

User:	PowerMac G4
Application:	QuarkXPress™ 4.11
Document:	antispam_sveta
Date:	Wednesday, March 5, 2003
Time:	6:25 PM
Printer:	Virtual Printer3
Pages:	2

---



slay spam the smart way

**MULTILEVEL**

E-MAIL  
FILTRATION SYSTEM

**POWERFUL**

CONTENT ANALYSIS  
CAPABILITIES

**MULTILANGUAGE**

SUPPORT

**DAILY UPDATES**

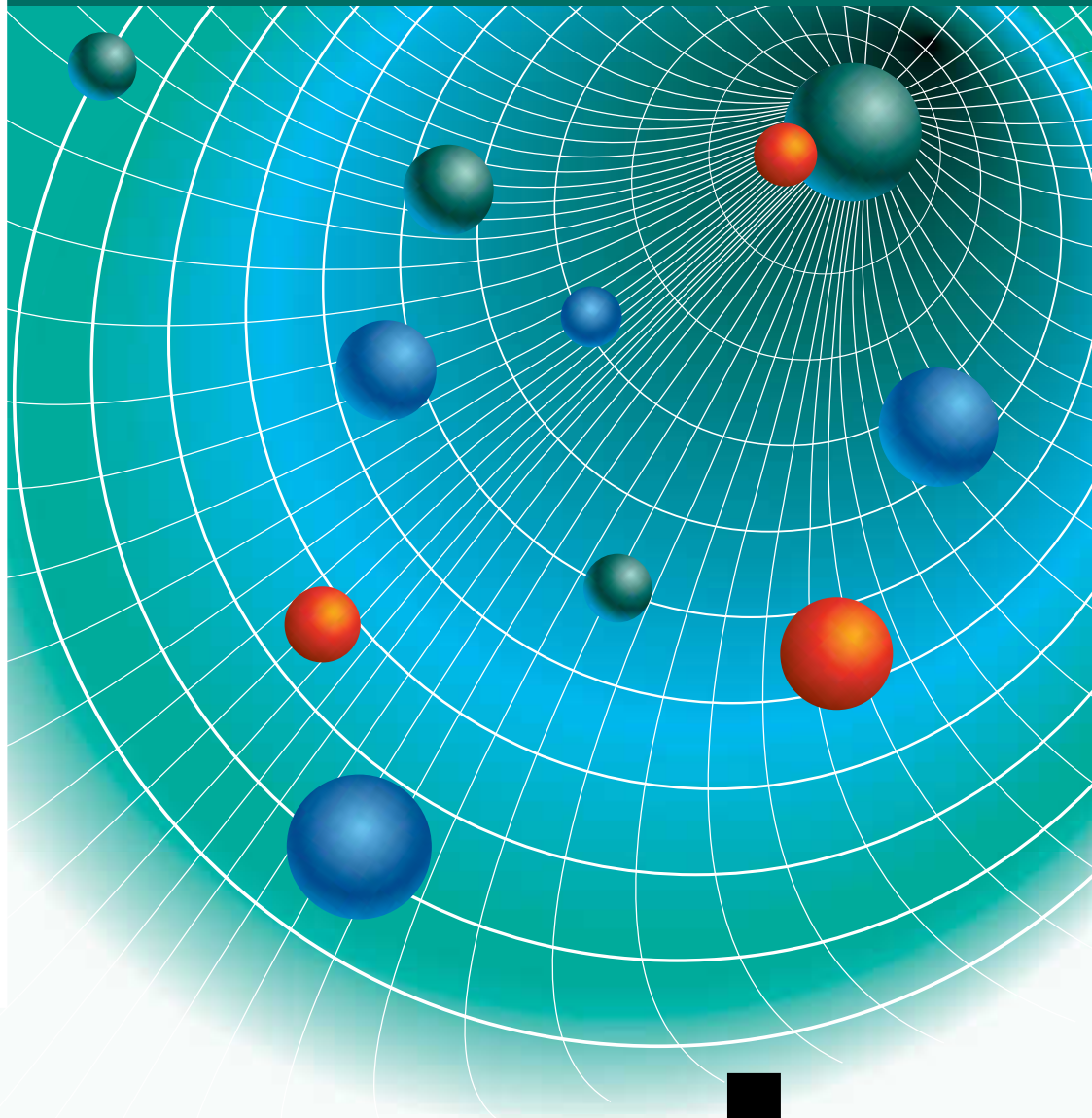
OF MESSAGE SAMPLE  
AND LINGUISTIC FORMS  
DATABASES

**REMOTE**

MANAGEMENT  
VIA WEB-INTERFACE

**ROUND-THE-CLOCK**

TECHNICAL SUPPORT



# Kaspersky<sup>®</sup>

## Anti-Spam

[www.kaspersky.com](http://www.kaspersky.com)





Presently 15-20 percent of total world email traffic is attributed to spam. Often the volume of spam in our mailboxes many times exceeds the amount of useful information. This problem points to a tremendous loss of work time and productivity as well as the huge strain put on communication systems forced to deal with gobs of useless data traffic. The spam epidemic literally threatens the normal functioning of an enterprise. Today the only way to fight this problem is via comprehensive e-mail filtration.

Kaspersky® Anti-Spam is a highly intuitive system designed to protect businesses with small and medium-size networks from the spam onslaught. The software provides comprehensive filtration of incoming email via SMTP protocol – in other words, filtration is performed before messages reach end-user mailboxes. This solution significantly decreases expenses associated with Internet traffic and other non-operational costs.



### Powerful Message Filtration Capabilities

Kaspersky® Anti-Spam combines four methods of incoming message analysis. Firstly, a message is checked with the use of the unique smart content detection kernel SpamTest™, which can separate spam messages from ordinary mail. Then, a signature method is used – each message is compared with samples stored in a daily updated database. Next, formal message characteristics are used for analysis, such as sender address, method of distribution, etc. Lastly is the use of «black lists», a standard method of message filtration based on addresses considered to be spam sources. These addresses are stored in a daily updated database. Kaspersky® Anti-Spam filters the content of all message components (including headers and attached files) and handles attached files stored in Plain Text ASCII, HTML, MS Word 6.0 and RTF formats.

### Multilingual Support

Kaspersky® Anti-Spam offers multilingual functionality via a system of built-in linguistic modules supporting English, Russian, German, French and Spanish.

### Unique Heuristic Analysis

Kaspersky® Anti-Spam contains a smart kernel that supports checking messages for certain parameters typical of spam, such as the presence of certain keywords and terms. A unique heuristic analysis method is used during the text comparison process that searches for key words. Using approximate message comparisons allows a special lexical signature to be created for each message labelled as spam. In the future these signatures make it possible to detect similar messages as spam based on comparisons with existing samples. The result is a flexible system that allows for some text differentiation.

### Flexible Message Handling Options

Depending on predefined settings, a message which passes all filtration levels and has been assigned to a particular category, can then be delivered to its intended recipient (without any changes), redirected to the predefined address or deleted. Kaspersky® Anti-Spam also supports the rejection of messages by category and delivers appropriate notifications to senders.

### Comprehensive Content Filtration Database

To perform message content filtration Kaspersky® Anti-Spam utilizes linguistic data in a content filtration database. The database is composed of three types of data: 1. A spam "rubricator" or list of spam categories. There are more than 500 rubrics corresponding with different spam categories. 2. Semantic images of categories. 3. Message sample signatures.

Currently the database contains more than 12, 000 keywords based on which messages can be referred to a concrete spam category. The database is updated daily by a special linguistic laboratory.

### Regular Updates Of The Content Filtration Database

The high effectiveness of Kaspersky® Anti-Spam is ensured by the daily update of its content filtration database. Updates can be performed both automatically and manually via the Internet. Manual updates allow users to add their own samples of "unwanted" messages to the database. Regular update of «black lists» via the Internet is also supported.

### Handy Administration Tools

You can easily set Kaspersky® Anti-Spam parameters via the Web with a specialized management module. Administrators can create lists of e-mail and IP addresses to be used in the filtration process, establish handling methods for messages that have passed filtration, choose settings for the module responsible for automatic content filtration updates, or add their own samples.

### Easy Integration

Kaspersky® Anti-Spam can be easily integrated into existing enterprise networks. The software can be installed on a dedicated server as well as on the present mail server. It is completely compatible with existing mail systems and has minimal influence on network performance.

System requirements: OS: Linux, FreeBSD 4.x ● Processor: Intel Pentium –III 500MHz or higher ● At least 128 MB RAM

To purchase any Kaspersky Labs product please contact your local distributor. More details are found at:

**www.kaspersky.com**



For further information please contact us at: 10 Geroyev Panfilovtsev Str., Moscow, 125363, Russia. Phone: +7 095 797 8700. Fax: +7 095 948 4331

e-mail: sales@kaspersky.com; info@kaspersky.com; http://www.kaspersky.com; www.viruslist.com

© 2003 Kaspersky Labs  
Kaspersky® Anti-Virus and Kaspersky® Security are registered trademarks of Kaspersky Labs Ltd.  
All other names and trademarks are the copyrighted work of their respective owners.