УТВЕРЖДЕН

BY.ИАДВ.00137-01 90 01-ЛУ

КОМПЛЕКС VBA32 ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Консольный сканер для Windows

Руководство администратора

BY.ИАДВ.00137-01 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 руководство администратора консольного сканера для ОС Windows.

Консольный сканер для ОС Windows является средством защиты от воздействия вредоносных программ.

Разработчиком консольного сканера для ОС Windows является ОДО «ВирусБлокАда».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Консольный сканер предназначен для защиты персональных компьютеров и серверов, работающих под управлением ОС Windows XP SP3, Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 от воздействия вредоносных программ.

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.

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 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 сканер функционирует на рабочих станциях и серверах под управлением ОС Windows XP SP3, Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

2.3. Общие характеристики входной и выходной информации

Входными данными для консольного антивирусного сканера являются:

- Параметры командной строки;
- 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 вредоносных программ.

3. ОПИСАНИЕ ЗАДАЧИ

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

3.1 Работа с консольным сканером посредством командной строки

Синтаксис командной строки следующий:

Для Windows:

vba32w.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/ка 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 .

3.2 Обновление консольного сканера

– Обновление консольного сканера обеспечивается запуском файла update.bat и происходит в автоматическом режиме.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для консольного антивирусного сканера являются:

- Параметры командной строки;
- Проверяемые файлы;
- Ключевой файл.

Параметры командной строки изменяются в зависимости от решаемой задачи и должны соответствовать параметрам, приведенным в разделе 3.

Проверяемые файлы задаются администратором для проверки воздействия на них вредоносных программ. При этом для проверки может быть задан как диск, каталог с файлами так и отдельный файл.

Ключевой файл предназначен для перевода работы консольного сканера в полнофункциональный режим. При отсутствии ключевого файла или при истечении его срока действия консольный сканер будет работать в демонстрационном режиме.

Выходными данными для консольного антивирусного сканера являются:

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

Отчет о работе программы в текстовом виде содержит информацию о времени проведения сканирования и его результаты.

Изменения файлов и файловой системы, необходимые для обезвреживания вредоносных программ подразумевают удаление вредоносных программ, а также обезвреживание вредоносных программ внедренных в легитимные файлы операционной системы, прикладных программ и файлов данных.

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 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 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*

Лист регистрации изменений									