбранного объекта, щелкнуть правой кнопкой мыши и в открывшемся контекстном меню Windows и выбрать пункт «Scan by Vba32...».

В появившемся диалоговом окне «Настройки обработки» (рис. 40) будет предложено выбрать параметры обработки.

Пункт «Инфицированный файл» позволяет выбрать в выпадающем списке действие над инфицированными файлами:

– «Пропустить» - инфицированный файл пропускается, никаких действий не предпринимается;

– «Обезвредить» - инфицированные файлы обезвреживаются;

– «Удалить» - инфицированный файл удаляется из системы;

– пункт «При невозможности» позволяет выбрать в выпадающем списке действие над инфицированными файлами в случае, если невозможно выполнить действие, указанное в выпадающем списке выше;

– «Пропустить» - инфицированный файл пропускается;

– «Удалить» - инфицированный файл удаляется.

Пункт «Избыточный режим» устанавливает избыточный режим обработки файлов.

Пункт «Обрабатывать почту» устанавливает режим, при котором Сканер обрабатывает все файлы почтовой системы.

Пункт «Детектировать вирусные инсталляторы» устанавливает режим, при котором Сканер обрабатывает инсталляторы.

Пункт «Обрабатывать архивы» устанавливает режим, при котором Сканер обрабатывает все заархивированные файлы.

Пункт «Отображать макросы в документах» устанавливает дополнительную опцию, позволяющую отображать в окне отчёта при сканировании документов задействованные в данном документе макросы.

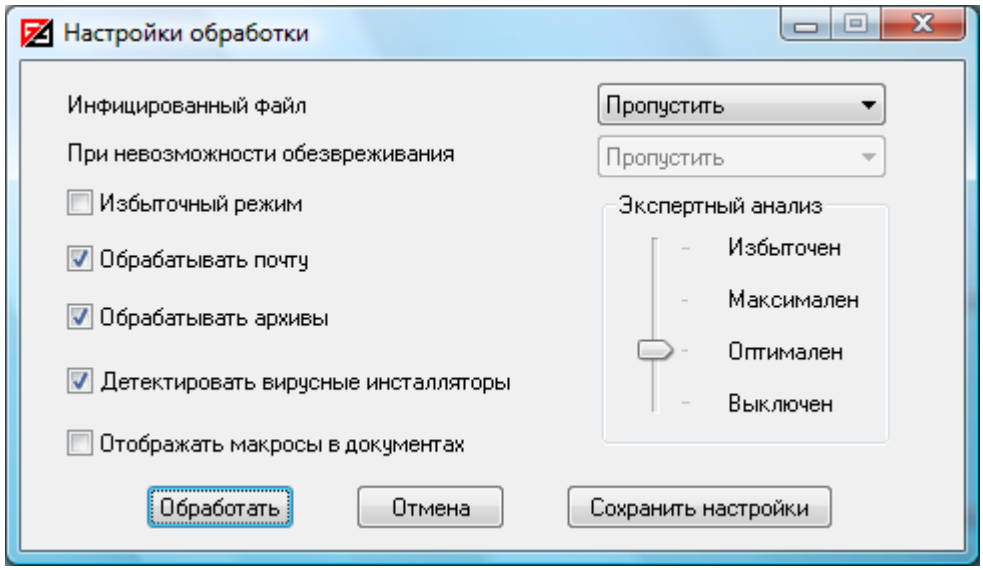

Рис. 40

Пункт «Экспертный анализ» позволяет обнаруживать неизвестные вредоносные программы и модификации известных вредоносных программ, что позволяет обеспечить более надежную защиту компьютера. Можно выбрать один из следующих уровней экспертного анализа:

– «Выключен» - при выключенном экспертном анализе неизвестные вредоносные программы обнаружены не будут;

– «Оптимален» - данный уровень экспертного анализа оптимально подобран разработчиками. Он позволяет осуществлять детектирование неизвестных вредоносных программ и практически не снижает скорость обработки;

– «Максимален» - обеспечивает максимальный уровень детектирования неизвестных вредоносных программ при минимальном количестве ложных срабатываний, но несколько снижает скорость обработки;

– «Избыточен» - обнаруживает максимальное количество неизвестных вредоносных программ при большей вероятности ложных срабатываний. Рекомендуется только для опытных пользователей.

Для запуска процесса обработки необходимо нажать «Обработать». Кнопка «Отмена» предназначена для закрытия окна «Настройки обработки». В этом случае обработка не будет выполнена. Кнопка «Сохранить настройки» предназначена для сохранения текущих настроек и установки данных настроек по умолчанию.

После запуска обработки появляется окно «Результаты обработки» (рис. 41), в котором отображается информация об обрабатываемых объектах и их состоянии после обработки. Существует возможность в любой момент прервать процесс обработки, нажав кнопку «Прервать». По окончании процесса обработки нужно нажать кнопку «Закрыть» для закрытия окна результатов обработки.

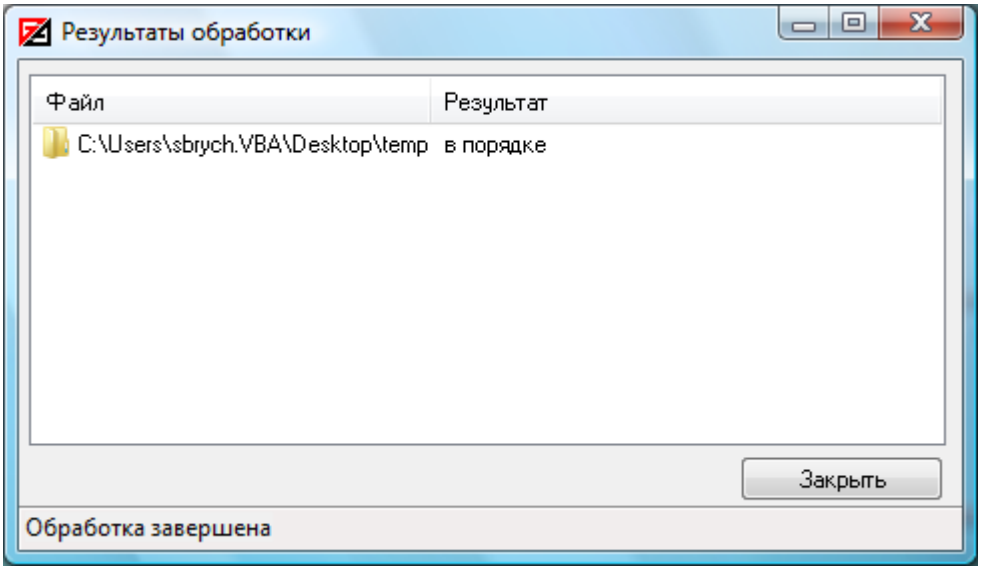

Рис. 41

3.1.7. Почтовый фильтр

Антивирусный Почтовый фильтр предназначен для фильтрации входящих почтовых сообщений.

Для вызова диалога настроек Почтового фильтра необходимо выбрать соответствующий пункт в выпадающем меню антивирусного Комплекса ОДО «ВирусБлокАда» (рис. 42).

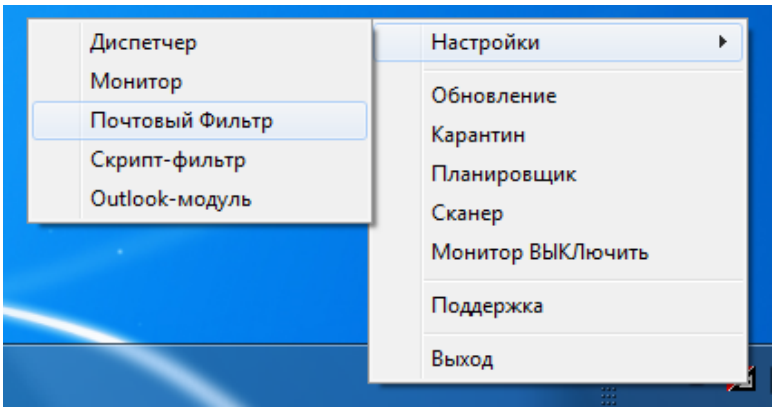

Рис. 42

Диалог конфигурации Почтового фильтра состоит из трех частей: «Объекты», «Перехват», «Статистика».

Первая закладка (рис. 43) диалога конфигурации позволяет выбрать режимы обработки объектов. На этой закладке имеется возможность отключить обработку сообщений, используя флаг «Обрабатывать почту». Здесь также можно указать действия над инфицированными и подозрительными сообщениями (перемещать, принимать и удалять), а так же, установив значение «сохранять копию в Карантин», помещать копии обработанных инфицированных писем в Карантин.

Для настройки уровня экспертного анализа используется ползунок, который может быть установлен в одну из позиций: «Выключен», «Оптимален», «Максимален», «Избыточен». В положение «Выключен» неизвестные вредоносные программы обнаружены не будут. Положение «Оптимален» позволяет осуществлять детектирование неизвестных вредоносных программ практически не снижает скорость обработки. Положение «Максимален» обеспечивает максимальный уровень детектирования неизвестных вредоносных программ при минимальном количестве ложных срабатываний, но несколько снижает скорость обработки. Положение «Избыточен» обеспечивает обнаружение максимального количества неизвестных вредоносных программ при большей вероятности ложных срабатываний. Рекомендуется только для опытных пользователей.

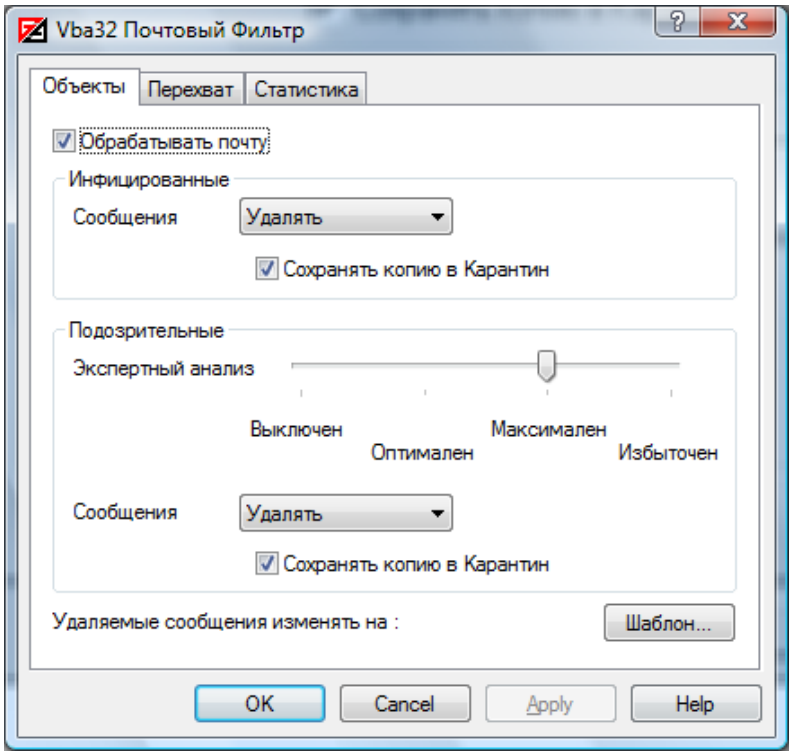

Рис. 43

В случае обнаружения и последующего перемещения/удаления сообщения с вирусом исходное сообщение заменяется на шаблон. Шаблон письма может формироваться пользователем после нажатия кнопки «Шаблон…» (рис. 44) на закладке «Объекты». При изменении текста и темы шаблона можно использовать следующие переменные:

– %action% - выполненное над инфицированным письмом действие;
– %from% - отправитель инфицированного письма;
– %subject% - тема инфицированного письма;
– %virlist% - вирусы, обнаруженные в письме.

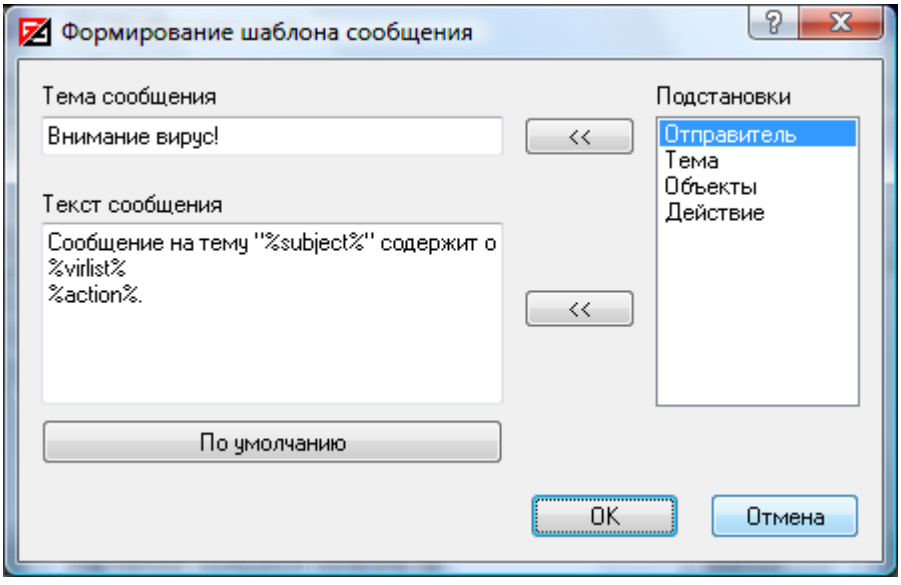

Рис. 44

Закладка «Перехват» (рис. 45) позволяет указать параметры соединений, которые будут обрабатываться фильтром. В соответствующие поля вводятся порт и адрес почтового сервера. В поле «Адрес сервера» можно указать «*», что означает обрабатывать соединения с любыми серверами по данному порту.

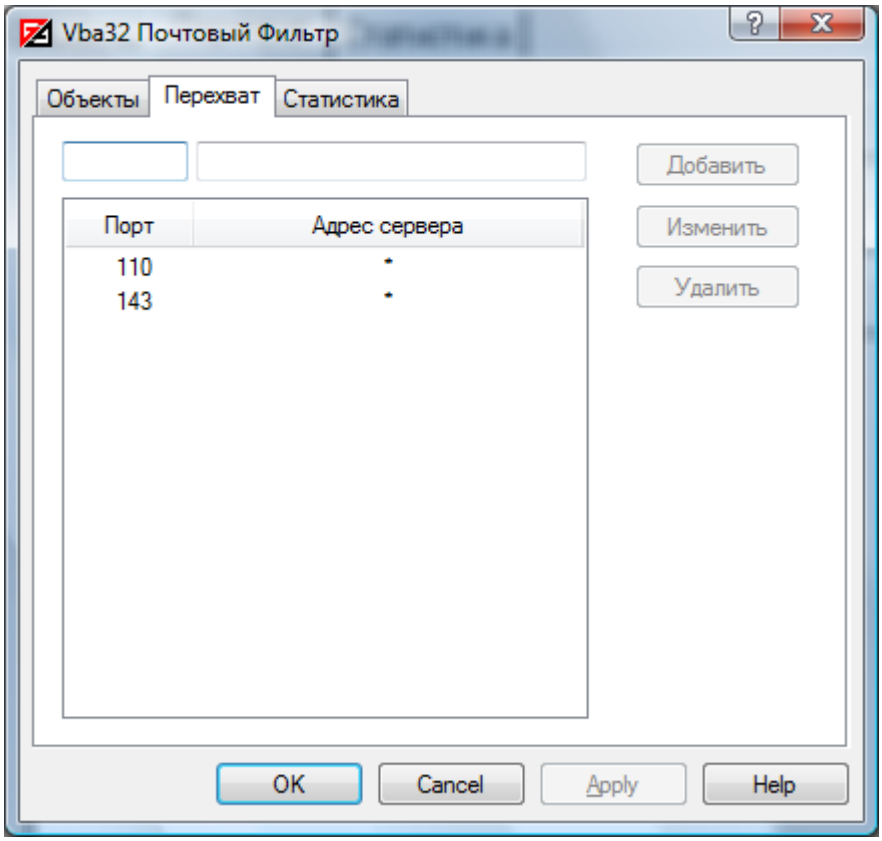

Рис. 45

Закладка «Статистика» (рис. 46) позволяет просмотреть результаты работы Почтового фильтра и настроить параметры ведения файла отчета. В статистике отображается информация об общем количестве обработанных сообщений, количестве инфицированных и подозрительных сообщений и произведенных над ними действиях. Кроме того, в данном окне выводятся имя вируса и время его обнаружения. Кнопка сброс позволяет обнулить статистику. Значение пунктов «Файл отчета» совпадает со значением аналогичных пунктов закладок «Статистика» для сканера и монитора.

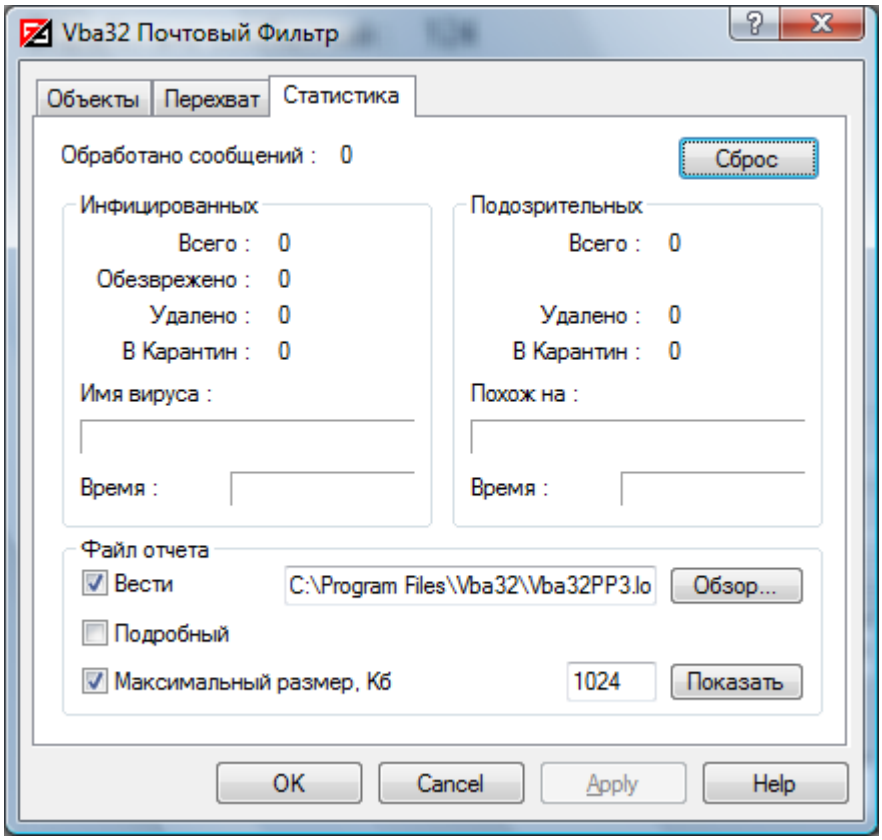

Рис. 46

3.1.8. Скрипт-фильтр

Скрипт-фильтр осуществляет антивирусную защиту Microsoft Internet Explorer и Microsoft Outlook Express, а также любых других приложений, использующих технологию Microsoft Windows Scripting Host (MS WSH).

Для вызова диалога настроек скрипт-фильтра необходимо выбрать соответствующий пункт в контекстном меню иконки Диспетчера в панели задач (рис. 47).

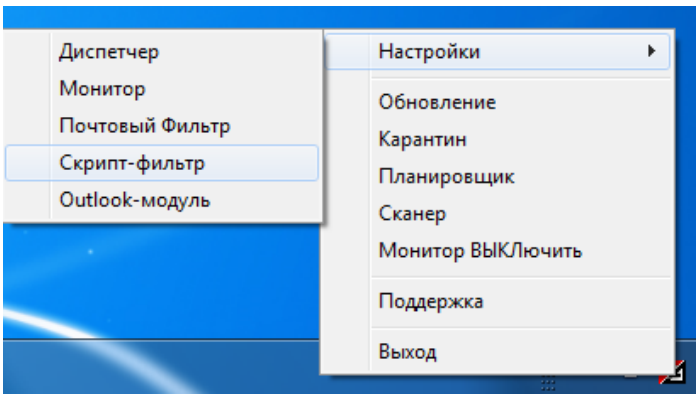

Рис. 47

Диалог настройки скрипт-фильтра (рис. 48) содержит следующие пункты:

– «Включить скрипт-фильтр»;
– «Сообщать о блокировке скриптов»;

№ изм.	*Подп.*	*Дата*

– «Файл отчета» – «Вести»;
– «Файл отчета» – «Подробный»;
– «Файл отчета» – «Максимальный размер, Кб».

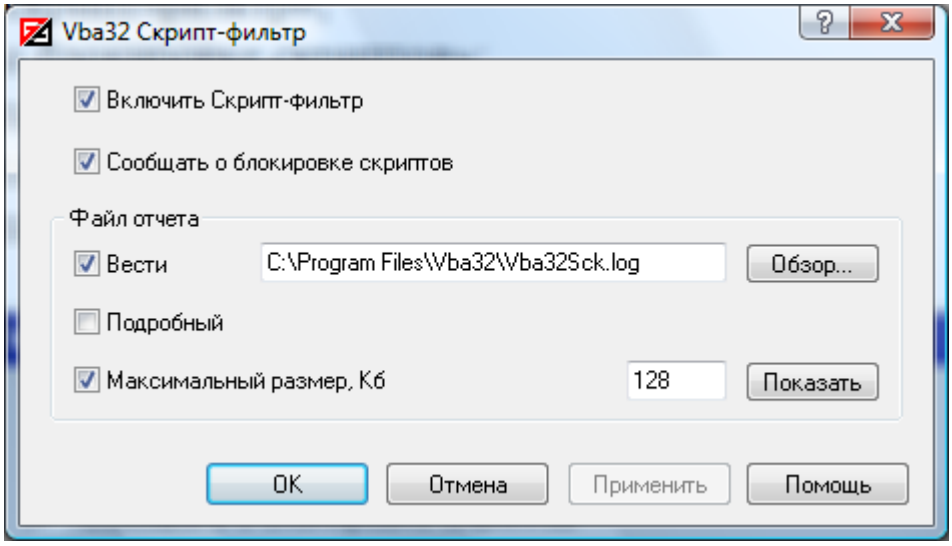

Рис. 48

3.1.9. Outlook-модуль

Outlook-модуль выполняет проверку и обезвреживание почтовых сообщений перед их прочтением и отправкой с использованием Microsoft Outlook и Microsoft Exchange Client. Для вызова диалога настроек Outlook-модуля необходимо выбрать соответствующий пункт в контекстном меню иконки Диспетчера в панели задач (рис. 49).

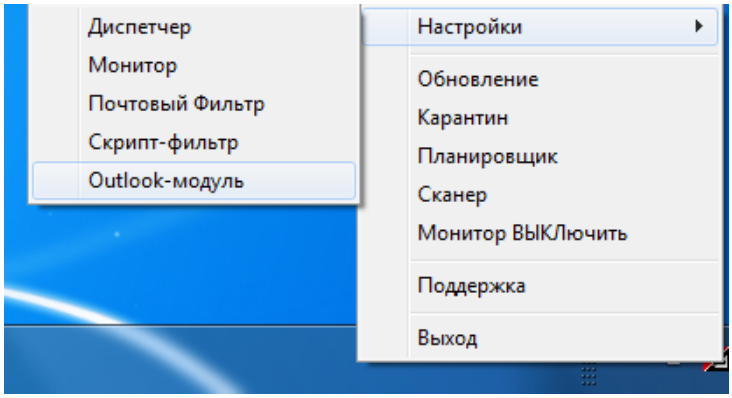

Рис. 49

После этого откроется диалог редактирования настроек Outlook-модуля (рис. 50). После изменения настроек Outlook-модуля необходимо нажать кнопку «ОК» для применения настроек и закрытия диалогового окна, кнопку «Применить» для применения настроек и продолжения редактирования. Для закрытия диалога без применения внесенных изменений необходимо нажать кнопку «Отменить».

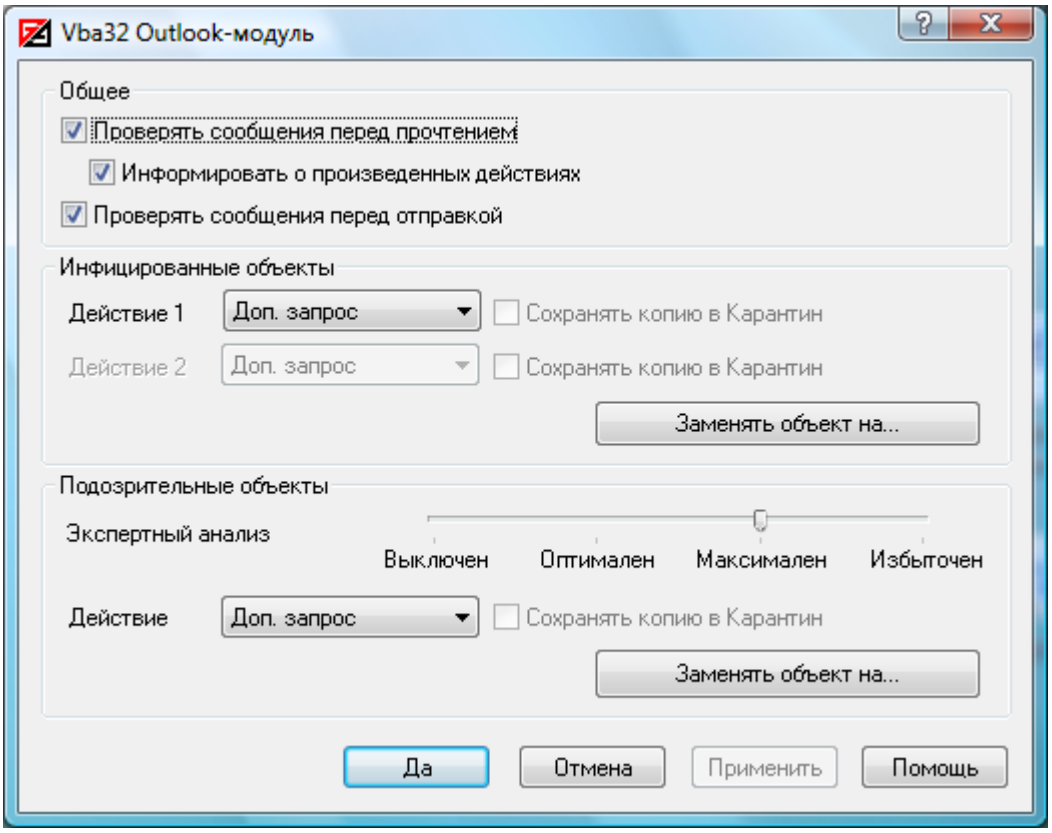

Рис. 50

В разделе «Общее» указываются настройки режимов обработки сообщений. Если установлен пункт «Проверять сообщение при чтении», то при попытке прочитать сообщение пользователь не получит к нему доступ, пока оно не будет проверено. Если установлен пункт «Информировать о произведенных действиях», то Outlook-модуль будет отображать окно с информацией о действиях, которые были произведены над инфицированным либо подозрительным объектом, обнаруженным в сообщении при проверке его перед прочтением (рис. 51).

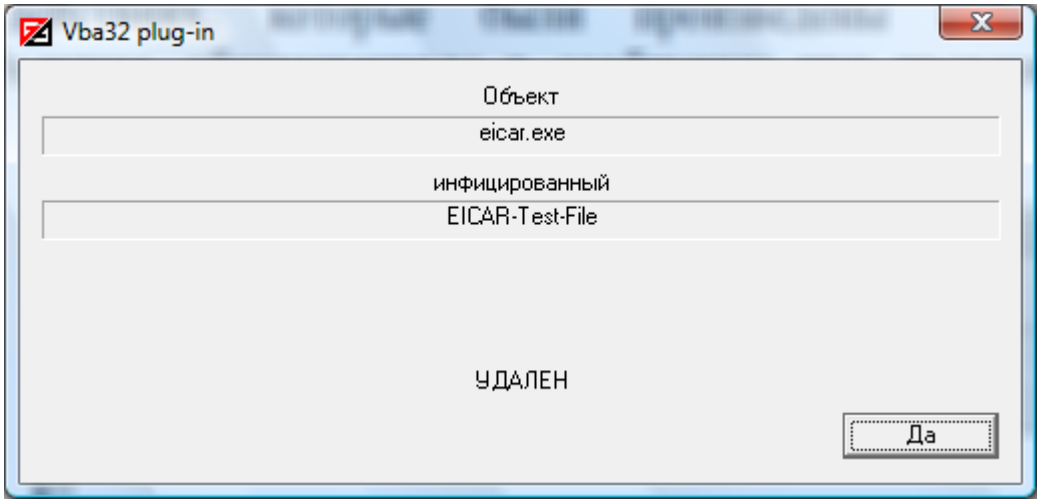

Рис. 51

№ изм.	*Подп.*	*Дата*

Если установлен пункт «Проверять сообщение при отправке», то при попытке отправить сообщение Outlook-модуль будет информировать пользователя об инфицированных либо подозрительных объектах, обнаруженных в сообщении. При этом пользователю будет предоставлен выбор – отправить сообщение как есть, либо отменить отправку этого сообщения (рис. 52).

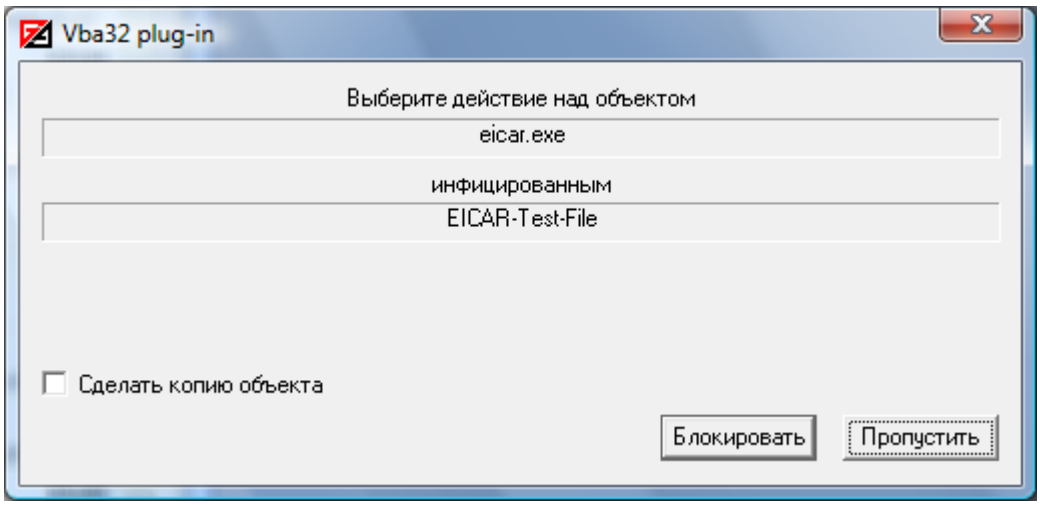

Рис. 52

В разделе «Инфицированные объекты» указываются действия, производимые над объектом сообщения (HTML телом сообщения либо прикрепленным к нему файлом) когда в нем обнаружена вредоносная программа. В поле «Действие 1» указывается действие, которое в первую очередь производиться над инфицированным объектом. В поле «Действие 2» указывается действие, которое производиться над инфицированным объектом, если над ним не удалось произвести первое действие.

Если указано «Пропустить», то при обнаружении инфицированного объекта (HTML тела сообщения либо прикрепленного к нему файла) с ним не будет производиться ни каких действий.

Если указано «Обезвредить», то при обнаружении инфицированного объекта (HTML тела сообщения либо прикрепленного к нему файла), он будет обезврежен.

Если указано «Удалить», то при обнаружении инфицированного объекта (HTML тела сообщения либо прикрепленного к нему файла) он будет удален. Это не означает, что будет удалено все сообщение, а лишь инфицированный объект, находящийся в нем.

Если указано «Доп. запрос», то при обнаружении инфицированного объекта (HTML тела сообщения либо прикрепленного к нему файла) будет выведен диалог для запроса у пользователя действия, которое необходимо выполнить над объектом (рис. 53).

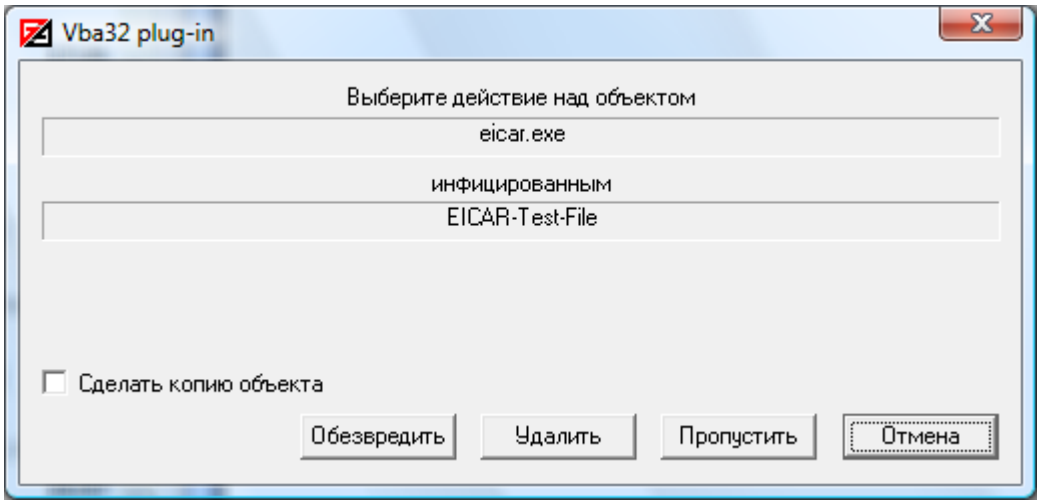

Рис. 53

Если установлен пункт «Делать копию» рядом с полем действия, то перед выполнением над объектом указанного действия будет сохранена его копия в Карантин.

При нажатии кнопки «Заменять объект на…» будет выведен диалог для редактирования содержимого уделенного объекта (см. ниже).

В разделе «Подозрительные объекты» указываются действия, производимые над объектом сообщения (HTML телом сообщения либо прикрепленным к нему файлом) когда в нем обнаружена подозрительная программа. С помощью переключателя «Экспертный анализ» устанавливается уровень эвристического анализа. В положение «Выключен» неизвестные вредоносные программы обнаружены не будут. Положение «Оптимален» позволяет осуществлять детектирование неизвестных вредоносных программ практически не снижает скорость обработки. Положение «Максимален» обеспечивает максимальный уровень детектирования неизвестных вредоносных программ при минимальном количестве ложных срабатываний, но несколько снижает скорость обработки. Положение «Избыточен» обеспечивает обнаружение максимального количества неизвестных вредоносных программ при большей вероятности ложных срабатываний. Рекомендуется только для опытных пользователей

В поле «Действие» указывается действие, которое производиться над подозрительным объектом.

Если указано «Пропустить», то при обнаружении подозрительного объекта (HTML тела сообщения либо прикрепленного к нему файла) с ним не будет производиться ни каких действий.

Если указано «Удалить», то при обнаружении подозрительного объекта (HTML тела сообщения либо прикрепленного к нему файла) он будет удален. Это не означает, что будет удалено все сообщение, а лишь подозрительный объект, находящийся в нем.

Если указано «Доп. запрос», то при обнаружении подозрительного объекта (HTML тела сообщения либо прикрепленного к нему файла) будет выведен диалог для запроса у пользователя действия, которое необходимо выполнить над объектом (рис.).

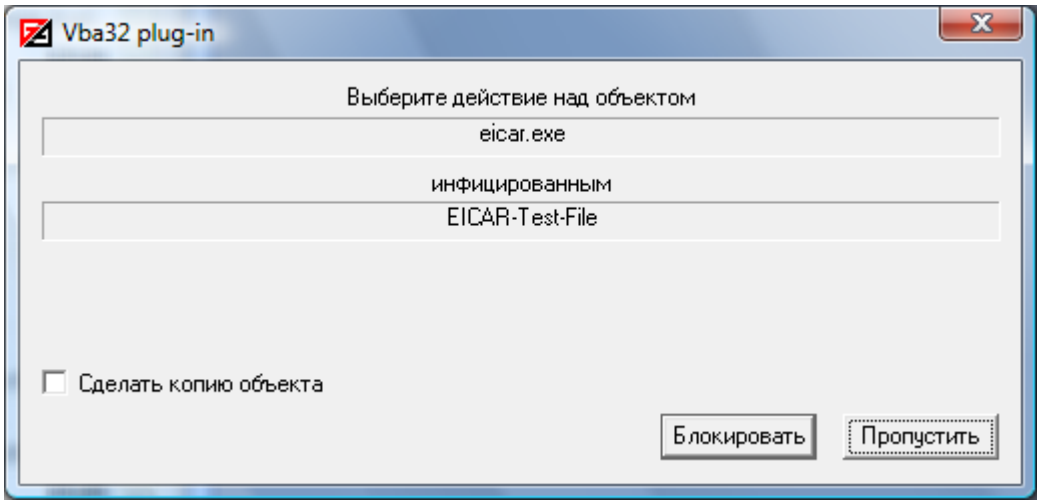

Рис. 54

Если установлен пункт «Делать копию» рядом с полем действия, то перед выполнением над объектом указанного действия будет сохранена его копия в Карантин.

При нажатии кнопки «Заменять объект на…» будет выведен диалог для редактирования содержимого удаленного объекта.

При удалении инфицированного либо подозрительного объекта изменяется его имя и содержимое. Для изменения имени и содержимого удаляемого инфицированного или подозрительного объекта необходимо нажать кнопку «Заменять объект на…» в соответствующем разделе («Инфицированные объекты» либо «Подозрительные объекты»). При этом появиться диалоговое окно (рис. 55).

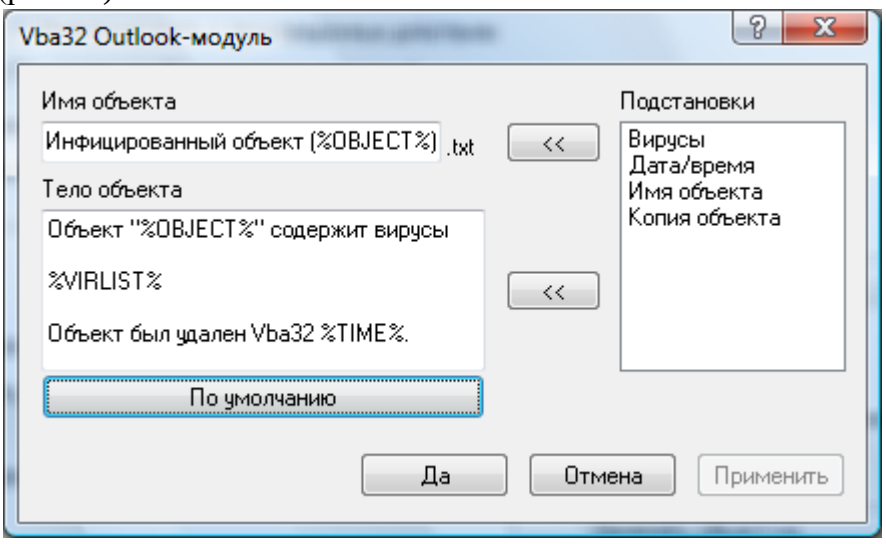

Рис. 55

В поле «Имя объекта» задается имя, которое устанавливается для удаляемого объекта. К заданному имени автоматически добавляется расширение «.txt» для того, чтобы текст, на который было изменено содержимое удаленного объекта, можно было просмотреть прямо из почтового клиента с помощью программы заданной по умолчанию для файлов «*.txt» (обычно Notepad). В полу «Тело объекта» указывается текст, который будет помещен в удаляемый объект вместо его содержимого.

При редактировании имени объекта и тела объекта, возможна вставка текстов подстановки, для этого необходимо нажать кнопку «<<», предварительно выбрав текст подстановки из списка «Подстановки». Далее следует описание текстов подстановки:

– «Дата/время» (%TIME%) – время удаления инфицированного/подозрительного объекта;

– «Имя объекта» (%OBJECT%) – исходное имя удаляемого объекта;

– «Вирусы» (%VIRLIST%) – список инфицированных/подозрительных объектов обнаруженных в проверяемом объекте.

Чтобы задать имя объекта и тело объекта, заданные производителем по умолчанию, необходимо нажать кнопку «По умолчанию».

3.1.10. Консольный сканер для Windows

Консольный сканер для Windows используется для запуска антивирусной обработки файлов из командной строки.

Чтобы запустить консольный сканер Vba32, измените текущий каталог на каталог с установленным комплексом Vba32. По умолчанию комплекс устанавливается в каталог c:\Program Files\Vba32\.

Синтаксис командной строки следующий:

Для Windows:

vba32**w**.exe [путь] ... [путь] [/ключ] ... [/ключ].

Синтаксис командной строки требует соблюдения определенного порядка следования: сначала перечисляются все пути обработки, затем следует перечисление ключей.

ПУТЬ	**Значение**
файл/каталог	Путь к файлу или каталогу, предназначенным для обработки. Длинные имена файлов приводятся в кавычках.
*:	Все локальные диски.
**:	Все сетевые диски.
@список	Список файлов.

Параметр КЛЮЧ задает режимы работы программы.

Примечание: По умолчанию включены параметры /QU /MR /BT /AS /RW

Для прекращения работы консольного сканера нажмите Ctrl+C.

Ниже перечислены все ключи командной строки, используемые при работе с консольным сканером для Windows:

/?[+|-] - вывод данной справки;

/H[+|-] - вывод данной справки;

/HELP[+|-] - вывод данной справки;

/M=1 - быстрый режим обработки;

/M=2 - безопасный режим обработки (/AF+);

/M=3 - избыточный режим обработки (/AF+ /PM+);

/AF[+|-] - все файлы;

/PM[+|-] - избыточный поиск;

/RW[+|-] - детектирование Spyware, Adware, Riskware;

/CH[+|-] - включить кэш при обработке объектов;

/FC[+|-] - обезвреживание инфицированных файлов;

/FD[+|-] - удаление инфицированных файлов;

/FR[+|-] - переименование инфицированных файлов;

/FM+[каталог] - перемещение инфицированных файлов в указанный каталог (по умолчанию C:\\Virus);

/SD[+|-] - удаление подозрительных файлов;

/SR[+|-] - переименование подозрительных файлов;

/SM+[каталог] - перемещение подозрительных файлов в указанный каталог (по умолчанию C:\\Virus);

/BC[+|-] - обезвреживание загрузочных секторов;

/NA[+|-] - отключение детектирования для подписанных файлов (только Windows);

/LF[+|-] - загрузить кириллический шрифт (только для DOS-версии), load Russian font (DOS-version only);

/HA=[0|1|2|3] - уровень экспертного анализа (0 - отключен, 2 - максимальный);

/MR=[0|1|2] - проверка памяти (0 - отключен, 2 - полный,
по умолчанию включен полный);

/AS=[0|1|2] - обработка файлов, автоматически запускаемых
при старте системы (0 - отключен, 2 - полный,
по умолчанию включен полный, только Windows);

/BT[+|-] - проверка загрузочных секторов (по умолчанию включен);

/QI[+[каталог]|-] - помещать в карантин инфицирование объекты;

/QS[+[каталог]|-] - помещать в карантин подозрительные объекты;

/D=[N,][имя_файла] - запуск программы один раз в N дней (по умолчанию 1);

/R=[имя_файла] - сохранение отчета в файл (по умолчанию VBA32.RPT);

/R+[имя_файла] - добавление отчета в файл (по умолчанию VBA32.RPT);

/UL[+|-] - вывод отчета в кодировке UTF-8;

/L=[имя_файла] - сохранение списка инфицированных файлов в файл (VBA32.LST);

/L+[имя_файла] - добавление списка инфицированных файлов в файл (VBA32.LST);

/QU[+|-] - прерывать выполнение программы (по умолчанию включен);

/DB=каталог - искать при запуске обновления баз в указанном каталоге;

/SS[+|-] - включить звуковую сигнализацию при обнаружении вируса;

/OK[+|-] - включение имен \"чистых\" файлов в отчет;

/AR[+|-] - включение обработки файлов в архивах;

/AL=[размер_файла,кБ] - не проверять архивы размером больше заданного;

/AD[+|-] - удаление архивов, содержащих инфицированные файлы;

/SFX[+|-] - детектирование вирусных инсталляторов;

/ML[+|-] - проверка почты;

/MD[+|-] - удаление писем с инфицированными файлами;

/VL[+|-] - вывод списка известных программе вирусов;

/VM[+|-] - показывать информацию о макросах в документах;
/SI[+|-] - дополнительная информация о поддержке программы;
/LNG=суффикс - выбор языкового файла VBA32<суффикс>.LNG;
/KF={каталог|путь} - указать расположение ключевого файла;
/EXT= - установить список проверяемых расширений;
/EXT+ - добавить расширения в список по умолчанию;
/EXT- - исключить расширения из списка по умолчанию;
/WK[+|-] - ожидать нажатия клавиши после завершения программы;
По умолчанию включены параметры /QU /MR /BT /AS /RW .

3.1.11. Vba32 Планировщик

Планировщик задач комплекса Vba32 предназначен для запуска задач (сторонних приложений, процесса сканирования, процесса обновления) в указанные временные ограничения на персональных компьютерах, рабочих станциях и серверах.

Следующие темы объясняют правильную работу с задачами планирования (рис. 56):

– создание задачи;
– редактирование задачи;
– удаление задачи;
– принудительный запуск.

Дополнительные возможности планировщика:

– отображение лога задачи;
– детальное отображение задачи.

Основные возможности настройки:

– типы действия задач .

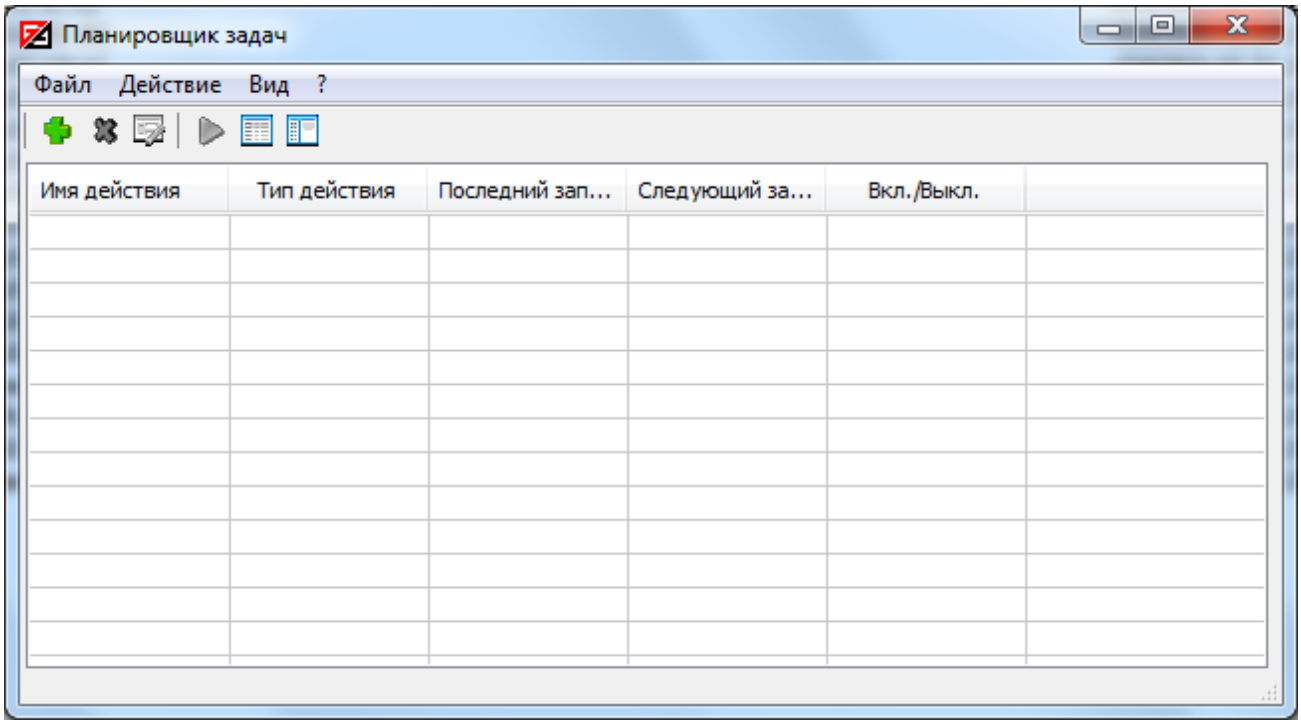

Рис. 56

3.1.11.1. Основные и дополнительные возможности планировщика

Создание задачи

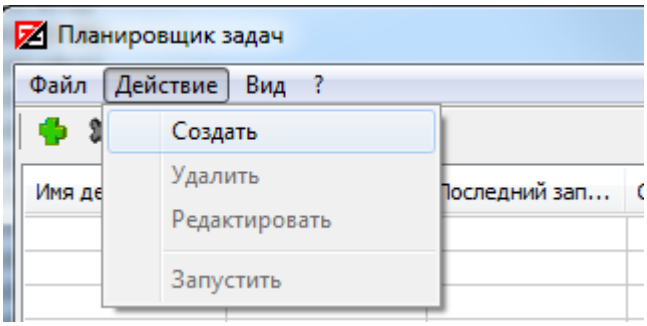

Рис. 57

Выберите действие **Создать** в меню (рис. 57) или нажмите кнопку **Создать**.
Введите название задачи, выберите тип действия задачи, нажмите кнопку **Далее->** .
При необходимости, настройте действие задачи и нажмите кнопку **Далее->.**
Имя задачи не может повторяться с именами существующих задач.
Выберите тип периодичности запуска задачи и нажмите кнопку **Далее->**
При необходимости, настройте периодичность запуска задачи и нажмите кнопку **Готово->**

Редактирование задачи

Выберите задачу из списка задач (рис. 58).

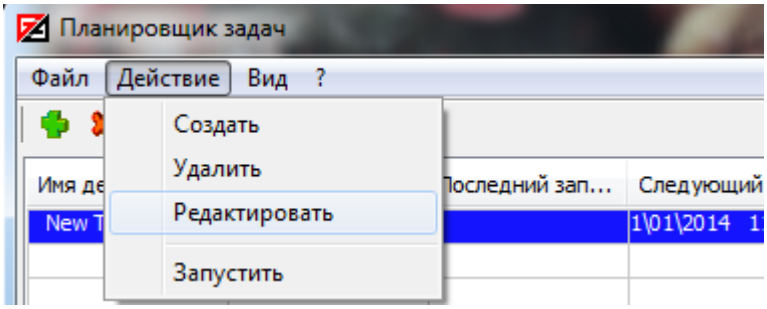

Рис. 58

Выберите действие **Редактировать** в меню или нажмите кнопку **Редактировать**.

В появившемся окне возможно редактирование параметров задачи (название задачи, тип действия, тип периодичности).

Для применения настроек нажмите кнопку **Применить** или кнопку **Ок**, для отмены действия кнопку **Отмена** или закройте окно.

Удаление задачи

Выберите задачу из списка задач (рис. 59).

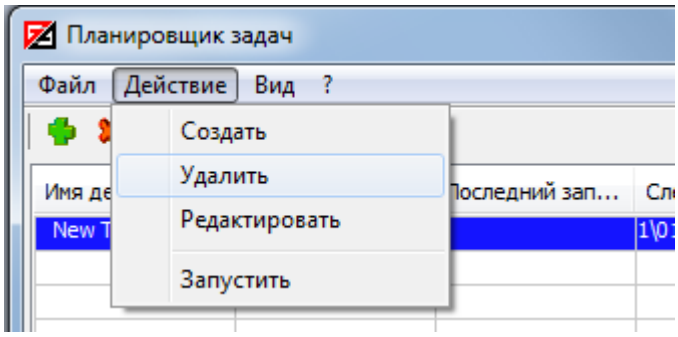

Рис. 59

Выберите действие **Удалить** в меню или нажмите кнопку **Удалить**.

Подтвердите ваше действие в диалоговом окне.

Запуск задачи

Выберите задачу из списка задач (рис. 60).

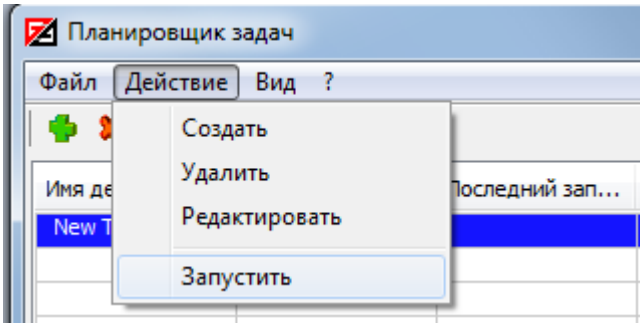

Рис. 60

Выберите действие **Запустить** в меню или нажмите кнопку **Запустить**.

Принудительные запуски не влияют на периодичности. Информация о них сохраняется только в логах задач.

Отображение лога задачи

Выберите в меню **Обзор логов** (рис. 61) или нажмите кнопку **Обзор логов**

Выберите задачу из списка задач.

В правой части окна будет отображен лог выбранной задачи.

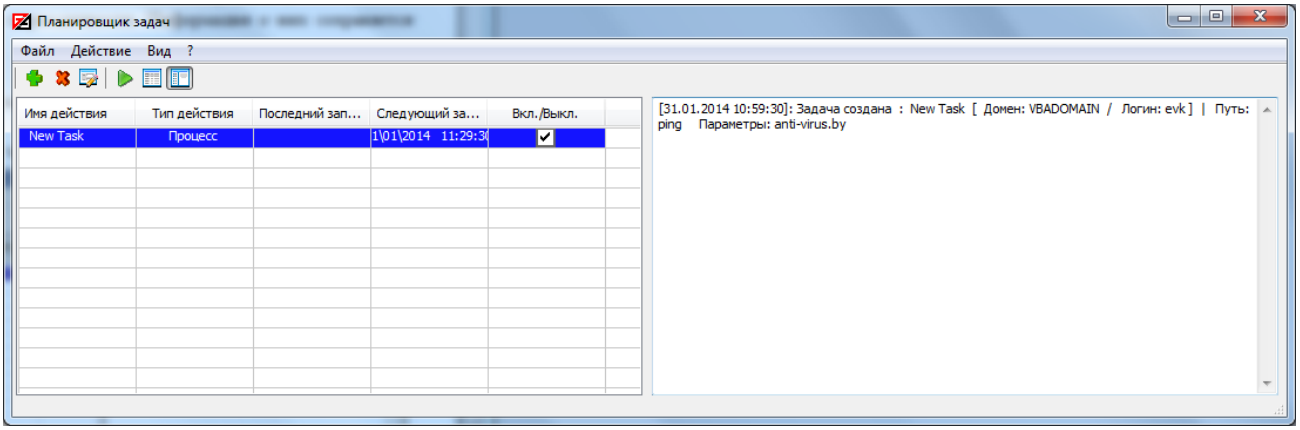

Рис. 61

Для детального отображения информации о задаче:

Выберите в меню Детальное отображение или нажмите кнопку  (рис. 62). Детальное отображение.

В списке задач будет отображаться дополнительная информация.

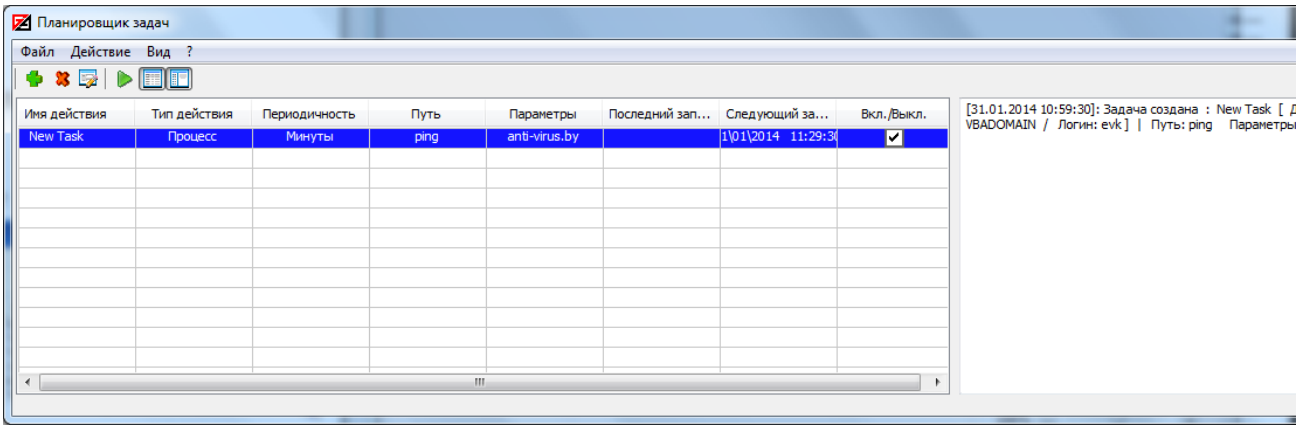

Рис. 62

3.1.11.2. Типы действия задач

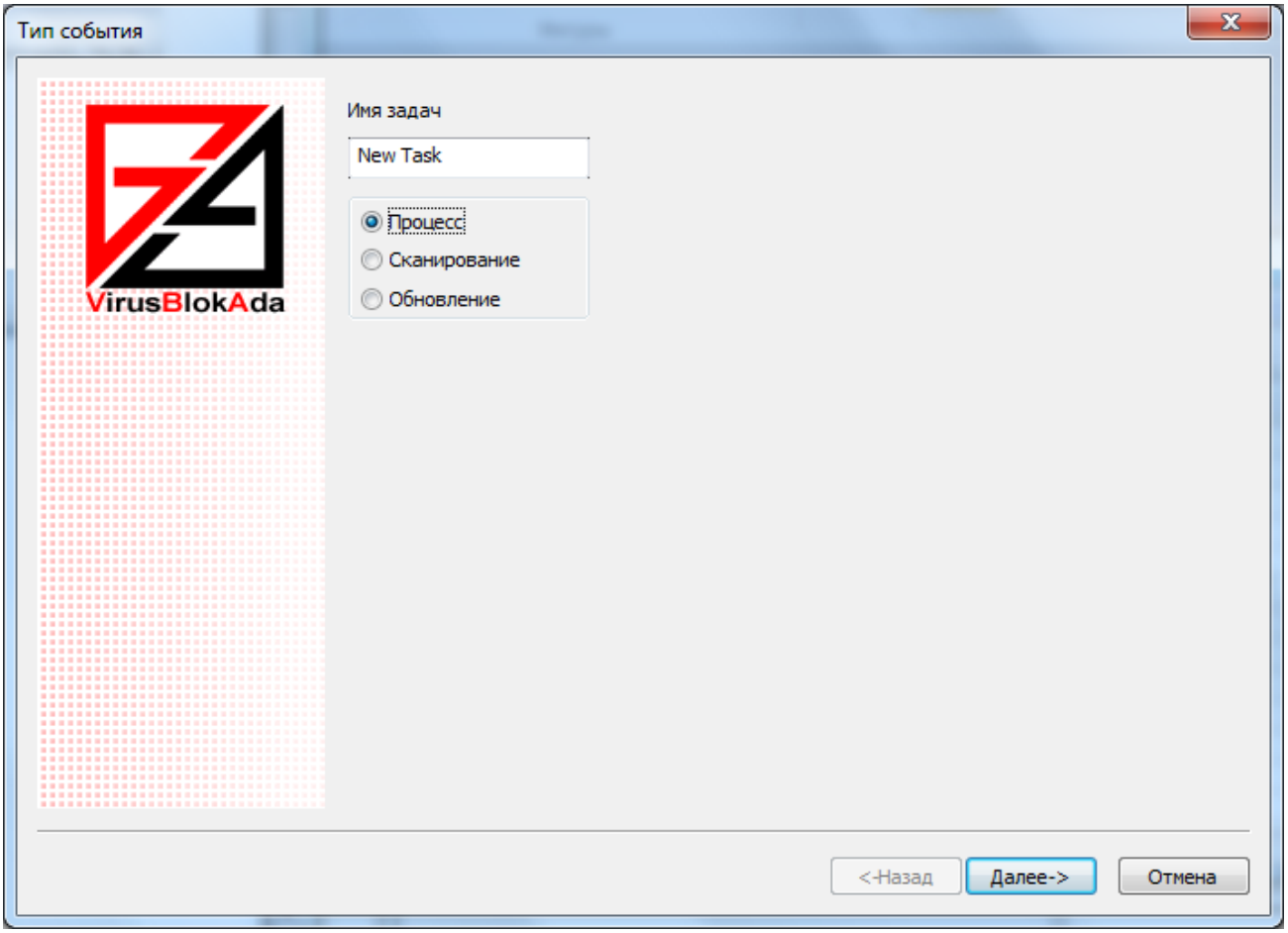

Рис. 63

Планировщик задач может создавать задачи с типами действий (рис. 63):

– Пользовательский процесс - запуск пользовательского процесса;
– Сканирование - запуск консольного сканера;
– Обновление - запуск процесса обновления.

Пользовательский процесс

Пользовательский процесс - процесс, настраиваемый пользователем (рис. 64).

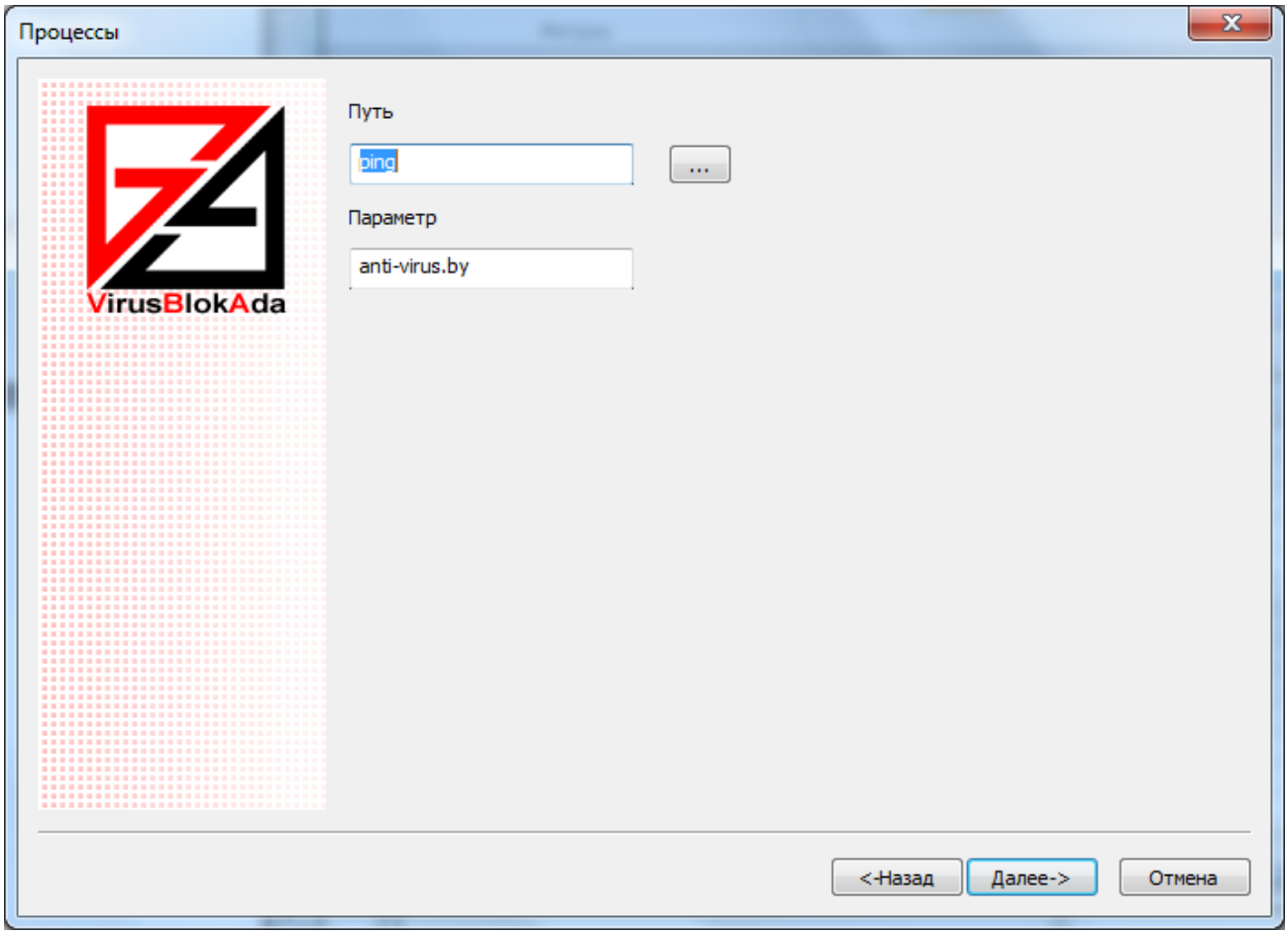

Рис. 64

Путь - путь к пользовательскому процессу.

Параметры - параметры, передаваемые процессу через командную строку при его запуске.

Процесс сканирования

Процесс сканирования - запуск консольного сканера (рис. 65).

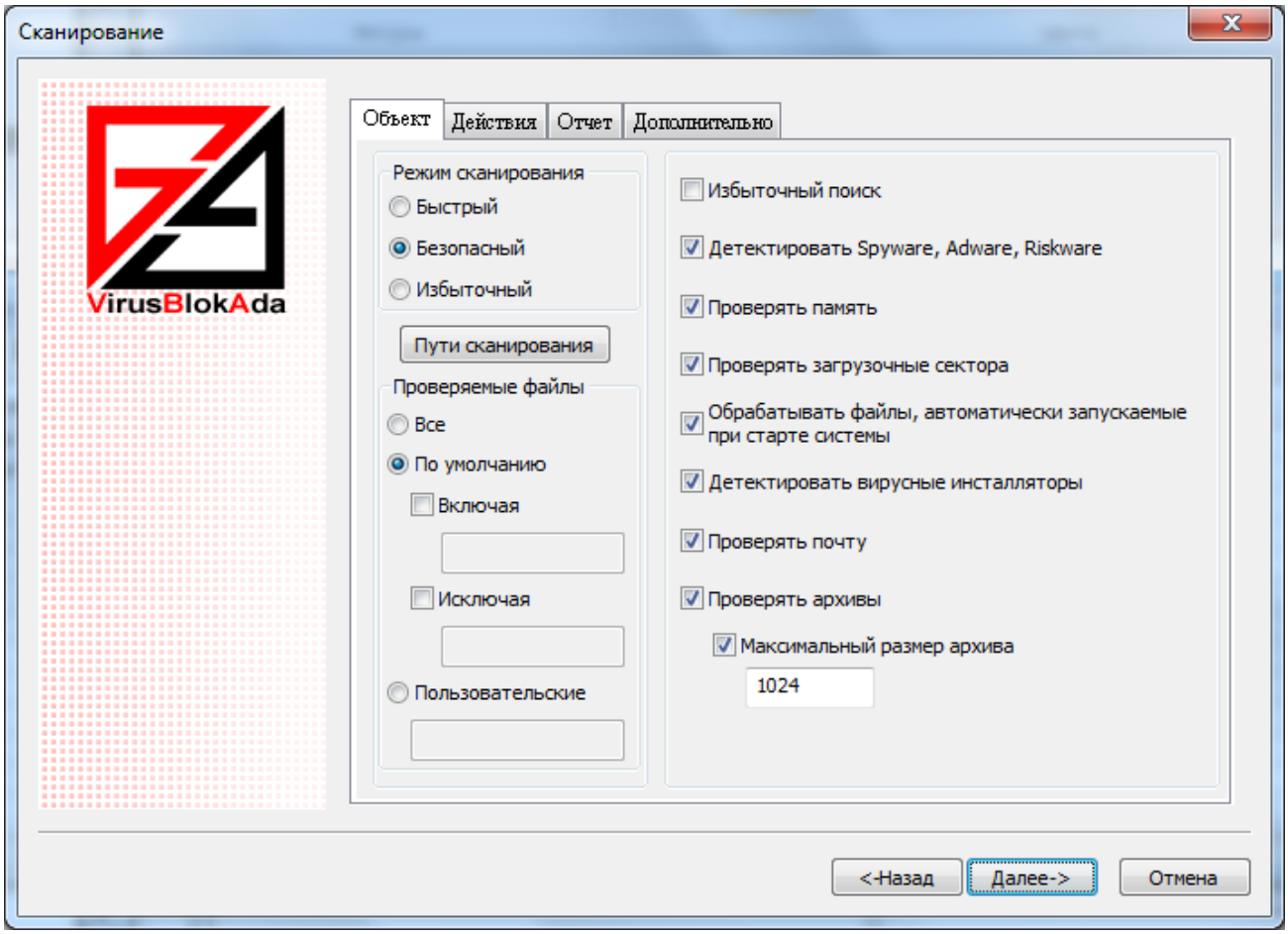

Рис. 65

Объект - настройка объекта сканирования, включает в себя:

– Режим сканирования:

- Быстрый (флаг /M=1);
- Безопасный (флаг /M=2);
- Избыточный (флаг /M=3);

– Пути сканирования – диалоговое окно с возможностью добавления, редактирования, удаления путей сканирования;

– Проверяемые файлы:

- Все ;
- По умолчанию;
- Включая (флаг /EXT+””);
- Исключая (флаг /EXT-””);
- Пользовательские (флаг /EXT=””);

– Избыточный поиск (флаг /PM);

– Детектировать Adware, Spyware, Riskware (флаг /RW);

– Проверять память (флаг /MR);

- Проверять загрузочные сектора (флаг /BT);
- Обрабатывать файлы, автоматически запускаемые при старте (флаг /AS);
- Детектировать вирусные инсталляторы (флаг /SFX);
- Проверять почту (флаг /ML);
- Проверять архивы (флаг /AR);

Максимальный размер архива (флаг /AL=).

Действия - выполняемые над объектами, включают в себя (рис. 66).

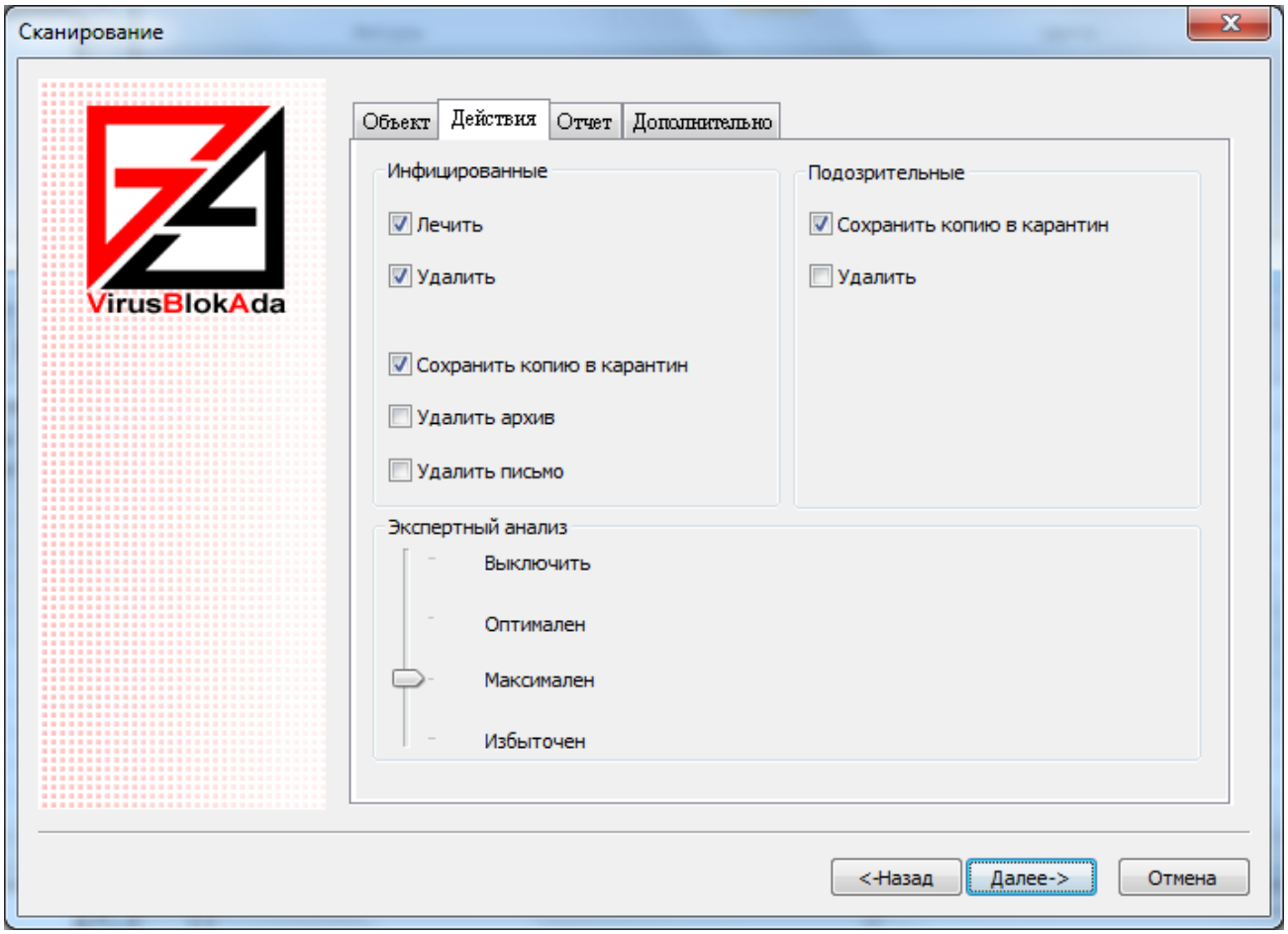

Рис. 66

- Инфицированные:
  - Лечить (флаг /FC);
  - Удалить (флаг /FD);
  - Сохранить копию в карантин (флаг /QI) ;
  - Удалить архив (флаг /AD);
  - Удалить письмо (флаг /MD);
- Подозрительные:
  - Сохранить копию в карантин (флаг /QS);
  - Удалить (флаг /SD);

– Экспертный анализ:
  - Выключен (флаг /HA=0);
  - Оптимален (флаг /HA=1);
  - Максимален (флаг /HA=2);
  - Избыточен (флаг /HA=3).

Отчет – настройка отчетов сканирования (рис. 67).

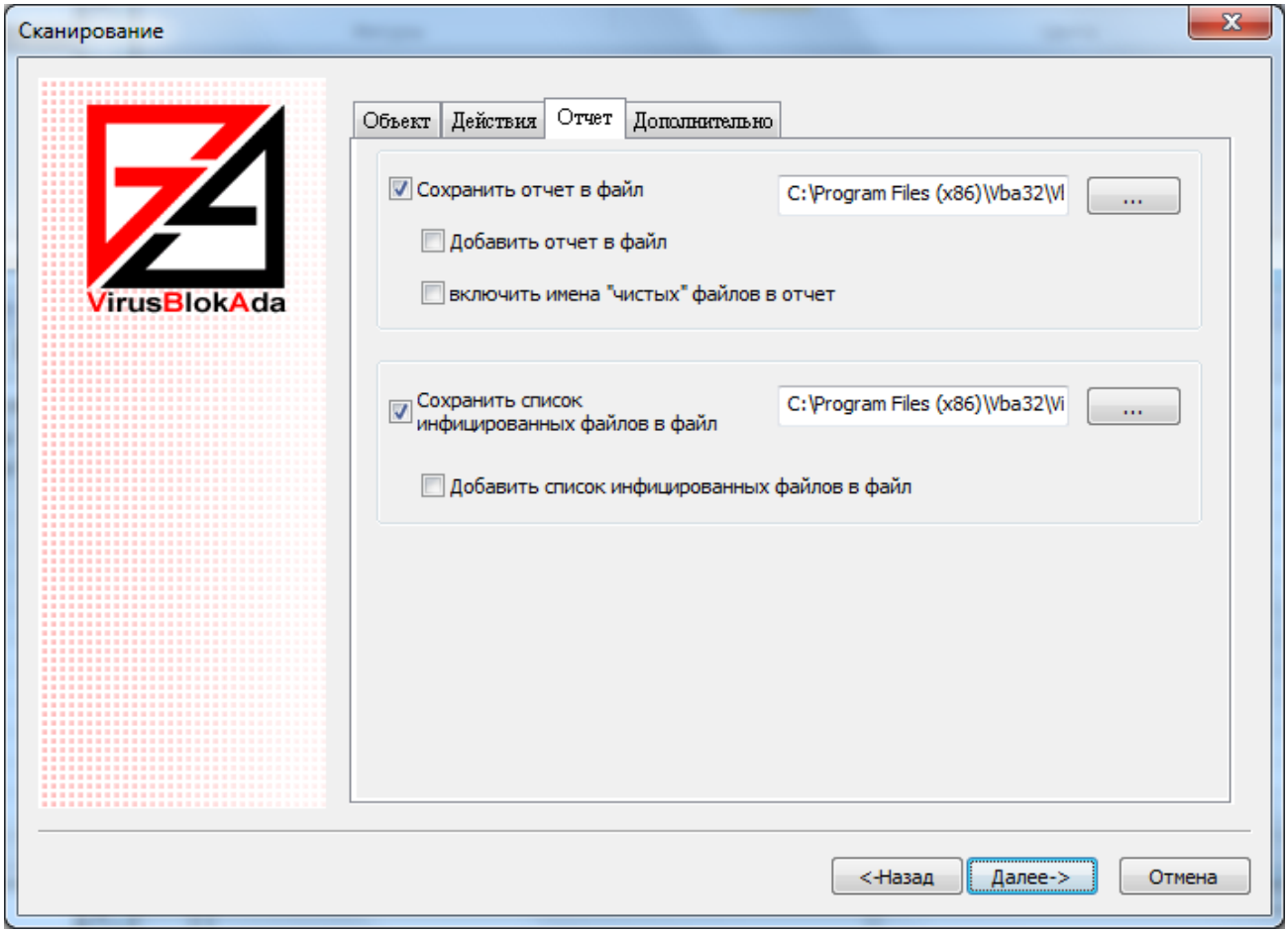

Рис. 67

Сохранить отчет в файл (флаг /R=).
Добавить отчет в файл (флаг /R+).
Включить имена «чистых» файлов в отчет (флаг /OK).
Сохранить список инфицированных файлов в файл (флаг /L=).
Добавить список инфицированных файлов в файл (флаг /L+).
Дополнительно - настройка дополнительных параметров сканирования (рис. 68).
Включить кэш (флаг /CH).
Прерывать выполнение программы (флаг /QU).
Искать при запуске обновление баз (флаг /DB=).
Включить звуковую сигнализацию (флаг /SS).

Прятать окно сканирования – процесс сканирования будет проходить без отображения окна консольного сканера.

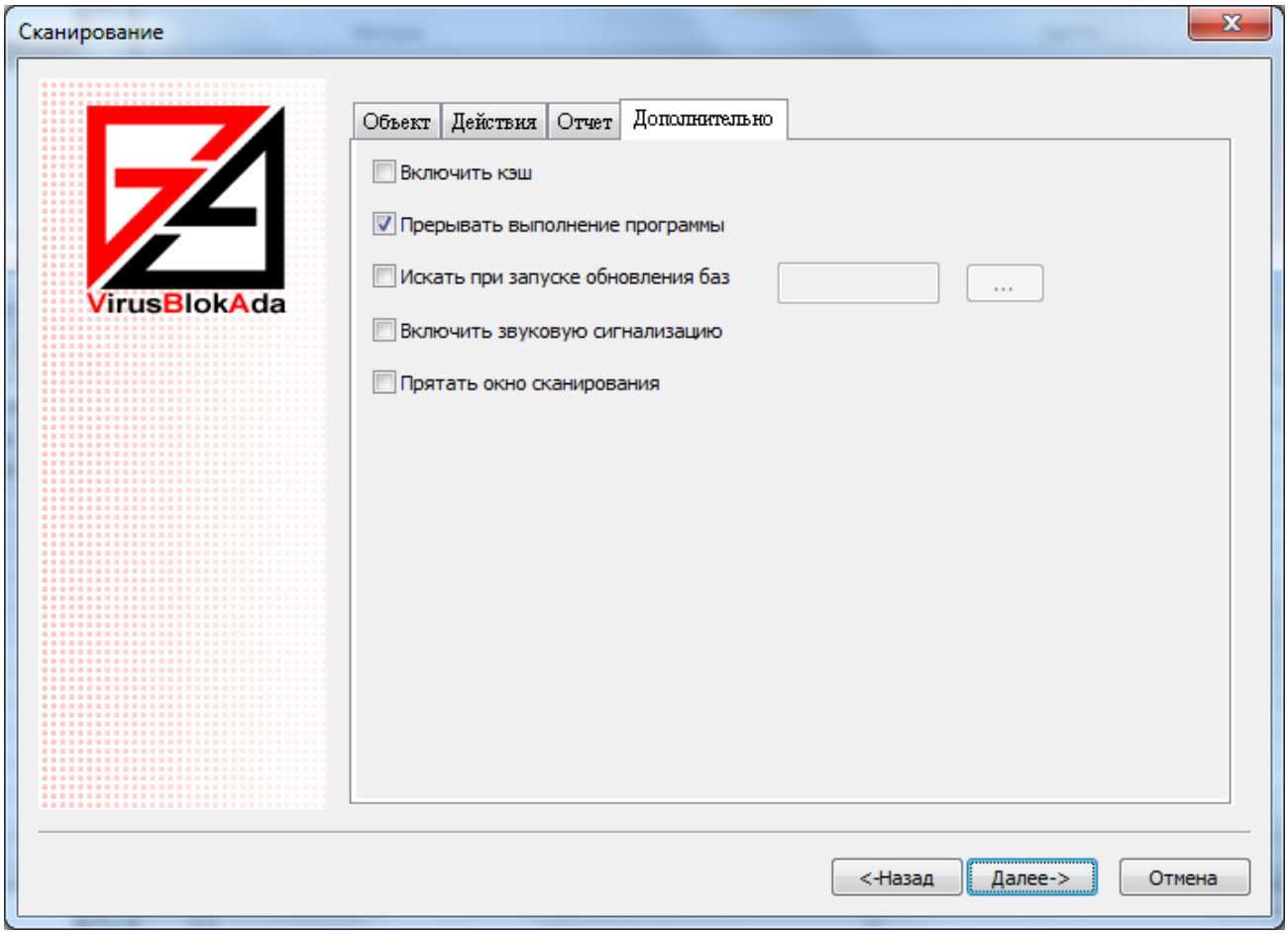

Рис. 68

Процесс обновления

Процесс обновления - обновление комплекса Vba32.

Настройки путей обновления и доступа к сети располагаются в закладке Дополнительно окна Диспетчера.

3.1.11.3. Планирование времени запуска

Планировщик задач может запускать задачи с периодичностями:

– Минуты - запуск задачи через определенное количество минут.. ;

– Часы - запуск задачи через определенное количество часов;

– Дни - запуск задачи через определенное количество дней, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня;

– Недели - запуск задачи в определенные дни недели, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня;

– Месяцы - запуск задачи в определенные дни месяца, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня;

– Фиксированное время - запуск задачи в определенный день, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня.

Планирование времени запуска: Минуты

Минуты - запуск задачи через определенное количество минут (рис. 69).

Вы можете задать любое число от 1 до 1440.

Рис. 69

Планирование времени запуска: Часы

Часы - запуск задачи через определенное количество часов (рис. 70).

Вы можете задать число от 1 до 168.

Рис. 70

Планирование времени запуска: Дни

Дни - запуск задачи через определенное количество дней, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня (рис. 71).

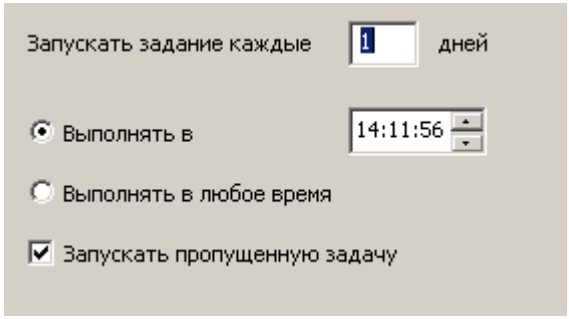

Рис. 71

Запускать задание каждые ... - задача выполняется через определенное количество дней. Вы можете задать число от 1 до 61.

Выполнять в…- задача выполняется в определенное время.

Выполнять в любое время – задача запускается при первой возможности.

Запускать пропущенную задачу – эта настройка дает возможность запустить задачу, которая была по какой-то причине пропущена.

Планирование времени запуска: Недели

Недели - запуск задачи в определенные дни недели, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня (рис. 72).

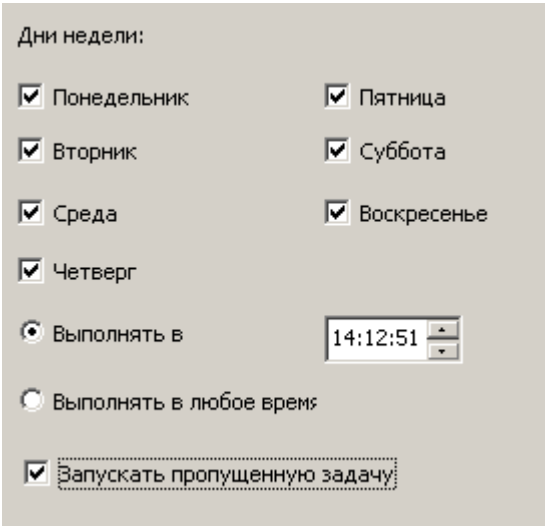

Рис. 72

Дни недели - дни, в которые необходим запуск задачи. Должен быть указан хотя бы один день.

Выполнять в… - задача выполняется в определенное время.

Выполнять в любое время – задача запускается при первой же возможности.

Запускать пропущенную задачу – эта настройка дает возможность запускать задачу, которая по каким-то причинам была пропущена.

Планирование времени запуска: Месяцы

Месяцы - запуск задачи в определенные дни месяца, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня (рис. 73).

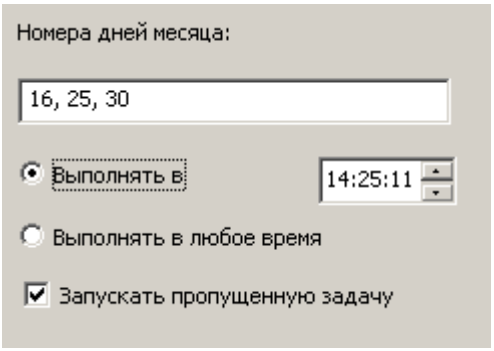

Рис. 73

Номера дней месяца - дни, в которые необходим запуск задачи. Вам необходимо ввести любые числа от 1 до 31, разделенные пробелами и/или запятыми.

Выполнять в… - задача выполняется в определенное время.

Выполнять в любое время – задача запускается при первой же возможности.

Запускать пропущенную задачу – эта настройка дает возможность запускать задачу, которая по каким-то причинам была пропущена.

Планирование времени запуска: Фиксированное время

Фиксированное время - запуск задачи в определенный день, с возможностью запуска пропущенной задачи, и запуском в определенное или произвольное время дня (рис. 74).

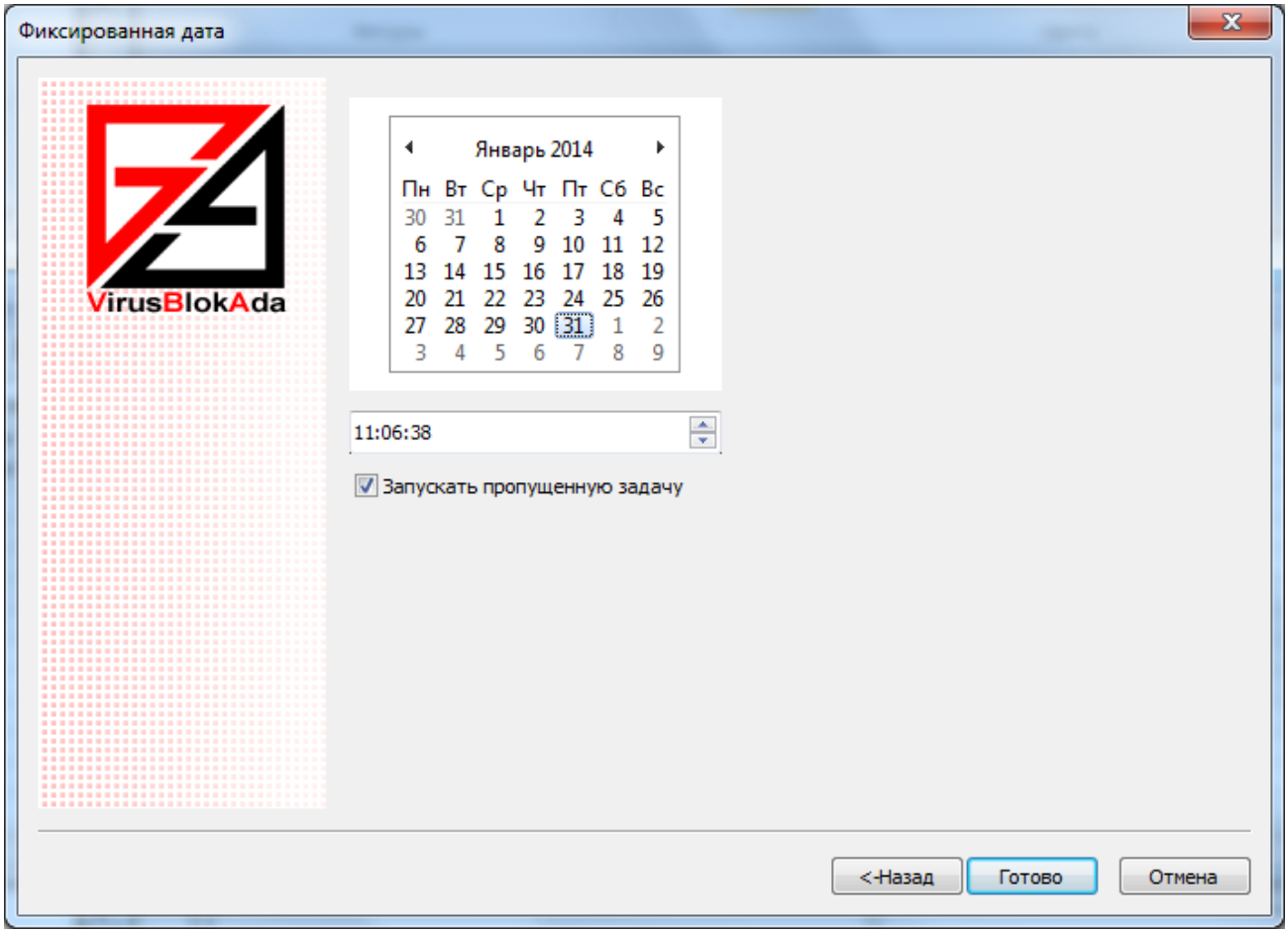

Рис. 74

Запускать пропущенную задачу – если не было возможности запустить задачу в назначенное время, она запустится при первой же возможности.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Комплекс состоит из модулей, каждый из которых предназначен для выполнения конкретной задачи. Пользователь взаимодействует с каждым модулем посредством графического интерфейса или параметров командной строки. Комплекс предоставляет дружественный графический пользовательский интерфейс, а также интерфейсы для взаимодействия с модулями. Входными данными для Комплекса являются команды, вводимые оператором с клавиатуры и «мыши». Входными данными также могут являться файлы конфигурации и сообщения (коды возврата) о результатах выполнения команд различными модулями. Выходными данными является информация, выводимая на дисплей или принтер по требованию оператора, а также информация, необходимая для работы модулей.

5. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе использованы следующие сокращения:
ОС – операционная система;
ПК – персональный компьютер;
ЦУ – центр управления.

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводи-тельного докум. и дата*	*Подп.*	*Дата*
	изменен-ных	*заменен-ных*	*новых*	*аннули-рованных*					

№ изм.	*Подп.*	*Дата*