УТВЕРЖДЕН

BY.ИАДВ.00131-02 90 01-ЛУ

КОМПЛЕКС VBA32 ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Консольный сканер для Linux

Руководство администратора

BY.ИАДВ.00131-02 90 01

Листов 12

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

2019

Литера

№ изм.	*Подп.*	*Дата*

АННОТАЦИЯ

Данный документ содержит описание применения консольного антивирусного сканера для Linux.

Разработчиком консольного антивирусного сканера для Linux является ОДО «ВирусБлокАда».

Консольный антивирусный сканер предназначен для защиты ПК, работающих под управлением ОС, совместимых с Linux на x86 процессоре и библиотеке glibc 2.18 и выше.

Консольный антивирусный сканер позволяет:

1) обнаруживать и обезвреживать:
   - резидентные компьютерные вирусы в оперативной памяти;
   - известные файловые компьютерные вирусы: исполняемые, интерпретируемые, макрокомандные, комбинированные, шифрованные, сложнополиморфные, «стелс» (при этом используется эмулятор процессора для обнаружения полиморфных и шифрованных вирусов);
   - известные почтовые «черви», «троянские» программы, программы типа «backdoor», программные закладки;
   - вредоносные программы в сообщениях, содержащихся в почтовых базах MS Outlook;
2) обнаруживать:
   - компьютерные вирусы в запакованных (UPX, PECompact, ASPack и т.д.) исполняемых файлах (при этом использование эмулятора процессора не требует введения процедур распаковки для каждого запаковщика);
   - неизвестные компьютерные вирусы (при помощи эвристического анализа);
   - неизвестные модификации «троянских» программ;
   - компьютерные вирусы в архивах RAR / ZIP / HA / ARJ / TAR / GZIP / BZIP2;
3) перемещать, удалять, переименовывать инфицированные и подозрительные объекты.
4) обрабатывать файлы по списку;
5) отображать информацию о макросах в документах MS Office;
6) удалять:
   - сообщения, содержащие компьютерные вирусы, в почтовых базах MS Outlook Express 4 и 5, The Bat!;
   - архивы, содержащие инфицированные файлы;
7) осуществлять контроль целостности компонент комплекса;
8) включать:
   - режим протоколирования событий.
9) задавать параметры работы из командной строки.

СОДЕРЖАНИЕ

_Toc378596200

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Консольный антивирусный сканер предназначен для защиты ПК, работающих под управлением ОС, совместимых с Linux на x86 процессоре и библиотеке glibc 2.18 и выше.

Консольный антивирусный сканер позволяет:

1) обнаруживать и обезвреживать:
   - известные файловые компьютерные вирусы: исполняемые, интерпретируемые, макрокомандные, комбинированные, шифрованные, сложнополиморфные, «стелс» (при этом используется эмулятор процессора для обнаружения полиморфных и шифрованных вирусов);
   - известные почтовые «черви», «троянские» программы, программы типа «backdoor», программные закладки;
   - вредоносные программы в сообщениях, содержащихся в почтовых базах MS Outlook;
2) обнаруживать:
   - компьютерные вирусы в запакованных (UPX, PECompact, ASPack и т.д.) исполняемых файлах (при этом использование эмулятора процессора не требует введения процедур распаковки для каждого запаковщика);
   - неизвестные компьютерные вирусы (при помощи эвристического анализа);
   - неизвестные модификации «троянских» программ;
   - компьютерные вирусы в архивах RAR / ZIP / HA / ARJ / TAR / GZIP / BZIP2;
3) перемещать, удалять, переименовывать инфицированные и подозрительные объекты.
4) обрабатывать файлы по списку;
5) отображать информацию о макросах в документах MS Office;
6) удалять:
   - сообщения, содержащие компьютерные вирусы, в почтовых базах MS Outlook Express 4 и 5, The Bat!;
   - архивы, содержащие инфицированные файлы;
7) осуществлять контроль целостности компонент комплекса;
8) включать:
   - режим протоколирования событий.
9) задавать параметры работы из командной строки.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

При работе программы используются ПК на базе архитектуры Intel x86. Аппаратная конфигурация ПК должна удовлетворять требованиям используемой ОС. Для установки консольного антивирусного сканера требуется не менее 500 МБ свободного дискового пространства на жестком диске ПК.

Минимальный объем ОЗУ – 500 МБ.

При использовании функции хранения копий инфицированных/подозрительных сообщений необходим достаточный объем свободного дискового пространства, размер которого определяется потребностями пользователя.

2.2. Требования к программным средствам

Консольный антивирусный сканер предназначен для защиты ПК, работающих под управлением ОС, совместимых с Linux на x86 процессоре и библиотеке glibc 2.18 и выше.

2.3. Общие характеристики входной и выходной информации

Входными данными для консольного антивирусного сканера являются:

- Параметры командной строки в формате:
  VBA32X.EXE [путь] ... [путь] [-ключ] ... [-ключ]
  где ПУТЬ - \каталог[\...\каталог\[файл]];
  @имя_файла - обработка списка файлов
  КЛЮЧ - задает режимы работы программы:
- Проверяемые файлы;
- Ключевой файл;

Выходными данными для консольного антивирусного сканера являются:

- Отчет о работе программы в текстовом виде.
- Изменения файлов и файловой системы, необходимые для обезвреживания ВП.

3. ОПИСАНИЕ ЗАДАЧИ

Консольный сканер позволяет управлять своими режимами с помощью параметров, вводимых в командной строке. Вызов программы осуществляется из командной строки следующим образом:

vbacl [путь] … [путь] [-ключ] … [-ключ],

где ПУТЬ - \каталог\...\каталог\, @имя_файла – обработка списка файлов;

КЛЮЧ - задает режимы работы программы:

-?[+|-] – вывод справки. Этот экран;

-M=1 – быстрый режим обработки;

-M=2 – нормальный режим обработки;

-M=3 – углубленный режим обработки;

-AF[+|-] – все файлы;

-PM[+|-] – избыточный поиск;

-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;

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

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

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

-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;

-OK[+|-] – включение имен «чистых» файлов в отчет;

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

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

-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;

-EXT= - установить список проверяемых расширений;

-EXT+ - добавить расширения в список по умолчанию;

-EXT- - исключить расширения из списка по умолчанию.

По умолчанию включены параметры, указанные в файле vbacl.ini (параметр DEFAULT_OPTIONS).

Данная программа позволяет использовать ее в пакетном режиме. При этом применяются те же параметры, что и при запуске из командной строки. Программа имеет следующие коды возврата для обработки в пакетном режиме:

- 000 - нормальное завершение, вирусы не обнаружены;
- 004 - тестирование прервано;
- 006 - обнаружены модификации вирусов;
- 007 - обнаружены вирусы в режиме "Тестировать, не лечить";
- 008 - обнаружены вирусы в режиме "Лечение".

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для консольного антивирусного сканера являются:

– Параметры командной строки в формате:
  vbacl [путь] ... [путь] [-ключ] ... [-ключ]
  где ПУТЬ - \каталог[\...\каталог\[файл]];
  @имя_файла - обработка списка файлов
  КЛЮЧ - задает режимы работы программы:
– Проверяемые файлы;
– Ключевой файл;

Выходными данными для консольного антивирусного сканера являются:

– Отчет о работе программы в текстовом виде.
– Изменения файлов и файловой системы, необходимые для обезвреживания ВП.

5. ОСНОВНЫЕ МЕРЫ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Организационные меры защиты

Основными организационными мерами обеспечения защиты от воздействия вредоносных программ, позволяющими уменьшить риск заражения ресурсов вычислительной техники и минимизировать отрицательные последствия в случае попадания ВП в вычислительную систему, являются следующие:

- обучение пользователей правилам безопасности, путям и причинам распространения ВП, методам профилактики;
- разработка инструкций и правил работы, контроль их выполнения;
- разработка плана действий пользователей и должностных лиц по локализации возможных вредоносных программ для уменьшения ущерба;
- разработка и внедрение правил, исключающих возможности использования не проверенного (не лицензионного) программного обеспечения.

5.2. Организационно-технические меры защиты

Правильная настройка программного обеспечения, установление минимально необходимых прав доступа пользователей к ресурсам вычислительной техники позволяют уменьшить риск заражения и потери. Следующие организационно – технические меры позволяют уменьшить потенциальную опасность от атак компьютерных вирусов:

- отключение в BIOS SETUP загрузки с дискеты;
- использование режима «защита загрузочного сектора от записи» в BIOS;
- резервное копирование ценной информации;
- установление минимально необходимых прав доступа к сетевым ресурсам.

5.3. Профилактика

Систематическая проверка целостности программного обеспечения с помощью программ защиты от воздействия ВП позволяет предупредить массовое распространение ВП. Одной из обязательных мер профилактики является проверка всей входящей информации.

В критических местах технологических звеньев серьезной профилактической мерой будет использование форматов документов, не содержащих управляющих структур (например «.TXT», «.RTF»).

6. МАРКИРОВКА СЕРТИФИЦИРУЕМОЙ ПРОДУКЦИИ

Знак соответствия, приведенный на рис. 1, означает, что консольный антивирусный сканер соответствует требованиям ТР 2013/027/BY.

Рис. 1

Знак соответствия, приведенный на рис. 2, означает, что система менеджмента качества применительно к проектированию, производству и технической поддержке консольного антивирусного сканера соответствует требованиям СТБ ISO 9001.

Рис. 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе использованы следующие сокращения:
ВП – вредоносная программа;
ИТ – информационная технология;
ОС – операционная система;
ПК – персональный компьютер;
ПО – программное обеспечение.

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводи-тельного докум. и дата*	*Подп.*	*Дата*
Изм.	*измененных*	*замененных*	*новых*	*аннулированных*					

№ изм.	*Подп.*	*Дата*