Спасательный Образ
Vba32 Rescue
Руководство пользователя

ВирусБлокАда

Содержание

Введение

Спасательный Образ **Vba32 Rescue** – продукт компании **«ВирусБлокАда»**, позволяющий восстановить систему после воздействия на нее вредоносного ПО. Этот продукт позволяет обезвреживать вредоносное (и подозрительное) ПО на компьютере пользователя с наибольшим эффектом. Процессы сканирования и лечения производятся независимо от операционной системы, установленной на компьютере. Благодаря этому, вредоносное ПО не сможет противодействовать процессу обезвреживания.

> **Внимание!** Данный продукт не защищает систему от возникновения подобных ситуаций в будущем. Для предотвращения случаев заражения компьютера необходимо воспользоваться всем комплексом решений, предоставляемых компанией **«ВирусБлокАда»**.

Спасательный Образ **Vba32 Rescue** представляет собой загрузочный образ, который может быть записан на компакт-диск или USB-носитель. В основе образа лежит ядро на базе операционной системы Linux, загрузчика Grub, консольного сканера **Vba32.CS.L** под Linux и других модулей работы с файловой системой, сетевым окружением, графическим интерфейсом пользователя и др. Спасательный Образ **Vba32 Rescue** работает в следующих режимах:

- **VbaRescue** - стандартный режим;
- **VbaRescue, with Linux 3.16.7-53-default**
- **VbaRescue, with Linux 3.16.7-53-default (recovery mod)**

Первый режим предоставляет стандартные возможности Спасательного Образа и вызывается по умолчанию. Данный режим менее требователен к аппаратным ресурсам компьютера.

Второй режим, …

> **Примечание.** Скачать спасательный образ Vba32 rescue можно на официальном ресурсе **«ВирусБлокАда»**:
> ftp://anti-virus.by/pub/VbaRescue.i686.7z

1. Аппаратные требования

Ниже перечислены необходимые аппаратные требования для различных режимов работы Спасательного Образа **Vba32 Rescue**.

Для загрузки:

- процессор i686;
- 96МБ оперативной памяти;
- CD/DVD-ROM или USB-носитель с объемом памяти не менее 128 Мб.

Для сканирования:

- процессор i686;
- 96МБ оперативной памяти;
- CD/DVD-ROM или USB-носитель с объемом памяти не менее 128 Мб;
- винчестер с интерфейсом PATA или SATA и соответствующим контроллером.

Для обновления и сканирования:

- процессор i686;
- 192МБ оперативной памяти;
- CD/DVD-ROM или USB-носитель с объемом памяти не менее 128 Мб;
- винчестер с интерфейсом PATA или SATA и соответствующим контроллером;
- Ethernet-интерфейс.

Поддерживаемые файловые системы: NTFS, FAT, ext2/3/4, reiserfs.

2. Создание загрузочного носителя

Для создания загрузочного Usb-носителя, рекомендуется воспользоваться бесплатной утилитой Rufus, которую можно скачать с официального сайта https://rufus.akeo.ie.

После скачивания утилиты необходимо её запустить, после чего откроется пользовательский интерфейс Rufus (рисунок 2.1).

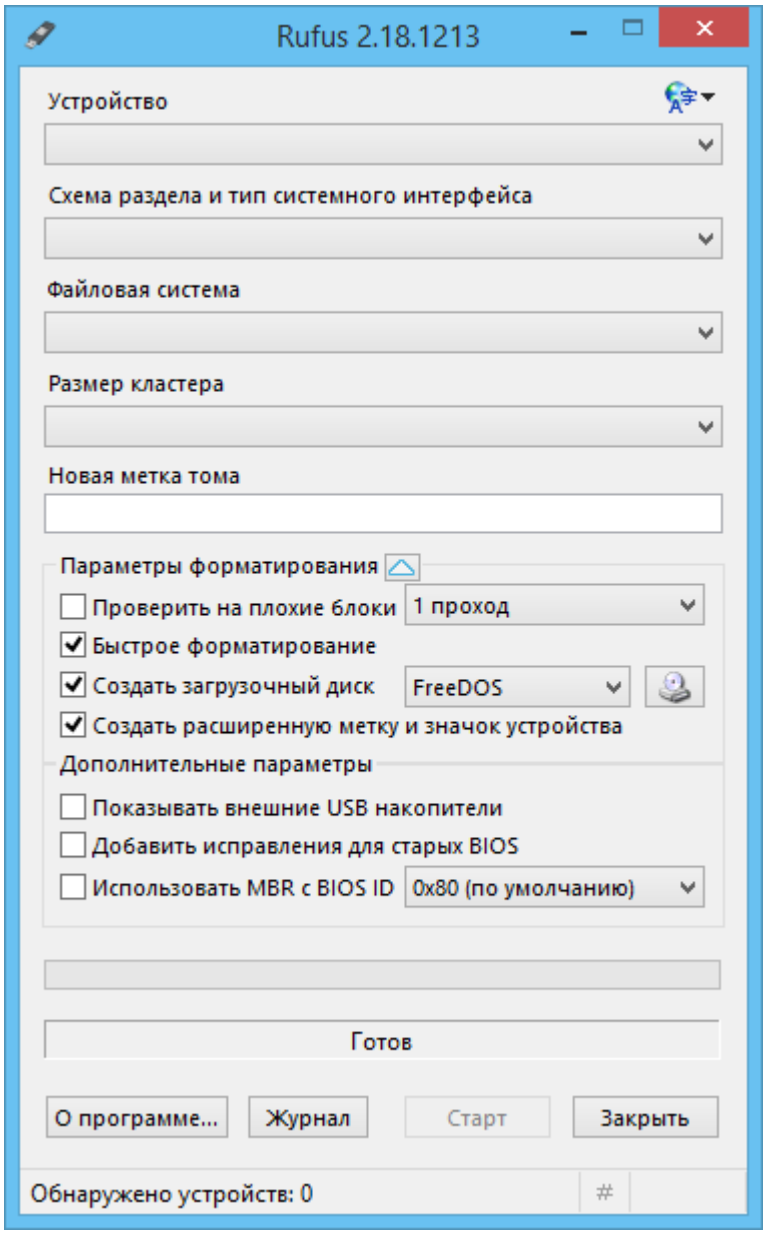

Рисунок 2.1 – пользовательский интерфейс Rufus

Присоединив Usb-устройство к компьютеру, утилита Rufus автоматически подставит параметры устройства в поля.

Примечание. Если к компьютеру присоединено несколько Usb-устройств, то необходимо в выпадающем списке «Устройство» выбрать нужное устройство.

После выбора Usb-устройствана которое необходимо записать спасательный образ **Vba32 Rescue,** необходимо напротив галочки «Создать загрузочный диск» нажать на изображение диска и дисковода (рисунке 2.2.2) и указать путь к спасательному образу **Vba32 Rescue**.

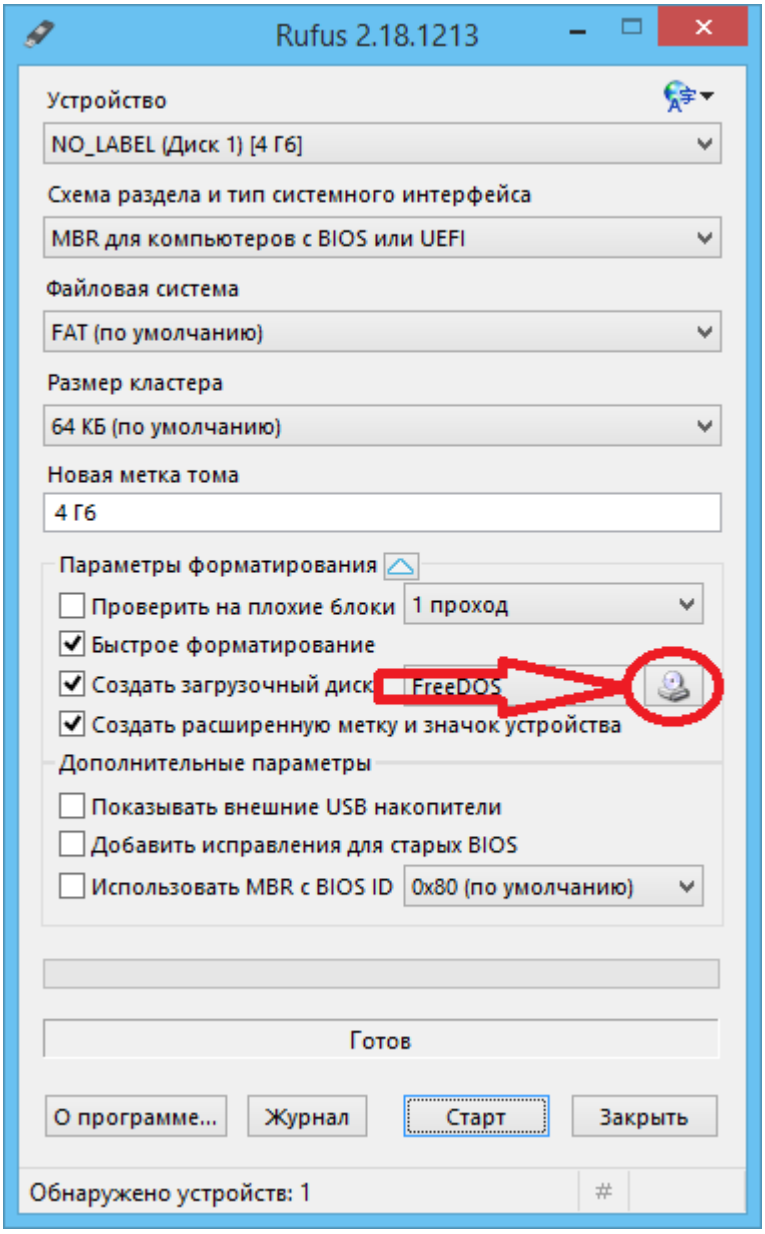

Рисунок 2.2 – Выбор образа для записи

Примечание. Если проводник не отображает нужный файл спасательного образа, включите отображение всех файлов.

Выбрав необходимый образ, утилита Rufus автоматически подставит остальные параметры для записи, после чего необходимо запустить процесс создания загрузочного Usb-носителя, нажав на кнопку «Старт» и дождаться окончания процесса.

3. Загрузка образа Vba32 Rescue

При загрузке Спасательного Образа **Vba32 Rescue** пользователю предлагаются на выбор следующие режимы работы (Рисунок 3.1):

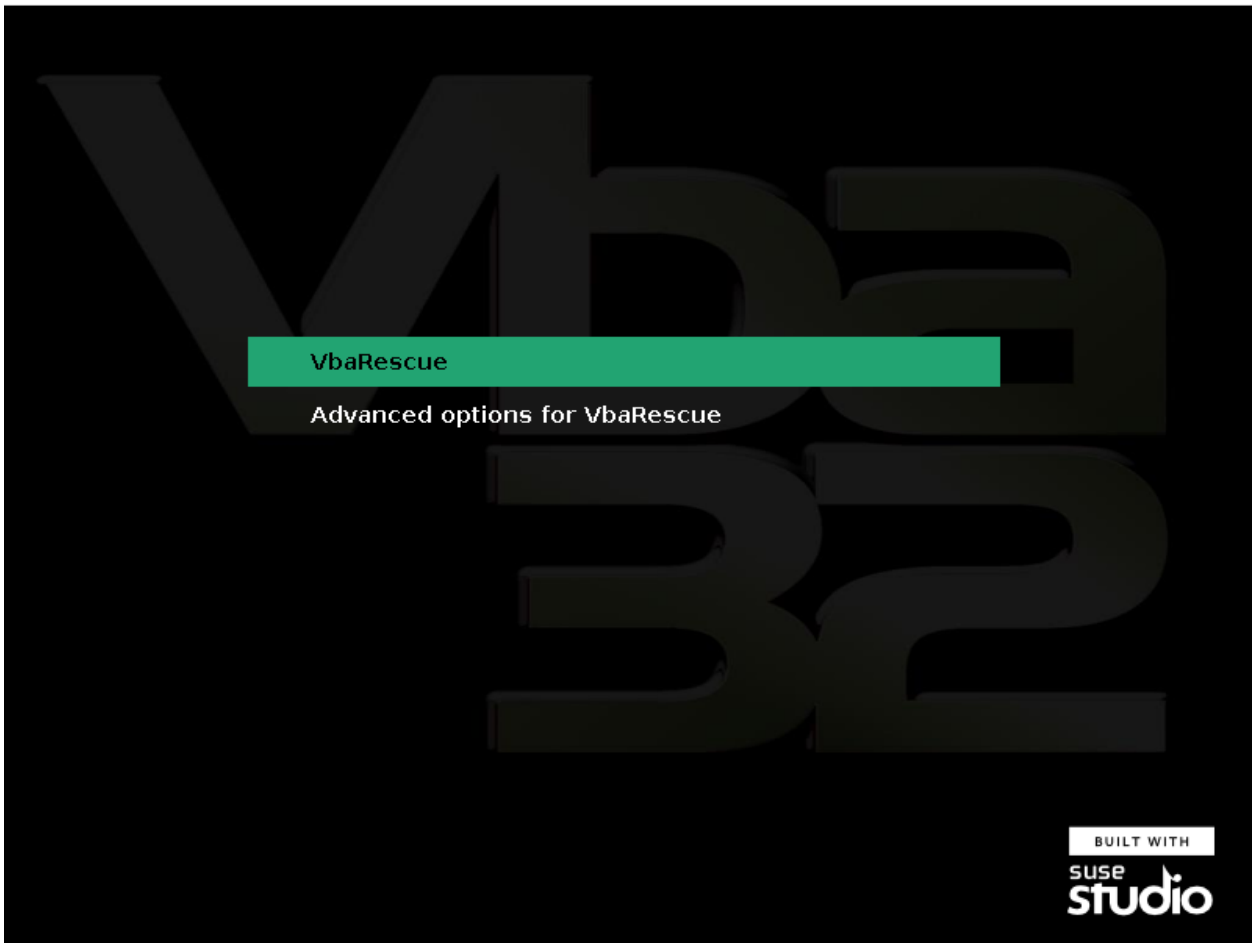

Рисунок 3.1 – Выбор режима работы Vba32 Rescue

- **VbaRescue** – стандартный режим работы Спасательного образа
- **Advanced options for VbaRescue** – загрузка образа с дополнительными настройками

VbaRescue позволяет загрузить пользовательский интерфейс спасательного образа в стандартном режиме (Рисунок 4.1).

Advanced options for VbaRescue позволяет выбрать дополнительные опции при запуске спасательного образа (Рисунок 3.2):

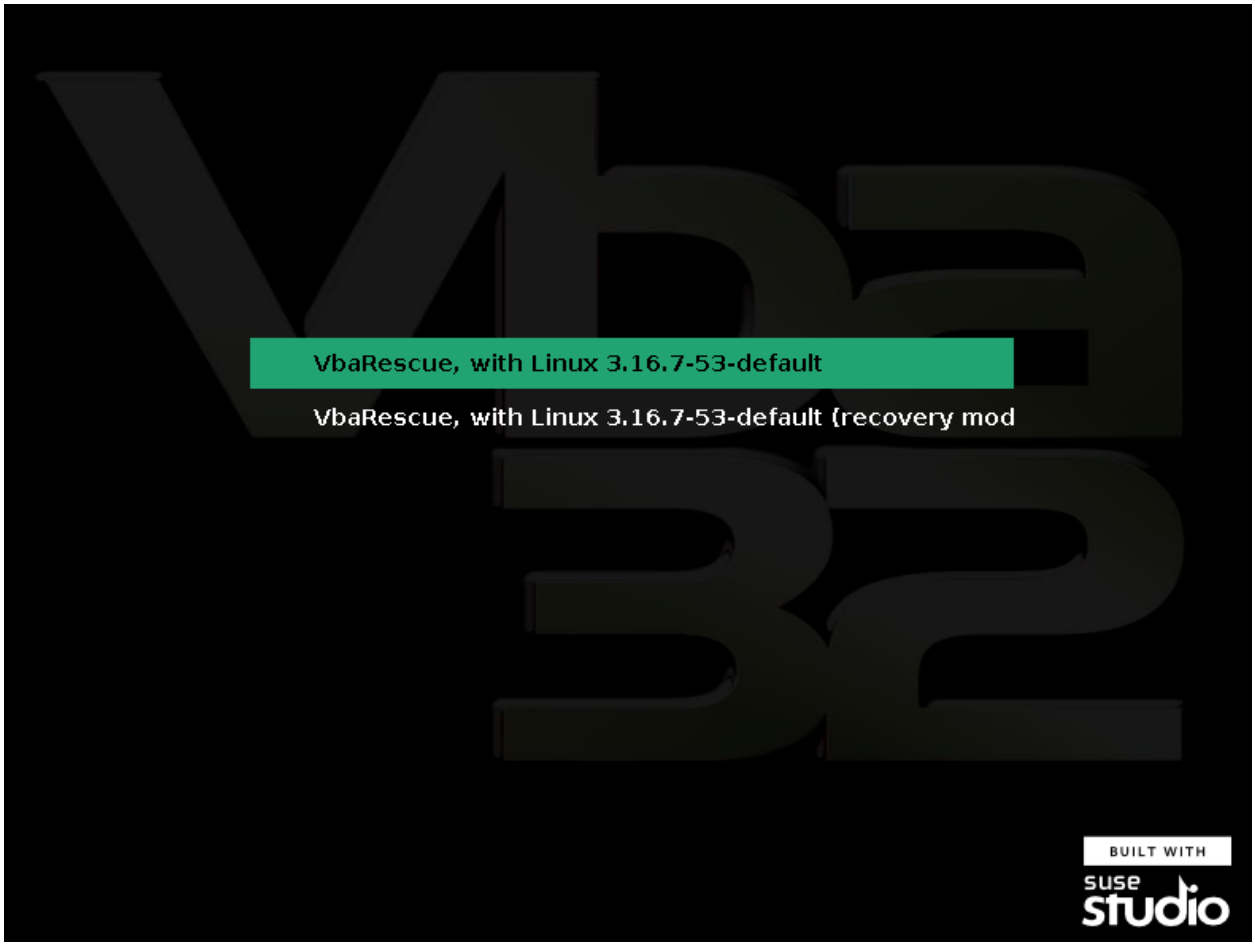

Рисунок 3.2 – Выбор дополнительных опций для VbaRescue

- **VbaRescue, with Linux 3.16.7-53-default**
- **VbaRescue, with Linux 3.16.7-53-default (recovery mod)**

VbaRescue, with Linux 3.16.7-53-default позволяет запустить спасательный образ в среде Linux 3.16.7-53-default.

VbaRescue, with Linux 3.16.7-53-default (recovery mod) позволяет запустить спасательный образ в среде Linux 3.16.7-53-default в режиме восстановления системы.

Выбор любого из данных режимов приведёт к загрузке пользовательского интерфейса спасательного образа **Vba32 Rescue** (Рисунок 4.1)

4. Пользовательский интерфейс Vba32 Rescue

Выбрав режим загрузки спасательного образа **Vba32 Rescue**, пользователь попадёт на главное меню (Рисунок 4.1).

Навигация по меню осуществляется при помощи следующих клавиш:

- Вверх/Вниз – навигация по спискам меню;
- Лево/Право – навигация по кнопкам действия;
- Пробел – включение/выключение выбранного пункта;
- Ввод – вход в меню или принятие изменений;
- Выход – выход из меню или отмена изменений;
- Цифры – быстрый выбор пункта меню. Переключение между полями ввода и другими элементами

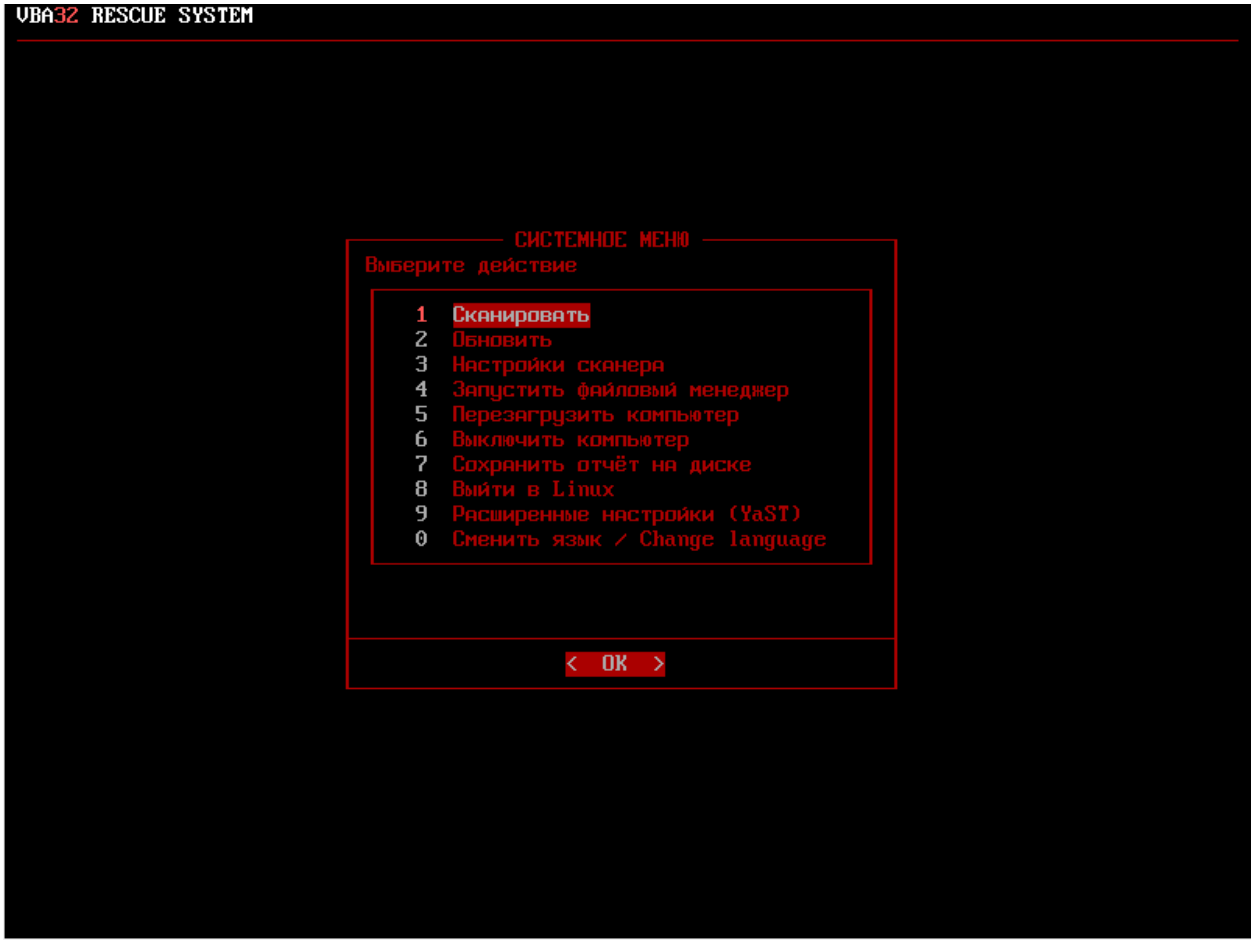

Рисунок 4.1 – Главное меню пользовательского интерфейса спасательного образа Vba32 rescue

В главном меню представлен список действий со спасательным образом.

- Сканировать
- Обновить
- Настройки сканера

- Запустить файловый менеджер
- Перезагрузить компьютер
- Выключить компьютер
- Сохранить отчёт на диске
- Выйти в Linux
- Расширенные настройки (YaST)
- Change language / Сменить язык

Сканировать – Позволяет начать сканирование системы на наличие вредоносных программ (Рисунок 4.2)

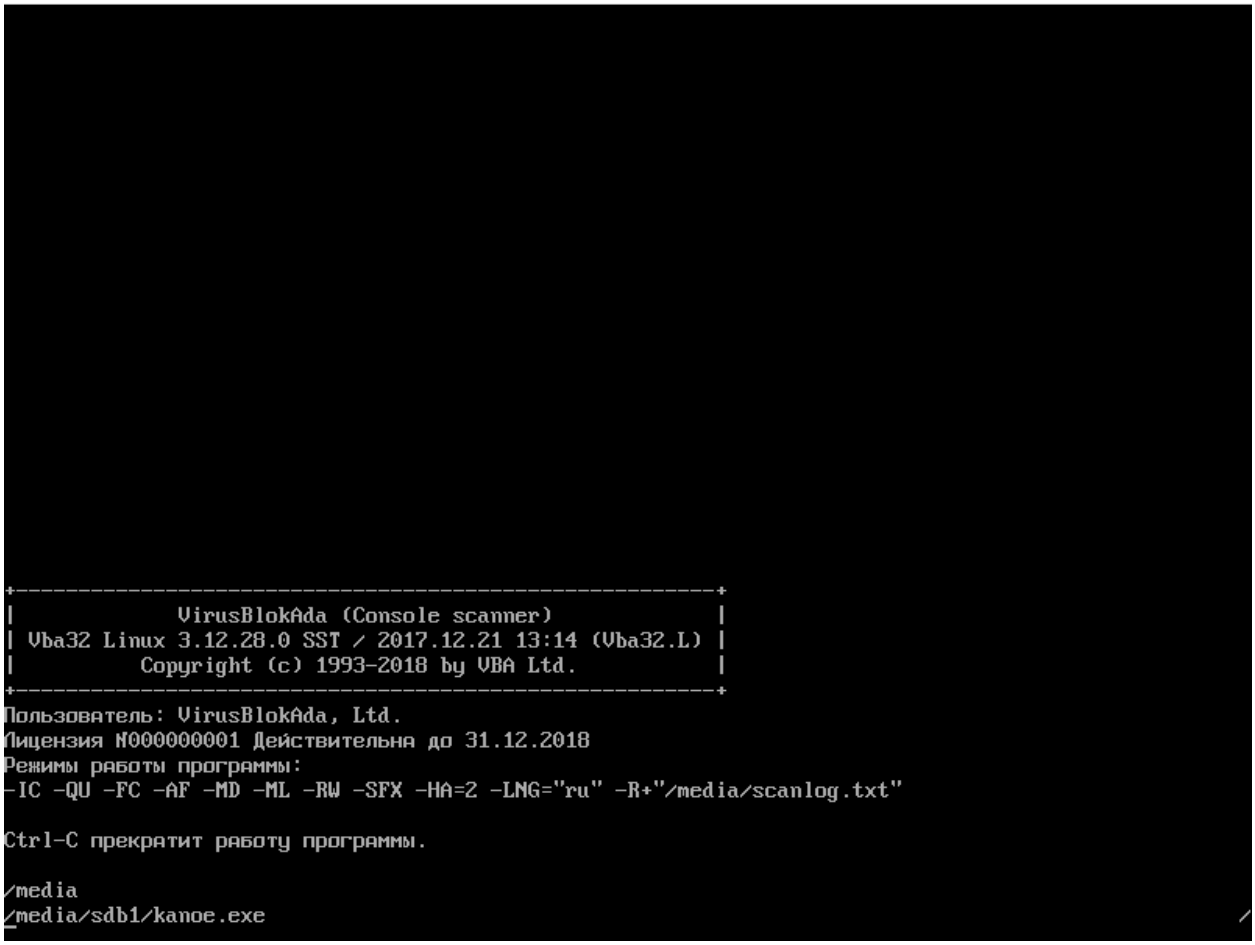

Рисунок 4.2 – Сканирование компьютера спасательным образом Vba32 Rescue

Обновить – позволяет обновить антивирусные базы, используемые сканером спасательного образа **Vba32 Rescue** (Рисунок 4.3).

Рисунок 4.3 – Обновление антивирусных баз сканера спасательного образа Vba32 Rescue

Примечание. Для обновления антивирусных баз необходимо, чтобы спасательный образ Vba32 Rescue работал в полноценном режиме. Для активации полноценного режима необходимо иметь действующий ключ данного продукта. Описание активации спасательного образа представлено в разделе «**Активация спасательного образа Vba32 Rescue»**

Настройка сканера – позволяет задать настройки, используемые сканером спасательного образа **Vba32 Rescue** (рисунок 4.4):

- Сканировать файлы в архивах (AR+) – задаёт необходимость проверки архивов
- Параноидальная эвристика (HA=3) – задаёт режим эвристического анализа (Оптимальный/Избыточный)
- Лечить или удалять инфицированные файлы (FC+) – задаёт действия над инфицированными файлами
- Сканировать почту (ML+) – задаёт необходимость сканировать почту
- Удалять инфицированные сообщения (MD+) – задаёт действия над инфицированными сообщениями

- Удалять инфицированные архивы (AD+) – задаёт действия над инфицированными архивами
- Удалять подозрительные файлы (SD+) – задаёт действия над подозрительными файлами
- Копировать вредоносные файлы в /var/virus

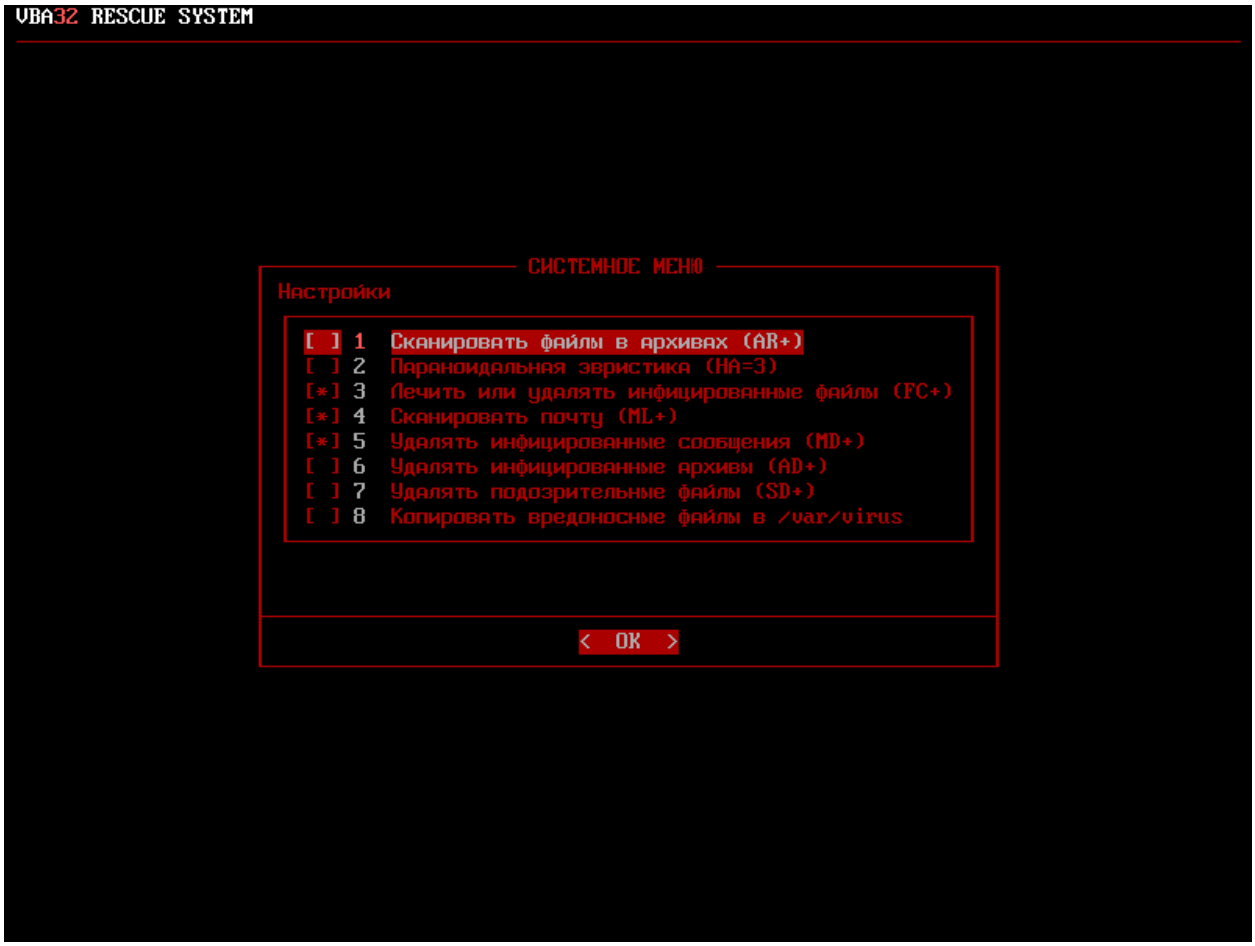

Рисунок 4.4 – Настройки сканера спасательного образа Vba32 Rescue

Запустить файловый менеджер – запускает встроенный файловый менеджер Midnight Commander (рисунок 4.5).

Midnight Commander — файловый менеджер с текстовым интерфейсом типа Norton Commander для UNIX-подобных операционных систем. Файловый менеджер предоставляет интуитивно понятный пользовательский интерфейс и позволяет выполнять наиболее частые операции над файлами — создание, просмотр, редактирование, перемещение, переименование, копирование, удаление и др. Домашняя страница проекта: http://www.midnight-commander.org.

Рисунок 4.5 – пользовательский интерфейс файлового менеджера Midnight Commander

Перезагрузить компьютер – позволяет пользователю перезагрузить компьютер.

Выключить компьютер – позволяет пользователю выключить компьютер

Сохранить отчёт на диске – позволяет пользователю сохранить отчёт о сканировании компьютера на диске.

Выйти в linux – позволяет пользователю закрыть пользовательский интерфейс спасательного образа **Vba32 Rescue** и продолжить дальнейшую работу в среде linux.

Примечание. Данный пункт рассчитан на опытных пользователей и не рекомендуется для использования новичками.

Расширенные настройки (YaST) – данный пункт предназначен для ручной настройки системы Linux. (Рисунок 4.6).

YaST - это программа, используемая в openSUSE и SUSE Enterprise Linux для установки системы и ее администрирования после установки. Он пользуется популярностью за простоту в использовании, привлекательный

графический интерфейс и возможность настроить систему быстро во время и после установки. YaST - это *Еще Один Инструмент Настройки* (Yet another Setup Tool). YaST может использоваться для настройки всей системы. Установка оборудования, настройка сети и системных сервисов, настройка параметров безопасности - это лишь несколько примеров. Все задачи могут быть достигнуты с помощью *Панели управления YaST*.

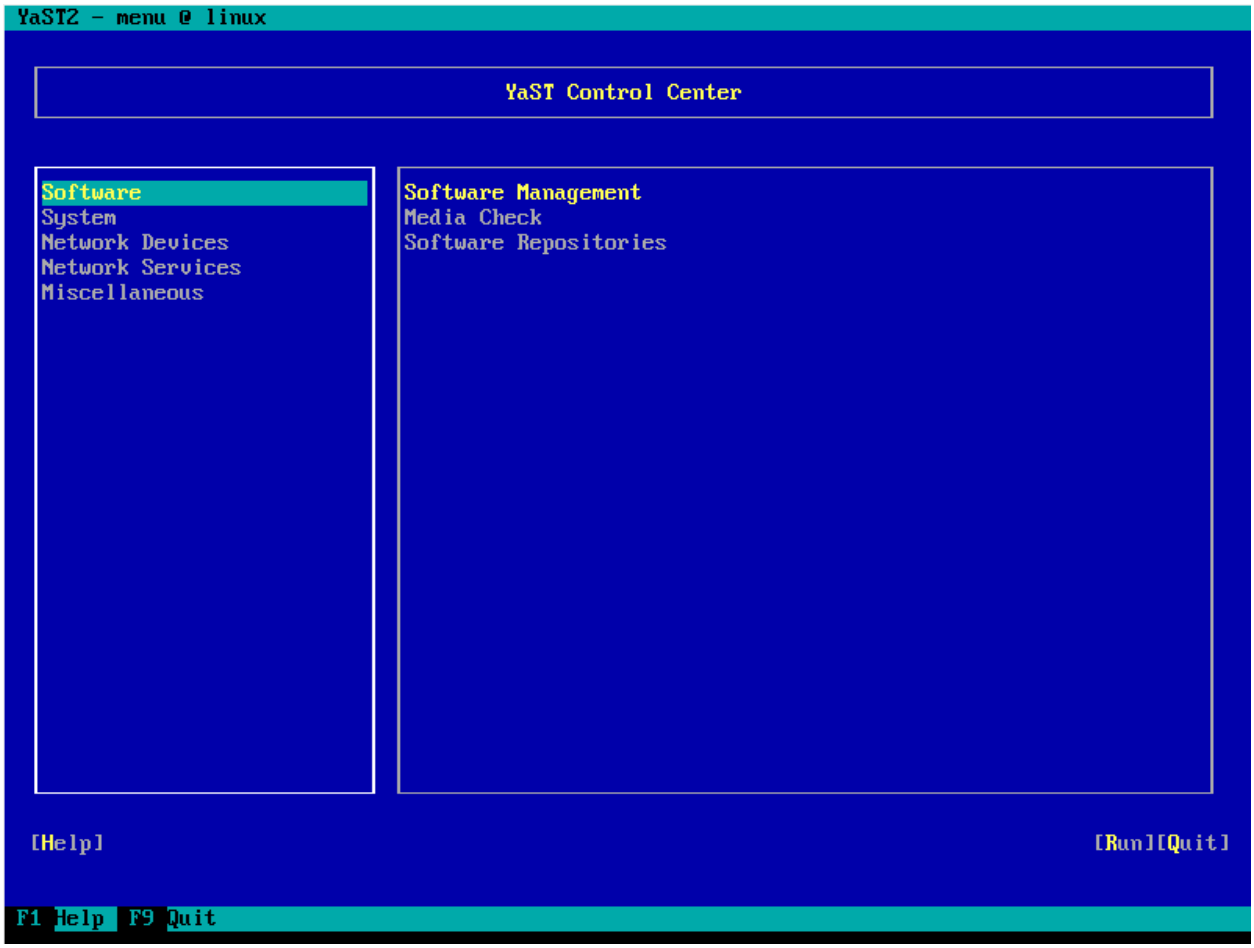

Рисунок 4.6 – пользовательский интерфейс настроек YaST

Change language / Сменить язык – позволяет сменить язык интерфейса спасательного образа **Vba32 Rescue**

5. Активация спасательного образа Vba32 Rescue

По умолчанию сканер спасательного образа работает в ознакомительном режиме. Чтобы активировать полный режим необходимо в корень флешки со спасательным образом скопировать действующий ключевой файл. Для этой операции можно воспользоваться файловым менеджером, встроенным в спасательный образ.