УТВЕРЖДЕН

BY.ИАДВ.00119-03 90 01-ЛУ

# КОМПЛЕКС VBA32 ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

**Антивирусный фильтр для почтового сервера Exim**

**Руководство администратора**

**BY.ИАДВ.00119-03 90 01**

**Листов 15**

| | |
|---|---|
| *Подп. и дата* | |
| *Инв. N* | |
| *Взам. инв.* | |
| *Подп. и дата* | |
| *Инв.N* | |

2019

Литера

| | | |
|---|---|---|
| | | |
| *№ изм.* | *Подп.* | *Дата* |

## АННОТАЦИЯ

Данный документ содержит руководство администратора антивирусного фильтра для почтового сервера Exim, функционирующего под управлением операционной системы Linux.

Разработчиком антивирусного фильтра для почтового сервера Exim является ОДО «ВирусБлокАда».

Антивирусный фильтр для почтового сервера Exim предназначен для защиты клиентов почтовой системы от воздействия вредоносных программ и компьютерных вирусов, которые могут содержаться во входящих и исходящих почтовых сообщениях.

Антивирусный фильтр для почтового сервера Exim обеспечивает:

- проверку поступающих на сервер почтовых сообщений;
- гибкость и удобство настройки действий, выполняемых над почтовыми сообщениями, содержащими вредоносные программы или компьютерные вирусы, подозрительные файлы и неизвестные макросы: отсылка уведомлений, сохранение копий в заданном каталоге, добавление строк в тему письма и mime-заголовок;
- настройку политики безопасности по отношению к сообщениям ContentType=message/partial;
- использование файлов шаблонов для отсылаемых сообщений, настраиваемых администратором;
- использование эвристического анализатора антивирусного ядра увеличивает шансы обнаружения новых неизвестных вирусов и таким образом возможность предотвращения эпидемий новых вирусов;
- проверку множества архивов различных типов и файлов, упакованных различными упаковщиками;
- автоматическую корректировку конфигурационного файла с возможностью уведомления администратора при наличии неправильно заданных значений параметров;
- многопоточный режим работы фильтра;
- обновление антивирусных баз без перезагрузки.

Антивирусный фильтр для почтового сервера Exim состоит из следующих модулей:

- vbaExim f – модуль фильтра;
- Exim -pipe – модуль, обеспечивающий взаимодействие с Exim;
- vbaupdater – модуль обновления.

## СОДЕРЖАНИЕ

# 1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Антивирусный фильтр для почтового сервера Exim предназначен для защиты клиентов почтовой системы от воздействия вредоносных программ и компьютерных вирусов, которые могут содержаться во входящих и исходящих почтовых сообщениях.

Антивирусный фильтр для почтового сервера Exim обеспечивает:

- проверку поступающих на сервер почтовых сообщений;
- гибкость и удобство настройки действий, выполняемых над почтовыми сообщениями, содержащими вредоносные программы или компьютерные вирусы, подозрительные файлы и неизвестные макросы: отсылка уведомлений, сохранение копий в заданном каталоге, добавление строк в тему письма и mime-заголовок;
- настройку политики безопасности по отношению к сообщениям ContentType=message/partial;
- использование файлов шаблонов для отсылаемых сообщений, настраиваемых администратором;
- использование эвристического анализатора антивирусного ядра увеличивает шансы обнаружения новых неизвестных вирусов и таким образом возможность предотвращения эпидемий новых вирусов;
- проверку множества архивов различных типов и файлов, упакованных различными упаковщиками;
- автоматическую корректировку конфигурационного файла с возможностью уведомления администратора при наличии неправильно заданных значений параметров;
- многопоточный режим работы фильтра;
- обновление антивирусных баз без перезагрузки.

# 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 антивирусного фильтра для почтового сервера Exim 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

Антивирусный фильтр для почтового сервера Exim функционирует под управлением операционной системы Linux совместно с Exim версий 3.xx, 4.xx. Также должна быть установлена библиотека glibc версии 2.18 и выше.

## 2.3. Общие характеристики входной и выходной информации

Входными данными для антивирусного фильтра являются почтовые сообщения в mime-формате, передаваемыми на проверку почтовой системой.

Выходными данными для антивирусного фильтра являются результаты проверки в виде числового (текстового) кода, сообщаемые фильтром почтовой системе.

# 3. ОПИСАНИЕ ЗАДАЧИ

## 3.1. Установка

Антивирусный фильтр поставляется в виде архива vbaExim f-[version].tar.gz, где version – версия пакета. Архив содержит:

- модуль обновления;
- фильтр для Exim;
- конфигурационный файл фильтра;
- антивирусные базы.

Для установки фильтра необходимо в командной строке последовательно ввести следующие команды:

- tar zxf vbaExim f-[version].tar.gz (распаковать архив);
- cd vbaExim f-[version] (зайти в распакованную директорию).
- скопировать ключевой файл в /opt/vba/vba32.key;
- создать для фильтра пользователя vbauser и группу vbagroup;
- после этого необходимо запустить скрипт установки (в командной строке набрать ./install).
- назначить параметры файлам фильтра:
  chown -R vbauser:vbagroup /etc/vba/vbaExim f* /opt/vba/vbaExim f /var/run/vba/vbaExim f /var/log/vba /usr/bin/vbaExim f-ctl
  chmod 0700 /usr/bin/vbaExim f-ctl
  chmod 4700 /opt/vba/vbaExim f/bin/vba*

Далее необходимо настроить взаимодействие фильтра и почтовой системы Exim. Для этого необходимо внести изменения в конфигурационный файл Exim (configure).

В файл конфигурации Exim необходимо внести следующие изменений:

Добавить в начало конфигурационного файла Exim (или изменить, если они уже существуют) следующие параметры транспорта для фильтра.

---------- insert ----------
```
##############################################################################
# MESSAGE FILTER CONFIGURATION SETTINGS #
##############################################################################
```
---------- insert ----------

Добавить к существующим или создать trusted user и group для Exim :

---------- insert ----------
```
trusted_users = _user_used_by_vba_
trusted_groups = _user_used_by_vba_
```
---------- insert ----------

добавить (или модифицировать, если они уже имеются) следующие опции:

Для Exim версии 3 (3.xx):

---------- insert ----------
```
message_filter = /opt/vba/vbaExim f/bin/system_filter.Exim
message_filter_pipe_transport = filter_pipe
message_filter_reply_transport = address_reply
```
---------- insert ----------

Для Exim версии 4 (4.xx):

---------- insert ----------
```
system_filter = /opt/vba/vbaExim f/bin/system_filter.Exim
```

system_filter_pipe_transport = filter_pipe
system_filter_reply_transport = address_reply
---------- insert ----------

Транспорт address_reply должен быть объявлен как минимум в следующем виде:

address_reply:
driver = autoreply

Обычно этот транспорт объявлен в конфигурации Exim по умолчанию, поэтому необходимо только убедиться в его наличии.

Далее в разделе

---------- insert ----------
##########################################################################
# TRANSPORTS CONFIGURATION #
##########################################################################
# ORDER DOES NOT MATTER #
# Only one appropriate transport is called for each delivery. #
##########################################################################
---------- insert ----------

необходимо добавить описание соответствующего транспорта:

---------- insert ----------
filter_pipe:
driver = pipe
user = _user_used_by_vba_
group = _user_used_by_vba_
return_fail_output
---------- insert ----------

Создать линк /opt/vba/vbaExim f/bin/Exim на исполняемый файл Exim .

Например, командой ln -s /usr/local/bin/Exim /opt/vba/vbaExim f/bin/Exim, если Exim установлен в директории /usr/local/bin.

Установка антивирусного фильтра для почтового сервера Eximи интегрирование его с почтовой системой Exim закончена.

### 3.2. Настройка

Конфигурационный файл vbaExim .conf разбит на секции, каждая из которых содержит логически связанные параметры. Название параметра приводится в одном из следующих вариантов:

- Parameter = value. В данном случае value является значением, заданным в конфигурационном файле по-умолчанию.
- Parameter = {list of values}. В данном случае list of values представляет собой перечисленные через запятую значения, которые может принимать параметр.

Для каждого параметра приводится краткое описание его назначения, затем - возможные значения, которые он может принимать.

Секция [Infected] содержит параметры, относящиеся к обработке инфицированных сообщений:

1) Action= {skip, discard} Определяет действие, выполняемое над инфицированными сообщениями.
   - skip – продолжить передачу сообщения пользователю;
   - discard – не доставлять сообщение пользователю.
2) CopyToDir = {yes, no} Определяет возможность сохранения копии инфицированного сообщения.

- yes – сохранять копию;
- no – не сохранять копию.

3) CopyDirPath = /opt/vba/vbaExim f/infected/ Указывает путь к каталогу для сохранения копий инфицированных сообщений. /opt/vba/vbaExim f/infected/ - является путем по умолчанию. При необходимости можно указать путь к другому существующему каталогу.
4) SenderNotify = {yes, no}
   RcptNotify = {yes, no}
   Определяют возможность отсылки уведомлений отправителю (SenderNotify) и получателю (RcptNotify) инфицированного сообщения.
   - yes – отправлять уведомление;
   - no – не отправлять уведомление.
5) SenderNotifyTemplate = /etc/vba/vbaExim f.template.msg RcptNotifyTemplate = /opt/vba/vbaExim f.templates/template.msg
   Определяют способ уведомления пользователей об инфицированном сообщении. Значение параметра указывает путь.

Секция [Suspicious] содержит параметры, относящиеся к обработке подозрительных сообщений:

1) HeuristicLevel = {0, 1, 2, 3} Определяет уровень эвристического анализатора:
   - 0 – отключен;
   - 1 – средний;
   - 2 – максимальный.
   - 3 – избыточный.

   Уровень эвристического анализатора определяет объем дополнительных действий, производимых антивирусным демоном при обработке объектов, для обнаружения новых неизвестных вредоносных программ и компьютерных вирусов. Таким образом, на почтовом сервере рекомендуется установить средний (1) уровень эвристического анализатора, для увеличения вероятности предотвращения эпидемий новых вирусов.
2) Action= {skip, discard} Определяет действие, выполняемое над инфицированными сообщениями.
   - skip – продолжить передачу сообщения пользователю;
   - discard – не доставлять сообщение пользователю.
3) CopyToDir = {yes, no} Определяет возможность сохранения копии подозрительного сообщения.
   - yes – сохранять копию;
   - no – не сохранять копию.
4) CopyDirPath = /opt/vba/vbaExim f/infected/ Указывает путь к каталогу для сохранения копий подозрительных сообщений. /opt/vba/vbaExim f/suspicious/ является путем по умолчанию. При необходимости можно указать путь к другому существующему каталогу.
5) SenderNotify = {yes, no}
   RcptNotify = {yes, no}
   Определяют возможность отсылки уведомлений отправителю (SenderNotify) и получателю (RcptNotify) подозрительного сообщения.
   - yes – отправлять уведомление;
   - no – не отправлять уведомление.
6) SenderNotifyTemplate = /etc/vba/vbaExim f.templates/template.msg RcptNotifyTemplate = /etc/vba/vbaExim f.templates/template.msg

Определяют способ уведомления пользователей об подозрительном сообщении. Значение параметра указывает путь к шаблону отсылаемого уведомления.

Секция [WithMacros] содержит параметры, относящиеся к обработке сообщений, содержащих неизвестные макросы. Описания всех параметров аналогичны соответствующим в вышеописанных секциях (Action, CopyToDir, CopyToDirPath, SenderNotify, RcptNotify, SenderNotifyTemplate, RcptNotifyTemplate).

Секция [Notifications] описывает параметры настройки отсылки уведомлений администратору. Значения параметров (OnVirus, OnSuspicious, OnWithMacros, OnError, OnVirusTemplate, OnSuspiciousTemplate, OnWithMacrosTemplate, OnErrorTemplate) аналогичны секции Infected (SenderNotify, SenderNotifyTemplate), далее приводится только общее описание их назначения:

1) OnVirus – отсылка уведомления об обнаруженном инфицированном сообщении;
2) OnSuspicious – отслылка уведомления об обнаруженном подозрительном сообщении;
3) OnWithMacros – отсылка уведомления об обнаруженном сообщении с неизвестными макросами;
4) OnError – отсылка уведомления о некоторой внутренней ошибке в антивирусном фильтре для почтового сервера Exim. Ошибкой является:
   - завершение срока действия ключевого файла (почтовый фильтр будет переведен в демонстрационный режим работы);
   - неправильно заданные значения параметров конфигурационного файла (активизируются значения по-умолчанию).

Секция [Common] описывает дополнительные настройки общего назначения, относящиеся к системе в целом:

1) MarkMessage = {yes, no} Определяет возможность добавления в RFC-822 заголовок сообщения строки о результате проверки сообщения.
   - `yes` – добавлять строку в заголовок сообщения;
   - `no` – не добавлять строку в заголовок сообщения.
2) В RFC-822 заголовок сообщения добавляется строка вида XVBA = result, где result отражает результат проверки сообщения и может принимать одно из следующих значений: Checked, Infected, Suspicious, WithMacros. Данная строка может быть использована почтовым клиентом пользователя для определения результата проверки сообщения сервером.
3) MarkSubject = {yes, no}
   Определяет возможность добавления в тему сообщения строки о результате проверки сообщения.
   - yes – добавлять строку в тему сообщения;
   - no – не добавлять строку в тему сообщения.

   В тему сообщения добавляется строка вида [VBA32: result], где result отражает результат проверки сообщения и может принимать одно из следующих значений: Checked, Infected, Suspicious, WithMacros.
4) `LogLevel = {low | high}` Уровень детализации выводимых в лог сообщений.
   - low – низкий уровень детализации сообщений (выводятся сообщения о проверяемом объекте, только если он является инфицированным / подозрительным / содержит неизвестные макросы);
   - high – высокий уровень детализации сообщений (выводятся сообщения о каждом проверяемом объекте).
5) FilterMail = mail Почтовый адрес фильтра. `mail` – строка, задающая почтовый адрес. Определяет почтовый адрес, указываемый в поле `From:` каждого сообщения,

отправленного почтовым фильтром (например, уведомления пользователю, администратору).

6) `AdminMail = mail` Почтовый адрес администратора. `mail` – строка, задающая почтовый адрес. Определяет почтовый адрес администратора почтовой системы, по которому будут при необходимости отправляться служебные сообщения/уведомления.
7) `MessagePartialDiscard = {yes | no}` Определяет действие почтового фильтра при обработке сообщений, имеющих поле `Content-Type = message/partial`.
   – yes – отбрасывать сообщения, не проверяя; при этом сообщение не доставляется пользователю;
   – no – продолжить проверку сообщения.
8) `NotifySenderPartial = {yes | no}`
   `NotifyRcptPartial = {yes | no}`
   Определяют возможность отсылки уведомлений отправителю (SenderNotify) и получателю (RcptNotify) сообщения с полем `Content-Type = message/partial`.
   – yes – отправлять уведомление;
   – no – не отправлять уведомление.
9) SenderPartialTemplate = /etc/vba/vbaExim f.templates/sender_message_partial.msg
   RcptPartialTemplate = /etc/vba/vbaExim f.templates/rcpt_message_partial.msg
   Определяют способ уведомления пользователей о сообщении с полем Content-Type=message/partial. Значения параметров аналогичны вышеописанным SenderNotifyTemplate и RcptNotifyTemplate.

В текущей версии могут быть приняты следующие сценарии работы с данным типом сообщения. Если MessagePartialDiscard = yes, то данное сообщение отбрасывается почтовым сервером и не доставляется пользователю. При этом если NotifySenderPartial = yes, то отправитель письма получит уведомление, указанное параметром SenderPartialTemplate. При NotifyRcptPartial = yes получатель получает уведомление; если MessagePartialDiscard = no, то данное сообщения пропускается почтовым сервером (пропускаются его части, если при проверке они оказались «чистыми»). При этом остаются справедливыми правила отсылки уведомления, описанные выше. То есть в этом случае есть возможность уведомить получателя письма о потенциальной опасности данного сообщения из-за невозможности его целостной проверки на почтовом сервере.

Файл шаблона уведомления содержит шаблон отсылаемого сообщения. Шаблоны находятся в каталоге /etc/vba/vbaExim f.templates. При необходимости их можно модифицировать или создать новые файлы шаблонов. В начале файла шаблона можно добавить несколько полей для MIME заголовка (Subject, Content-Type, MIME-Version). Сообщение может содержать подставляемые фильтром параметры (при указании пути к внешней программе эти параметры являются именами переменных окружения):
%SENDER% - заменяется фильтром на почтовый адрес отправителя сообщения;
%RCPT% - заменяется фильтром на почтовый адрес получателя сообщения;
%SUBJECT% - заменяется фильтром на тему сообщения;
%VIRUS% - заменяется фильтром на список вредоносных объектов, найденных в сообщении.

### 3.3. Применение изменений

После изменения конфигурации фильтра выполнить vbaExim f-ctl reload.

### 3.4. Обновление

Для обновления выполнить vbaExim f-ctl update.

## 4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для фильтра являются почтовые сообщения в mime-формате, передаваемые на проверку почтовой системой.

Выходными данными являются результаты проверки в виде числового (текстового) кода, сообщаемые фильтром почтовой системе.

# 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 антивирусный фильтр для почтового сервера Exim соответствует требованиям ТР 2013/027/BY.

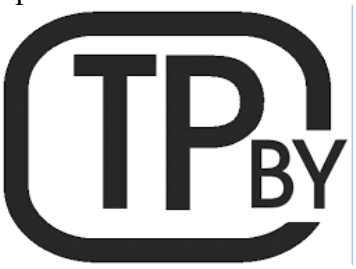


Рис. 1

Знак соответствия, приведенный на рис. 2, означает, что система менеджмента качества применительно к проектированию, производству и технической поддержке антивирусного фильтра для почтового сервера Exim 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* | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *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* |