

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 5.5
для Lotus Notes/Domino

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

АНТИВИРУС КАСПЕРСКОГО 5.5
ДЛЯ LOTUS NOTES/DOMINO

Руководство пользователя

© ЗАО «Лаборатория Касперского»
Тел./факс: +7 (495) 797-87-00, +7 (495) 645-79-39
<http://www.kaspersky.ru>

Дата редакции: май 2007 года

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	5
1.1. Компьютерные вирусы и вредоносные программы	5
1.2. Антивирус Касперского 5.5 для Lotus Notes/Domino.....	6
1.3. Аппаратные и программные требования к системе	8
1.4. Комплект поставки.....	9
1.4.1. Лицензионное соглашение.....	10
1.4.2. Регистрационная карточка	10
1.5. Сервис для зарегистрированных пользователей.....	11
1.6. Принятые обозначения.....	11
ГЛАВА 2. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ.....	13
2.1. Установка приложения	13
2.2. Настройка параметров Антивируса Касперского после установки	15
2.3. Удаление приложения	16
ГЛАВА 3. ОСНОВНЫЕ МОДУЛИ АНТИВИРУСА КАСПЕРСКОГО.....	17
ГЛАВА 4. НАСТРОЙКА ПАРАМЕТРОВ АНТИВИРУСНОЙ ЗАЩИТЫ	19
4.1. Общие параметры работы приложения.....	19
4.2. Обновление антивирусных баз	20
4.3. Параметры проверки репликаций.....	22
4.4. Параметры защиты почты	25
4.5. Защита от эпидемий	27
4.6. Защита баз данных	29
4.7. Параметры антивирусной защиты.....	31
4.7.1. Общие параметры проверки.....	31
4.7.2. Действия над объектами различных статусов	34
4.7.3. Уведомления.....	35
ГЛАВА 5. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ	37
5.1. База Карантин.....	37
5.1.1. Работа в карантине с документами баз данных.....	38
5.1.2. Работа с объектами почтовых сообщений в базе карантина.....	40

5.2. Журнал событий.....	42
5.3. Отчеты о работе приложения.....	44
5.4. Работа с ключами.....	45
5.4.1. Продление ключа	46
5.5. Работа с программой из командной строки.....	48
ГЛАВА 6. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ ПРИЛОЖЕНИЯ	50
ПРИЛОЖЕНИЕ А. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	51
ПРИЛОЖЕНИЕ В. КОДЫ ВОЗВРАТА МОДУЛЯ KAVUPDATER	54
ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»	56
С.1. Другие разработки «Лаборатории Касперского».....	57
С.2. Наши координаты	69

ГЛАВА 1. ВВЕДЕНИЕ

С увеличением количества людей, пользующихся компьютером, и возможностей обмена между ними данными по электронной почте и через интернет возросла угроза заражения компьютера вирусами, а также порчи или хищения информации прочими вредоносными программами.

Среди источников проникновения вредоносных программ наиболее опасными являются:

Интернет

Глобальная информационная сеть является основным источником распространения любого рода вредоносных программ. Как правило, вирусы и другие вредоносные программы размещаются на популярных веб-сайтах интернета, «маскируются» под полезное и бесплатное программное обеспечение. Множество скриптов, запускаемых автоматически при открытии веб-сайтов, могут также содержать в себе вредоносные программы.

Электронная почтовая корреспонденция

Почтовые сообщения, поступающие в почтовый ящик пользователя и хранящиеся в почтовых базах, могут содержать в себе вирусы. Вредоносные программы могут находиться как во вложении письма, так и в его теле. Как правило, электронные письма содержат вирусы и почтовые черви. При открытии письма, при сохранении на диск вложенного в письмо файла вы можете заразить данные на вашем компьютере.

Уязвимости в программном обеспечении

Так называемые «дыры» в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к вашему компьютеру, а, следовательно, к вашим данным, к доступным вам ресурсам локальной сети, к другим источникам информации.

1.1. Компьютерные вирусы и вредоносные программы

Чтобы знать, какого рода опасности могут угрожать вашим данным, полезно узнать, какие бывают вредоносные программы и как они работают. В целом вредоносные программы можно разделить на следующие три класса:

Черви (*Worms*) – данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Вирусы (*Viruses*) – программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – *заражение*. Скорость распространения вирусов несколько ниже, чем у червей.

Троянские программы (*Trojans*) – программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.



Далее по тексту Руководства в качестве обозначения вирусов, троянских программ и червей мы будем использовать термин «вирус». Акцент на конкретный вид вредоносной программы будет делаться только в случае, когда это необходимо.

1.2. Антивирус Касперского 5.5 для Lotus Notes/Domino

Антивирус Касперского® для Lotus Notes/Domino (далее также **Антивирус Касперского**, приложение) предназначен для обеспечения антивирусной защиты почтовых систем и баз данных, построенных на приложениях Lotus Notes и Lotus Domino. Антивирус Касперского устанавливается на сервере, работающем под управлением операционной

системы Microsoft Windows 2000/2003, и защищает всю проходящую через сервер почту и файлы баз данных от вредоносных программ.

Антивирус Касперского для Lotus Notes/Domino позволяет:

- *проводить антивирусную проверку сообщений*, проходящих через почтовую систему Lotus Notes/Domino. Поиск вирусов производится и в тексте сообщений и в присоединенных к ним файлах;
- *лечить* зараженные сообщения, если это было указано в параметрах;
- *осуществлять фильтрацию файлов по типу*. К файлам определенного формата применяются отдельные, установленные администратором правила обработки;
- *изолировать файлы в карантине* (специальном хранилище объектов, возможно зараженных вирусами), в целях сохранности информации;
- *уведомлять* отправителя, получателя и системного администратора о сообщениях, содержащих вредоносные объекты;
- *фиксировать* возникновение вирусных эпидемий и уведомлять о них администратора;
- *обновлять базы Антивируса* как автоматически, так и в ручном режиме. Ресурсом обновления баз могут быть серверы обновлений «Лаборатории Касперского», FTP- и HTTP-серверы, локальная или сетевая папка, содержащие актуальный набор обновлений;
- *фиксировать результаты работы* Антивируса в журнале событий;
- управлять ключами Антивируса.



Внимание! Каждый день появляются новые вирусы, поэтому для поддержания приложения в актуальном состоянии необходимо обновлять базы Антивируса ежечасно!

Обратите внимание на ряд ограничений при работе с приложением.

Антивирус Касперского для Lotus Notes/Domino:



- Не проверяет сообщения, зашифрованные стандартными средствами Lotus Notes/Domino..
- Может нарушать целостность электронной подписи отправителя сообщений при добавлении в текст письма отчета о проверке, при замене зараженных вложений вылеченными, а также при удалении объекта, вылечить который невозможно.
- Не проверяет файлы, созданные в OS/2 или Macintosh.
- Конвертирует письма из формата MIME в формат RichText, если в тело почтового сообщения добавляется отчет о проверке. При этом форматирование письма может быть нарушено.
- Не позволяет изменять параметры работы приложения через веб-интерфейс.

1.3. Аппаратные и программные требования к системе

Для функционирования Антивируса Касперского 5.5 для Lotus Notes/Domino на сервере должно быть установлено следующее **программное обеспечение**:

Одна из операционных систем:

- Microsoft Windows 2000 (с установленным пакетом обновлений Service Pack 4 и выше);
- Microsoft Windows 2000 Advanced Server (с установленным пакетом обновлений Service Pack 4 и выше);
- Microsoft Windows Server 2003 Standard Edition;
- Microsoft Windows Server 2003 Enterprise Edition.

- Одна из следующих версий Lotus Notes/Domino:
- версия 6.5 и выше;
- версия 7.0 и выше.



Версия Lotus Notes/Domino 7.0 поддерживается без использования технологии DB2 Universal Database.

Минимальные **аппаратные требования** для использования Антивируса Касперского:

- процессор Intel Pentium 300 МГц или выше;
- свободная оперативная память 64 МБ (рекомендуется 128 МБ);
- 11 МБ свободного дискового пространства для установки приложения (без учета объема служебных папок).
- Объем свободного места на диске рассчитывается исходя из среднего объема одного письма.



Системные требования для Lotus Notes/Domino могут отличаться от требований Антивируса Касперского.

1.4. Комплект поставки

Программный продукт вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, www.kaspersky.ru, раздел **Электронный магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;
- руководство пользователя;
- ключ, включенный в состав дистрибутива или записанный на специальную дискету;
- регистрационная карточка (с указанием серийного номера продукта);
- лицензионное соглашение.



Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением.

При покупке продукта в интернет-магазине вы копируете продукт с веб-сайта, в дистрибутив которого помимо самого продукта включено также данное руководство. Ключ либо включен в дистрибутив, либо отправляется вам по электронной почте по факту оплаты.

1.4.1. Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.



Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с Антивирусом Касперского дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с установочным компакт-дисксом должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-дисксом или устанавливая продукт на компьютер, вы тем самым принимаете все условия лицензионного соглашения.

1.4.2. Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели программный продукт.

Если впоследствии у вас изменится почтовый / электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока подписки. Кроме того, зарегистрированным пользователям, подписавшимся на

рассылку новостей ЗАО «Лаборатория Касперского», высылаются информация о выходе новых программных продуктов.

1.5. Сервис для зарегистрированных пользователей

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования Антивируса Касперского.

Приобретя подписку, вы становитесь зарегистрированным пользователем программы и в течение срока действия подписки получаете следующие услуги:

- предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО «Лаборатория Касперского»).



Консультации по вопросам функционирования и использования операционных систем, а также работы различных технологий не проводятся.

1.6. Принятые обозначения

Текст документации выделяется различными элементами оформления в зависимости от его смыслового назначения. В расположенной ниже таблице приведены используемые условные обозначения.

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.

Оформление	Смысловое назначение
 Примечание.	Дополнительная информация, примечания.
 Внимание!	Информация, на которую следует обратить особое внимание.
 <i>Чтобы выполнить действие,</i> <ol style="list-style-type: none"> 1. Шаг 1. 2. ... 	Описание последовательности выполняемых пользователем шагов и возможных действий.
 Задача, пример	Постановка задачи, примера для реализации возможностей программного продукта
 Решение	Реализация поставленной задачи
[ключ] – назначение ключа.	Ключи командной строки.
Текст информационных сообщений и командной строки	Текст конфигурационных файлов, информационных сообщений программы и командной строки.

ГЛАВА 2. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Перед тем как начинать установку Антивируса Касперского, необходимо убедиться в том, что аппаратное и программное обеспечение компьютера соответствует системным и аппаратным требованиям. Минимально допустимая конфигурация указана в разделе 1.3 на стр. 8.



Для установки/удаления Антивируса Касперского 5.5 для Lotus Notes/Domino необходимо наличие прав локального администратора на компьютере, где осуществляется установка/удаление, а также прав администратора Lotus Notes/Domino.

2.1. Установка приложения

Процедура установки выполняется аналогично большинству приложений Microsoft Windows.

Чтобы установить Антивирус Касперского на компьютер, на дистрибутивном CD-диске приложения запустите исполняемый файл. Установка сопровождается мастером. Рассмотрим подробно каждый шаг процедуры установки приложения.



Установка приложения с дистрибутива, полученного через интернет, полностью совпадает с установкой приложения с дистрибутивного CD-диска.

Шаг 1. Проверка версии установленной операционной системы

Перед установкой приложения на компьютере выполняется проверка соответствия установленной операционной системы, а также пакетов обновлений (Service Packs) программным требованиям Антивируса Касперского. Если какой-либо из требуемых пакетов не установлен, проведите обновление, после чего повторно запустите установку Антивируса Касперского.

Если на компьютере установлены другие антивирусные программы для Lotus Notes/Domino, совместное их использование с Антивирусом Касперского может привести к возникновению нестандартных ситуаций. Рекомендуем вам самостоятельно удалить их, после чего продолжить установку.

Шаг 2. Приветствие и Лицензионное соглашение

На первых этапах установки Антивируса Касперского открываются окно приветствия и окно, содержащее лицензионное соглашение. Внимательно прочтите текст лицензионного соглашения и примите его условия для продолжения установки.

Шаг 3. Ввод сведений о пользователе

В диалоговом окне **Информация о пользователе** введите имя пользователя. По умолчанию в окне указана информация из реестра Microsoft Windows.

Шаг 4. Запуск установки

По окончании определения сведений о пользователе запустите процесс установки. Для этого в окне мастера нажмите на кнопку **Установить**.



Антивирус Касперского по умолчанию будет установлен в папку <Диск>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus for Lotus Notes.

Шаг 5. Установка ключа

На данном шаге выполняется установка ключа Антивируса Касперского для Lotus Notes/Domino. Ключ является вашим личным «ключом», в котором находится служебная информация, необходимая для полнофункциональной работы приложения.

В открывшемся окне **Установленные ключи** нажмите на кнопку **Добавить**. В окне выбора файлов укажите файл ключа, который необходимо установить (файл с расширением *.key). В результате указанный ключ будет добавлен в качестве активного ключа для Антивируса Касперского. В случае если на момент установки приложения у вас нет ключа (например, вы заказали его в «Лаборатории Касперского» через интернет, но еще не получили), вы сможете установить его позже, при первом запуске приложения. Помните, что без ключа вы не сможете приступить к работе с Антивирусом Касперского.

Шаг 6. Завершение установки

На этом шаге отображается информация об окончании процесса установки Антивируса Касперского.



Данные о процессе установки фиксируются приложением в файле `%TEMP%\kav_lotus.log`.

Прежде чем приступать к работе с приложением, вам необходимо выполнить предварительную настройку параметров совместной работы приложения и сервера Domino (см. п. 2.2 на стр. 15).

2.2. Настройка параметров Антивируса Касперского после установки



Для корректного функционирования приложения после завершения установки необходимо подписать некоторые базы сервера Domino:

- Убедитесь, что у вас есть права администратора Lotus Notes/Domino.
- Запустите **Domino Administrator**.
- Выполните подключение к серверу, на котором установлен Антивирус Касперского.
- Раскройте закладку **Files**.
- На закладке **Files** выберите из списка базы **kldsettings.nsf** и **kldquarantine.nsf** (базы Антивируса Касперского).
- Выполните команду **Sign** для обеих баз.



Команду необходимо выполнить с правами **Active Server's ID**.

2.3. Удаление приложения

Удаление Антивируса Касперского для Lotus Notes/Domino вы можете провести стандартными средствами установки и удаления программ Microsoft Windows. При этом с компьютера будут удалены все установленные компоненты Антивируса Касперского.



Для удаления Антивируса Касперского:

- Остановите работу сервера.
- В панели управления Microsoft Windows выберите пункт **Установка и удаление программ**→**Антивирус Касперского для Lotus Notes/Domino** и нажмите на кнопку **Удалить**.

ГЛАВА 3. ОСНОВНЫЕ МОДУЛИ АНТИВИРУСА КАСПЕРСКОГО

Рассмотрим внутреннюю архитектуру Антивируса Касперского для наиболее полного отражения алгоритма его работы. Кроме того, информация данного раздела будет полезна для детального анализа отчетов о работе приложения, так как отчеты формируются по работе каждого из модулей.

Антивирус Касперского включает в себя следующие модули:

- **Hook** – модуль перехвата почтовых сообщений.
- **Kavmailmonitor** – модуль проверки почтовых сообщений.
- **Kavdbscanner** – модуль проверки баз данных.
- **Kavreplmonitor** – модуль проверки репликаций.
- **Kavupdater** – модуль обновления баз Антивируса.
- **Систему детектирования вирусных эпидемий.**

В процессе работы Антивирус Касперского использует несколько баз данных, хранящихся на сервере:

- Конфигурационную базу.
- Базу карантина.
- Базу отчетов и журнал событий приложения.

Модули **Kavreplmonitor**, **Kavupdater**, **Kavmailmonitor** и **Kavdbscanner** запускаются автоматически при старте сервера Domino.

После запуска модуль **Hook** перехватывает все сообщения, отправляемые и принимаемые сервером Domino, и передает их модулю **Kavmailmonitor** для антивирусной проверки и обработки.

По результатам проверки объект может быть признан незараженным, зараженным, подозреваемым на заражение вредоносными программами, а также непроверенным из-за сбоя или повреждения.

Модуль **Kavmailmonitor** проверяет полученные сообщения на присутствие вирусов и обрабатывает эти сообщения в соответствии с заданными

параметрами антивирусной защиты. Например, модуль может лечить все зараженные объекты и помещать те, которые не удалось вылечить, на карантин. Кроме того, модуль **Kavmailmonitor** сообщает о своих действиях в журнал работы.

Модуль **Kavdbscanner** проверяет базы данных сервера Domino и обрабатывает их в зависимости от заданных параметров антивирусной защиты. Все функции и действия данного модуля аналогичны функциям модуля **Kavmailmonitor**.

Модуль **Kavreplmonitor** предупреждает заражение сервера через репликации документов с других, незащищенных Антивирусом Касперского серверов Domino. Локальные репликации, проводимые в рамках одного сервера Domino, не проверяются.

Система детектирования предупреждает возникновение вирусных эпидемий. Правила и критерии, по которым детектируется эпидемия, а также возможные действия при обнаружении ее, определяются администратором.

Модуль **Kavupdater** обновляет антивирусные базы, используемые при поиске и лечении вирусов.

При изменении параметров модули **Kavmailmonitor**, **Kavdbscanner**, **KavReplMonitor** и **KavUpdater** будут работать с новыми значениями параметров практически сразу же после их сохранения.



При изменении параметров с помощью файла настроек *notes.ini* обновленные значения вступают в силу после перезапуска модуля.

ГЛАВА 4. НАСТРОЙКА ПАРАМЕТРОВ АНТИВИРУСНОЙ ЗАЩИТЫ

Сразу же после установки приложения и проведения процедуры подписывания баз Антивирус Касперского готов к работе. Общие параметры работы уже заданы.

Настройка параметров работы Антивируса Касперского выполняется локально, с помощью консоли администрирования приложения. Управление через командную строку возможно только для некоторых основных задач (подробнее см. п. 5.5 на стр.48). В данном разделе будут рассмотрены задачи конфигурирования приложения через консоль администрирования.

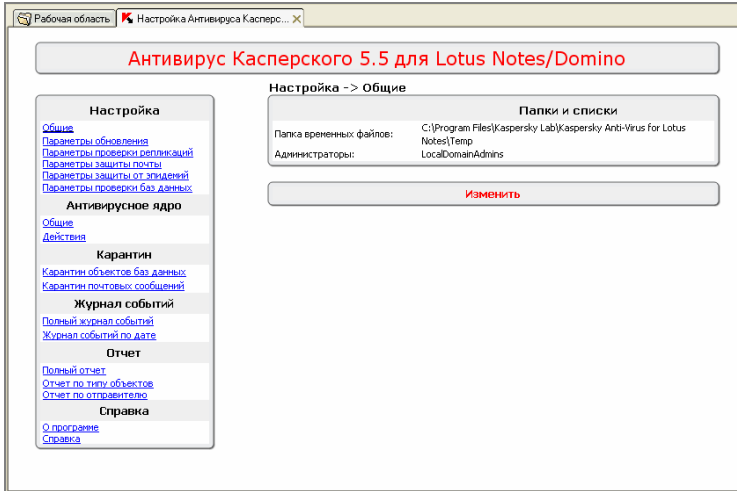
Для удобства пользования настройки выделены в отдельные группы. Каждая группа отражает определенную функциональность Антивируса. Группа включает в себя более частные задачи.

Перейти в окна отдельных задач вы можете из групп **Настройки** и **Антивирусное ядро** в панели результатов консоли Антивируса Касперского, выбрав соответствующую ссылку.

4.1. Общие параметры работы приложения

В окне **Общие** группы **Настройка** в (см. рис. 1) представлена информация общего характера об Антивирусе Касперского:

- **Папка временных файлов** – путь к папке для размещения временных файлов. В папке хранятся временные файлы, используемые Антивирусом во время работы. Если на вашем сервере установлен антивирус, контролирующий файловую систему (например, **Антивирус Касперского для файловых серверов**) рекомендуется настроить исключение этой папки из антивирусной проверки.
- **Администраторы** – список электронных адресов, на которые будут рассылаться уведомления.

Рисунок 1. Закладка **Общие**

4.2. Обновление антивирусных баз

Обновление антивирусных баз может выполняться автоматически с заданным периодом обновления и вручную администратором. Получение антивирусных баз возможно из двух источников:

- с серверов обновлений «Лаборатории Касперского»;
- с FTP- или HTTP-сервера или из локальной/сетевой папки.



Антивирусные базы на серверах обновлений «Лаборатории Касперского» обновляются ежедневно.

Управление обновлением антивирусных баз осуществляется в окне **Параметры обновления** группы **Настройка** (см. рис. 4). Вы можете:

- Определять папки хранения баз (основной и резервной копии).
В резервной папке сохраняется более ранняя версия антивирусных баз, что позволяет в случае возникновения нештатной ситуации в процессе копирования обновления восстановить базы.
- Задавать папку хранения временных файлов, используемых модулем обновления **Kavupdater**.
- Выбирать источники обновлений и параметры загрузки антивирусных баз.

В разделе **Параметры обновления баз** определите ресурс, с которого будут производиться обновления, а также их параметры. Это может быть:

- **HTTP-, FTP-сервер или сетевая папка** – локальный сервер или папка, куда администратор помещает обновления, полученные из интернета. В поле **Локальный источник** укажите путь к данной папке с помощью кнопки **Изменить**.
- **Серверы обновлений Лаборатории Касперского** – HTTP-и FTP-серверы «Лаборатории Касперского» в интернете, куда ежедневно выкладываются обновленные базы.
- Флажок **Пассивный режим FTP** используется в том случае, если вы загружаете обновления с ftp-сервера, соединение с которым выполняется в пассивном режиме (например, через межсетевой экран). Если используется активный режим работы с FTP, вы можете снять данный флажок.
- Если для выхода в интернет используется прокси-сервер, установите флажок **Использовать** прокси-сервер.

Запланируйте частоту обновлений. Для этого в разделе **Расписание** определите периодичность запуска копирования обновлений антивирусных баз:

- Флажок **Обновлять по расписанию** определяет, что обновление программы производится в соответствии с установленным графиком.
- В группе параметров **Частота запуска** выберите один из следующих вариантов:
 - **Дни** – программа обновляется раз в некоторое количество дней. В параметрах расписания определите, как часто нужно запускать обновление: уточните интервал **N** для параметра **Каждый N-й день**. Дополнительно к частоте укажите, в какое время суток будет производиться обновление.
 - **Часы** – интервал между обновлениями исчисляется в часах. Если вы выбрали такую частоту, в параметрах расписания укажите интервал: **Каждый N-й час** и уточните интервал **N**. Например, для ежедневного обновления установите **Каждый 1 час**.
 - **Обновить сейчас** – запуск обновления немедленно.

В процессе работы модуль **Kavupdater** фиксирует свое состояние в виде записей кодов возврата в логах (логи можно просмотреть в базе *log.nsf*, в папке Data сервера Domino).

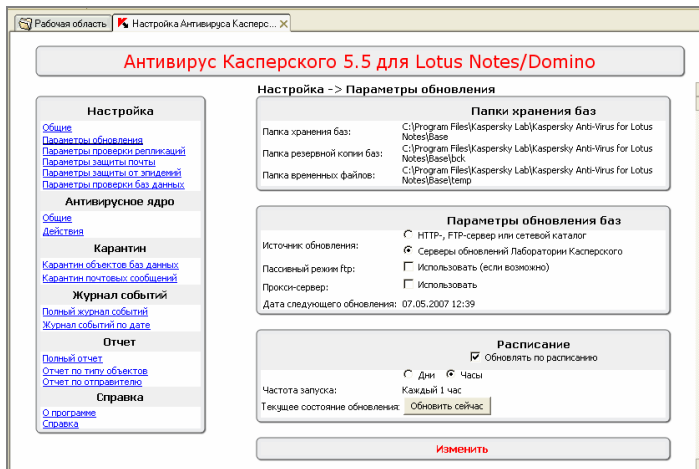


Рисунок 2. Параметры обновления

4.3. Параметры проверки репликаций

Модуль **KavrepImonitor**, входящий в состав Антивируса Касперского, предназначен для обеспечения антивирусной безопасности проводимых сервером репликаций. Настройка параметров проверки осуществляется в окне **Параметры проверки репликаций** группы **Настройка**.

Вы можете устанавливать флажок, определяющий включение проверки **Проверять следующие объекты** и выбрать типы объектов, которые будут проверяться:

- **Вложенные объекты** – проверка на присутствие вирусов все вложенных в почтовое сообщение файлов.
- **Тело письма** – проверять тело почтового сообщения.
- **OLE-объекты** – проверять погруженные в сообщение объекты (например, объекты текстового формата, графические и звуковые объекты и проч.).

Задавать исключение из проверки с помощью группы параметров **Фильтрация по имени** и **Фильтрация по типу**. Условия фильтрации могут быть следующими:

- **Фильтрация по имени** объекта. К отфильтрованным объектам будут применяться особые правила обработки, определенные на вкладке **Фильтр по имени** окна **Действия**.

При вводе имени объекта-исключения вы можете формировать маски, используя следующие символы:

- * – любая последовательность символов. Например, при вводе маски **abc*** не будет проверяться любой файл, имя которого начинается с последовательности **abc** (**abc.exe**, **abc1.com**, **abc2.rar**).
- ? – любой один символ. Например, при вводе маски **abc?.exe** не будет проверяться файл, содержащий заданную последовательность символов и любой символ, следующий за **c**, например, **abc1.exe**. Однако файл **abc12345.exe** будет проверен.

Для определения нескольких масок задайте их в поле **Фильтрация по имени**, разделяя символом ;



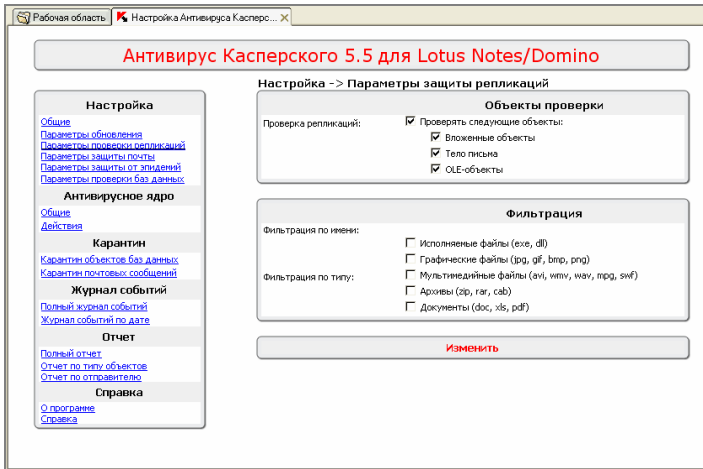
При фильтрации по имени регистр букв в имени файла не учитывается.

- **Фильтрация по типу объекта**. Это могут быть файлы следующих типов:
- **Исполняемые файлы** – файлы формата exe или dll. Данный тип файлов исключать из проверки не рекомендуется.
- **Графические файлы** – файлы графического формата хранения изображений (jpg, gif, bmp, png).
- **Мультимедийные файлы** – файлы форматов мультимедиа (avi, wmv, wav, mpg, swf).
- **Архивы** – файлы некоторых архивов (zip, rar, cab).
- **Документы** – файлы документов Microsoft Office, Microsoft Office Excel, Adobe Acrobat (doc, xls, pdf).



Действия, применяемые к объектам после фильтрации, задаются в окне **Действия** группы настроек **Антивирусное ядро**.

Обратите внимание на особенность работы приложения с объектами карантина. При попытке репликации восстановленного из карантина объекта модуль **Kavreplmonitor** перехватит его и вновь отправит на антивирусную проверку и обработку.

Рисунок 3. Закладка **Параметры проверки репликаций**

Кроме того, Антивирус Касперского может проверять репликации, проводимые на кластерах серверов.

По умолчанию проверка кластерных репликаций включена и будет проводиться сразу же после установки Антивируса Касперского на сервер. Если по каким-либо причинам проверка не производится, отредактируйте файл настроек **notes.ini** описанным ниже способом.



Для включения антивирусной проверки кластерных репликаций:

- Откройте файл настроек сервера Domino **notes.ini**.
- Отредактируйте параметр **KavMailHookEnabledTasks**, добавив к списку его значений параметр **clrepl.exe**.
- Перезапустите сервер Domino.



Если вы хотите отключить проверку репликаций, удалите параметр **ncirepl.exe из списка значений **KavMailHookEnabledTasks**.**

Особый случай проверки репликаций возникает при взаимодействии двух серверов Domino.

Если один из серверов (назовем его **Сервер1**) защищен Антивирусом Касперского для Lotus Notes/Domino, а другой сервер (**Сервер2**) нет, схема антивирусной проверки может быть следующей:

- По умолчанию проверка исходящих репликаций отключена (опция **KavMailHookOutgoingReplication=0** в файле настроек **notes.ini** сервера Domino). При этом проверяются pull-репликации **Сервера1** и push-репликации с **Сервера2** на **Сервер1**.
- Если проверка исходящих репликаций включена (опция **KavMailHookOutgoingReplication=1** в файле настроек **notes.ini** сервера Domino) также проверяются push-репликации с **Сервера1**. Однако pull-репликации с **Сервера2** на **Сервер1** проверяться не будут.



Pull-репликации, инициированные удаленным сервером, Антивирусом Касперского не обрабатываются!

В случае совместной работы двух серверов, защищенных Антивирусом Касперского для Lotus Notes/Domino, при включении опции проверки исходящих репликаций (**KavMailHookOutgoingReplication=1**) хотя бы на одном из серверов, в процессе репликации возникнет конфликт репликаций. Поэтому в такой конфигурации не рекомендуется включать данную опцию.



Как и в случае с обычной репликацией, при работе на кластере серверов могут возникать конфликты репликаций.

Если необходимо проверять исходящие репликации, рекомендуется включать проверку только на одном сервере из кластера и только в случае, если остальные сервера кластера не защищены.

4.4. Параметры защиты почты

При проверке почтовых сообщений сервера Domino Антивирус Касперского использует модуль **Kavmailmonitor**. Настройка параметров проверки почты осуществляется в окне **Параметры защиты почты** группы **Настройка** (см. рис.4).



Антивирус Касперского не проверяет зашифрованные почтовые сообщения!

Настраивая параметры проверки почтовых сообщений, вы можете устанавливать флажок, определяющий включение проверки **Проверять следующие объекты** и выбрать типы объектов, которые будут проверяться:

- **Вложенные объекты** – проверка вложения почтовых сообщений. По умолчанию на присутствие вирусов будут проверяться все вложенные файлы.

- **Тело письма** – проверять тело почтового сообщения.
- **OLE-объекты** – проверять погруженные в сообщение объекты (например, объекты текстового формата, графические и звуковые объекты и проч.).

Задавать исключения из проверки с помощью группы параметров **Фильтрация по размеру**, **Фильтрация по имени** и **Фильтрация по типу**. Условия фильтрации могут быть следующими:

- **Не проверять объекты более ... КБ** – установите флажок для ограничения проверки одного объекта по размеру и в поле справа укажите максимально допустимый размер объекта. В результате, если данное значение будет превышено, письмо будет исключено из проверки.
- **Фильтрация по имени** файла вложения. К отфильтрованным объектам будут применяться особые правила обработки, определенные на закладке **Фильтр по имени** окна **Действия**.

При вводе имени объекта-исключения вы можете формировать маски, используя следующие символы:

- * – любая последовательность символов. Например, при вводе маски **abc*** не будет проверяться любой файл, имя которого начинается с последовательности **abc** (**abc.exe**, **abc1.com**, **abc2.rar**).
- ? – любой один символ. Например, при вводе маски **abc?.exe** не будет проверяться файл, имя которого начинается с последовательности **abc** и дополняется любым одним символом, следующим за **c**, например, **abc1.exe**. Однако файл **abc12345.exe** будет проверен.

Для определения нескольких масок задайте их в поле **Фильтрация по имени**, разделяя символом ;



При фильтрации по имени регистр букв в имени файла не учитывается.

- **Фильтрация по типу** вложенных в почтовое сообщение файлов (подробнее о настройке данного параметра см. п. 4.3 на стр. 22).

Почтовое сообщение проверяется Антивирусом Касперского по частям (тело письма, вложение). Если какая-либо часть письма окажется зараженной (подозрительной, отфильтрованной по какому-либо признаку и т.д.), к ней будет применено действие, заданное на закладке соответствующего статуса проверки (окно **Действия** группы **Антивирусное ядро**). Подробнее см. п. 4.7.2 на стр. 34. Если в качестве действия над объектом в окне **Действия** группы **Антивирусное ядро** будет задано **Поместить на карантин**, в хранилище карантина будет перенесена часть почтового сообщения.

Если вы установите флажок **Помещать письмо на карантин**, при обнаружении подозрительного объекта сообщение будет перенесено в карантин полностью.

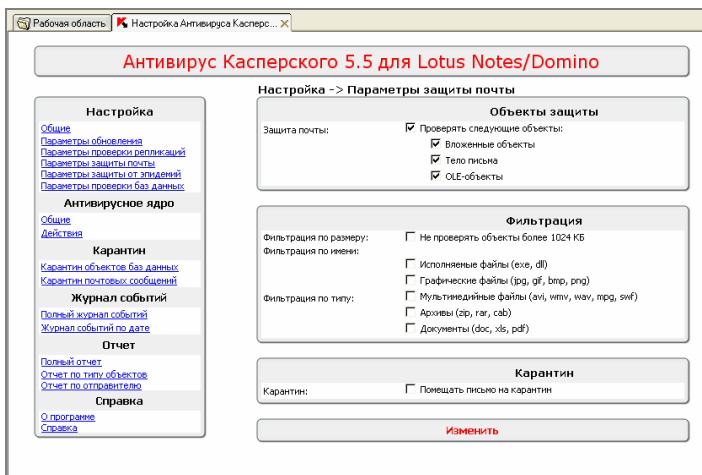


Рисунок 4. Закладка **Параметры защиты почты**

4.5. Защита от эпидемий

Обнаружение вирусной эпидемии до момента наступления ее пика позволяет существенно снизить риск заражения. В состав Антивируса Касперского входит система обнаружения эпидемий, позволяющая фиксировать повышение вирусной активности на защищаемом сервере Domino и уведомлять об этом администратора и других пользователей. Это позволяет администратору своевременно реагировать на возникающие угрозы.

Определение параметров работы системы производится в окне **Параметры защиты от эпидемий** группы **Настройка** (см. рис. 5).

Вирусная активность определяется на основании данных, передаваемых модулем **Kavmailmonitor**, и позволяет фиксировать обнаружение:

- Зараженных объектов.
- Подозрительных объектов.
- Поврежденных объектов.

- Одного и того же вируса несколько раз.

Вы можете включить оповещение о повторном обнаружении какого-либо вида объекта (или вируса) за определенное время. Для этого:

- Установите флажок **Включить защиту**.
- Задайте частоту обнаружения события определенного статуса в поле **Частота**. Определите количество объектов и время, за которое будет учтено обнаружение объекта данного статуса. Если вирусная активность превышает установленную частоту, отправляется уведомление о возникновении угрозы вирусной эпидемии.

При формировании текста уведомления могут использоваться следующие макросы:

- **%с** – количество обнаружения объектов данного статуса;
- **%р** – период, за который ведется статистика обнаружения объектов;
- **%v** – имя вируса, которым заражен объект. Данная макроподстановка может быть использована только при обнаружении объекта со статусом **Зараженный**.

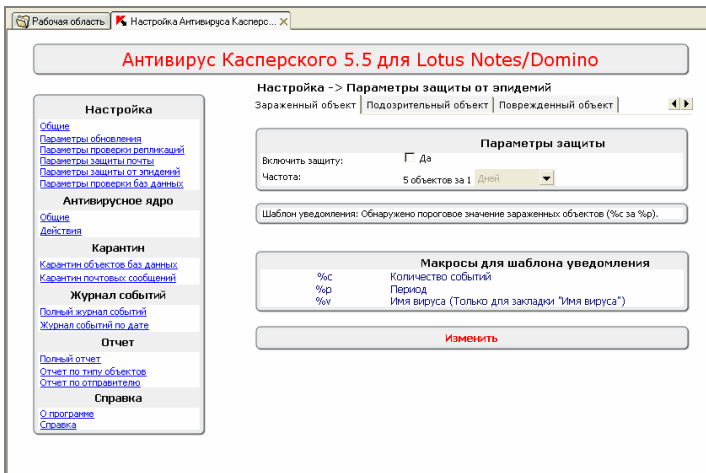


Рисунок 5. Закладка **Параметры защиты от эпидемий**

4.6. Защита баз данных

Во время проверки файлов баз данных сервера Domino Антивирус Касперского использует модуль **Kavdbscanner**. При этом приложение использует параметры, заданные в окне **Параметры проверки баз данных**. Перейти в данное окно вы можете из раздела **Настройка** в панели результатов консоли Антивируса Касперского, выбрав ссылку [Параметры проверки баз данных](#) (см. рис. 6).

Настраивая параметры проверки баз данных, вы можете:

- Определять типы объектов проверки (подробнее о настройке данного параметра см. п. 4.3 на стр. 22).
- Устанавливать маски и задавать включение вложенных папок в списке проверяемых объектов.

При вводе масок вы можете использовать следующие символы:

* – любая последовательность символов, кроме символов разделения папок / и \. Например, если указана маска **abc*.nsf**, будут проверены все базы, имена которых начинаются с комбинации символов **abc** (**abc.nsf**, **abcd.nsf**, **abc123.nsf**). Однако базы, находящиеся внутри вложенных папок (например, **abc\123.nsf**) проверены не будут.



Маски задаются с учетом пути к базам относительно папки **Data** сервера Domino (например, для базы **database.nsf** из папки **folder**, маска проверки должна быть определена как **folder\database.nsf**). Папка **Data** создается на компьютере при установке сервера Domino.

? – любой один символ, кроме символов разделения папок / и \. Например, если указана маска **abc?.nsf**, будут проверены базы, имена которых начинаются с последовательности **abc** и дополняется любым одним символом, следующим за **c**, например, **abc1.nsf**. Однако файл **abc12345.nsf** будет проверен.

Для включения символов / и \ в список символов, попадающих под действие масок, установите флажок **Проверка вложенных папок**.

- Определять объекты, исключаемые из проверки.



Рекомендуется исключить из проверки базу карантина. Для этого в поле **Исключения из проверки** необходимо указать путь к базе относительно папки **Data**.

- Осуществлять фильтрацию проверяемых объектов по типу файла (подробнее о настройке данного параметра см. п. 4.3 на стр. 22).
- Планировать частоту проверок. Для этого в разделе **Расписание** задайте периодичность запуска задачи:
 - **Проверять по расписанию** – запускать проверку баз автоматически в соответствии с заданным расписанием.
 - **Дни** – ежедневный запуск проверки в определенное время суток.
 - **Часы** – запуск проверки в определенное время с интервалом в один или несколько часов.
- Запускать проверку баз данных вручную, с помощью кнопки **Запустить проверку**.

В процессе работы модуль **KavDbScanner** фиксирует свое состояние в виде записей логов (логи можно просмотреть в базе *log.nsf*, в папке Data сервера Domino). При запуске, в процессе и по окончании антивирусной проверки соответствующие записи будут занесены в лог. Например, строка о запуске проверки будет выглядеть следующим образом: KavDbScanner Сканирование баз, о завершении проверки – KavDbScanner Сканирование баз успешно завершено. Если в процессе произошла ошибка, из-за которой проверка не может быть продолжена, это также будет зафиксировано в логах.



В любое время просмотреть состояние процесса проверки можно, введя на консоли сервера Domino команду **show tasks**.

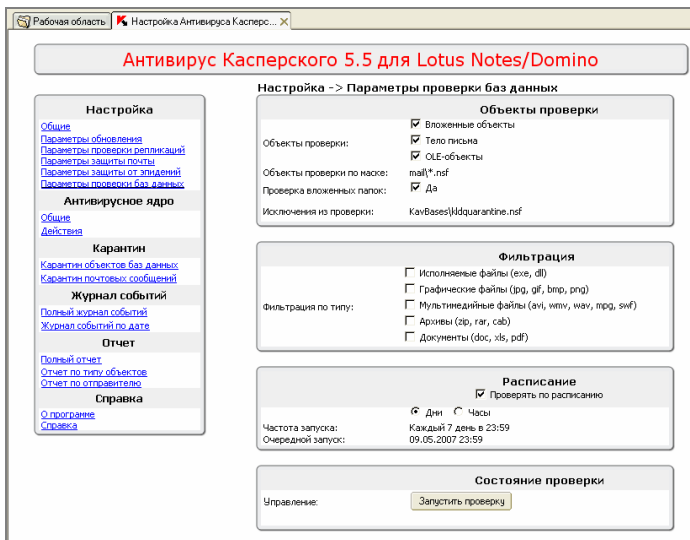


Рисунок 6. Закладка Параметры проверки баз данных

4.7. Параметры антивирусной защиты



В данном разделе под объектами проверки мы будем понимать любой из проверяемых файлов.

Например, зараженным может быть как вложенный файл почтового сообщения, так и OLE-объект файла базы данных. К этим объектам будут применены одни и те же настройки, определенные как действия над зараженным объектом.

Для настройки параметров антивирусной защиты, необходимо определить типы объектов, которые будут проверяться, и задать действия Антивируса Касперского в случае обнаружения вредоносных объектов определенных статусов.

4.7.1. Общие параметры проверки

Во время работы Антивирус Касперского использует параметры антивирусной защиты, заданные в окне **Общие**. Перейти в данное окно вы можете из раздела **Антивирусное ядро** в панели результатов консоли Антивируса Касперского, выбрав ссылку [Общие](#) (см. рис. 7).

Настраивая параметры антивирусной защиты, вы можете:

- Определять автоматическое лечение зараженных объектов. Для этого установите флажок **Лечить зараженные объекты**.
- Включать антивирусную проверку для объектов типа:
 - **Архивы**. Приложение обеспечивает антивирусную проверку архивированных и сжатых файлов и их содержимого.
 - **Упакованные исполняемые файлы**. Проверять исполняемые файлы, упакованные с помощью специальных утилит-упаковщиков. Если внутри упакованного файла обнаружен вирус, то возможно его лечение (если в качестве действия с зараженными файлами указано лечение). При этом исходный файл будет замещен распакованным и вылеченным.
 - **Зашифрованные объекты**. Проверять объекты, зашифрованные стандартными средствами Lotus Notes/Domino.
- Определять время максимальной проверки одного объекта в поле **Не проверять объекты более**. Если за указанный интервал проверка не проведена, объект будет пропущен.
- Устанавливать количество одновременно запущенных процессов проверки в поле **Количество экземпляров ядра**. Каждая задача антивирусной проверки использует одно ядро. При увеличении количества экземпляров ядра, растёт число запущенных параллельно процессов. Это влияет на загрузку процессора, что в свою очередь отражается на скорости его работы. Мы рекомендуем вам не запускать более 3 экземпляров антивирусного ядра одновременно.

Выбирать тип антивирусных баз, используемых при проверке:

- *Стандартные базы (только вирусы)* – антивирусные базы, содержащие подробное описание всех существующих на данный момент вирусов, методов их обнаружения и лечения. Данные антивирусные базы используются по умолчанию.
- *Расширенные базы (вирусы + потенциально опасное ПО)* – антивирусные базы, которые помимо вирусов содержат также информацию о потенциально опасном ПО, рекламных программах, программах автодозвона. Подобные программы содержат уязвимости, которые могут использоваться для хакерских атак, внедрения неавторизованных программ и т.п.

- **Избыточные базы (вирусы + RiskWare, SpyWare, AdWare)** – наиболее полные антивирусные базы. Помимо описанной выше информации, они включают в себя также описания шпионских программ (SpyWare) и рекламных программ (AdWare).

Шпионские программы позволяют несанкционированно получать персональную информацию (например, адреса посещаемых веб-сайтов, пароли, банковские реквизиты) и рассылать ее заинтересованным лицам.

Рекламные программы устанавливаются совместно с каким-либо программным обеспечением и в дальнейшем выводят рекламную информацию, либо отображая ее в дополнительных окнах, либо вынуждая пользователя посещать веб-сайт рекламодателя. Помимо того, что происходит навязывание рекламной информации, подобные программы также существенно загружают линии связи и увеличивают суммарный трафик.

Для обычного режима работы достаточно выбрать стандартные антивирусные базы. Расширенные и избыточные антивирусные базы используются для обеспечения более высокого уровня защиты информации. Использование более полных антивирусных баз приводит к увеличению затрат ресурсов системы на проверку данных.

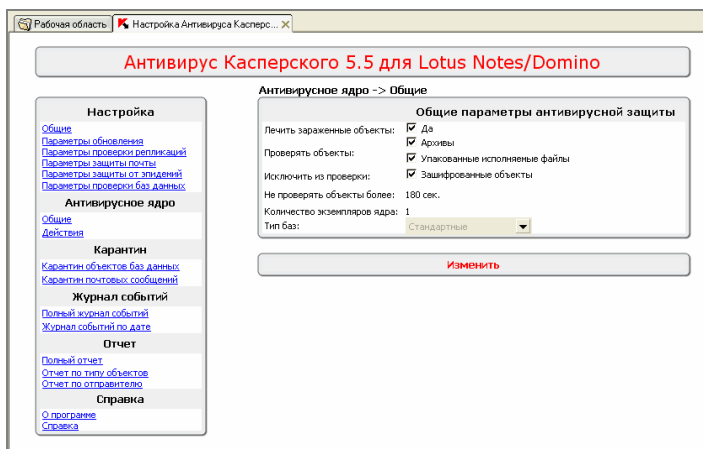


Рисунок 7. Закладка **Общие**

4.7.2. Действия над объектами различных статусов

В результате антивирусной проверки каждому объекту будет присвоен один из следующих статусов:

- **Незараженный** – объект не содержит вирусов.
- **Вылеченный** – объект был заражен и успешно вылечен.
- **Зараженный** – объект содержит вредоносный код.
- **Подозрительный** – объект содержит код неизвестного вируса либо модифицированный код известного вируса.
- **Поврежденный** – код объекта поврежден.
- **Непроверенный** – объект не может быть проверен (например, если объект защищен паролем).
- **Фильтр по размеру** – объект не проверен из-за того, что превышено значение размера объекта, установленное параметром **Фильтрация по размеру**.
- **Непроверенный из-за сбоя** – объект не проверен из-за системной ошибки (например, нет прав доступа к объекту).
- **Фильтр по типу** – объект не проверен, так как в настройках определено исключение объектов данного типа из проверки.
- **Фильтр по имени** – объект не проверен, так как в настройках определено исключение объектов с данным именем из проверки.
- **Фильтр по времени** – объект не проверен из-за превышения времени антивирусной проверки, определенного настройкой **Не проверять объекты более**.

В зависимости от статуса объекта к нему применяются различные действия. Настройка этих действий производится на закладках статусов проверки окна **Действия**. Перейти в данное окно вы можете из раздела **Антивирусное ядро** в панели результатов консоли Антивируса Касперского, выбрав ссылку [Действия](#) (см. рис. 8).

Вам предлагается выбрать одно из следующих действий над объектом:

- **Пропускать** – доставлять объект, не выполняя над ним никаких действий, лишь зафиксировать информацию о нем в отчете.
- **Удалять** – удалить объект.

- **Помещать на карантин** – поместить копию исходного объекта в хранилище карантина.
- Отправить уведомление об обнаружении объекта данного статуса. Для формирования письма-уведомления отметьте в группе настроек **Параметры уведомления** адресатов, которым будет отправлено письмо (подробнее см. 4.7.3 на стр. 35).
- **Добавлять информацию в отчет** – фиксировать информацию об обнаружении объектов данного статуса в отчете.

Для объектов со статусом **Вылеченный** Антивирус Касперского автоматически заменяет зараженный объект вылеченным.

Кроме того, с помощью настроек можно определить сохранение копии исходного объекта в карантине, и отправку уведомления об этом заданным адресатам.

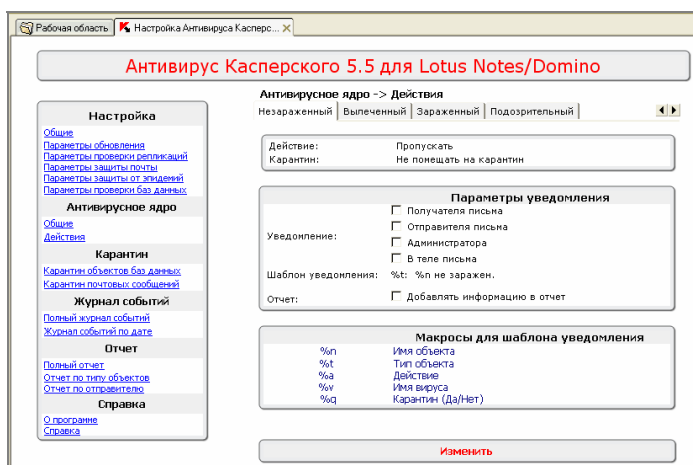


Рисунок 8. Закладка **Действия**

4.7.3. Уведомления

В процессе работы Антивируса Касперского происходит обнаружение объектов различных статусов, уведомления о которых возможно получать по электронной почте. Например, приложение может фиксировать обнаружение поврежденных объектов, проверка которых невозможна.

Для формирования уведомлений выставите флажок, указывающий адресата уведомления, на закладках статусов объектов после проверки (в окне **Действия** раздела **Антивирусное ядро**, см. рис. 8 на стр. 35).

При этом при проверке почтовых сообщений письмо-уведомление может быть отправлено:

- Администратору сервера;
- Отправителю почтового сообщения;
- Адресату почтового сообщения.

При проверке репликаций уведомление направляется только администратору.

Уведомление может быть направлено отдельным сообщением, а также быть добавлено в тело почтового сообщения с помощью опции **В теле письма**.



Если уведомление необходимо добавить в сообщение MIME-типа, оно будет преобразовано в формат Rich Text. При этом форматирование письма может быть нарушено.

Текст рассылаемых сообщений формируются с помощью шаблона уведомления.

Вид сформированного шаблона уведомлений представлен в строке **Шаблон** группы настроек **Параметры уведомления** окна **Действия** раздела **Антивирусное ядро**.

При формировании текста уведомления могут использоваться следующие макросов:

- **%n** – имя проверенного объекта;
- **%t** – тип проверенного объекта (тело письма, вложенный объект, архив и проч.);
- **%a** – действие, которое было применено к данному объекту;
- **%v** – имя вируса, которым заражен объект. Данная макроподстановка может быть использована только при обнаружении зараженного объекта;
- **%q** – помещен ли объект на карантин (макрос может принимать значение **Да** либо **Нет**).



Если в входящих уведомлениях некорректно отображается заголовок письма, вам следует изменить кодировку по умолчанию в настройках вашего почтового клиента (подробнее о настройках кодировки см. справку почтовой программы).

ГЛАВА 5. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

В процессе работы Антивирус Касперского для Lotus Notes/Domino использует:

- Базу **Карантин** для:
 - **объектов баз данных** – база объектов, отправленных на карантин в результате проверки модулями **Kavdbscanner** и **Kavrepmonitor**.
 - **почтовых сообщений** – база объектов, отправленных на карантин в результате проверки модулем **Kavmailmonitor**.
- **Журнал событий** – база, в которой хранятся уведомления о событиях, возникающих в процессе работы Антивируса Касперского.
- Базу **Отчет** – база, в которой хранится результирующая статистика всех проверенных объектов.

5.1. База Карантин

Карантин – это специальное хранилище, в которое помещаются объекты, подозреваемые на заражение вирусами или их модификациями.

Не всегда можно однозначно определить, является объект зараженным или нет. Причины могут быть следующие:

- Код анализируемого объекта похож на известную угрозу, но частично изменен.
Если вредоносная программа изменяется и в антивирусные базы эти изменения еще не внесены, то Антивирус Касперского отнесет объект, пораженный измененной вредоносной программой, к возможно зараженным объектам и обязательно укажет, на какую угрозу похоже это заражение.
- Код обнаруженного объекта напоминает по структуре вредоносную программу.

Вполне возможно, что это новый вид угроз, поэтому Антивирус Касперского относит такой объект к возможно зараженным объектам.

Перемещение объектов в карантин может быть полезно, если зараженный объект не может быть вылечен в данный момент. Если сохранить объект важно, его рекомендуется изолировать, а затем провести повторное лечение с помощью обновленной версии антивирусных баз.

Для того чтобы помещать объекты какого-либо статуса на карантин, установите флажок **Помещать на карантин** в окне **Действия** группы настроек **Антивирусное ядро** (подробнее о статусах объектов см. п. 4.7.2 на стр. 34).



Если в качестве действия над объектом статуса **Вылеченный** задано **Помещать на карантин**, в карантине будет сохранен объект после лечения, а не оригинальный.

Данные в базе карантина подразделяются на:

- **Карантин объектов баз данных** – раздел базы карантина для объектов баз данных сервера Domino.
- **Карантин почтовых сообщений** – раздел базы карантина для объектов почтовых сообщений.

5.1.1. Работа в карантине с документами баз данных

Для работы с карантинном объектом баз данных сервера Domino воспользуйтесь ссылкой [Карантин объектов баз данных](#), расположенной в разделе **Карантин** в панели результатов консоли Антивируса Касперского (см. рис. 9).

В правой части окна представлена таблица, содержащая следующую информацию:

- **Дата помещения объекта в карантин.**
- **Задача** – название модуля, в результате работы которого перехвачен зараженный объект.
- **База** – название базы, в которой содержался задержанный объект.
- **Изменено** – информация о пользователе, который последним изменял задержанный документ.
- **Вложения** – имя задержанного документа.

- **Количество записей** – суммарное количество объектов для каждой строки.

Если объект, помещенный на карантин, представляет высокую информационную ценность, его можно восстановить.



Обратите внимание, что восстановление изолированного объекта может привести к заражению сервера, поэтому эксперты «Лаборатории Касперского» рекомендуют выполнять это только в исключительных случаях.

Для восстановления объекта в окне **Карантин объектов баз данных** в разделе **База** выберите имя базы данных, документ которой вы хотите восстановить. В раскрывшемся списке выберите нужный объект и нажмите кнопку **Восстановить**. Документ будет перемещен из карантина в ту же базу, откуда он был удален.



Восстановить из карантина OLE-объект невозможно.

Антивирус Касперского 5.5 для Lotus Notes/Domino

Настройка

Общие
 Параметры обновления
 Параметры проверки сигнатур
 Параметры защиты почты
 Параметры защиты от эпидемий
 Параметры проверки баз данных

Антивирусное ядро

Общие
 Действия

Карантин

Карантин объектов баз данных
 Карантин почтовых сообщений

Журнал событий

Пользовательский журнал событий
 Журнал событий по дате

Отчет

Пользовательский отчет
 Отчет по типу объектов
 Отчет по отправителю

Справка

Справка
 Справка

Выделить все

Дата	Задача	База	Изменено	Вложения
02.05.2007		KavDbScanner	Test	
			TestDB.nsf	
			administrator	eicar.com
			administrator	eicar.com
			administrator	eicar.com
			administrator	eicar.com
			administrator	eicar.com
			administrator	eicar.com

База	Test\TestDB.nsf
Документ	36CF9F95CE4FD6A4C32572CF004CBF97
Изменено	02.05.2007 17:58:26 пользователем CN=administrator
Сервер	CN=tids/O=urixvm

В доставленном сообщении:
 Вложение: eicar.com заражен EICAR-Test-File. Выполнено действие: Объект удален. Помещен на карантин: Да.

Оригинальные объекты:

Восстановить

Рисунок 9. Закладка **Карантин баз данных**

Объект сохраняется в карантине до тех пор, пока его не удалит администратор. Рекомендуется периодически проводить удаление объектов, не имеющих информационной ценности, из карантина.



Чтобы удалить объект из карантина вручную:

- В таблице, отображающей содержимое хранилища, выберите объект для удаления.
- Откройте контекстное меню и воспользуйтесь командой **Удалить**.
- В результате объект будет отмечен специальной меткой для удаления.

5.1.2. Работа с объектами почтовых сообщений в базе карантина

Для работы с базой карантина объектов почтовых сообщений воспользуйтесь ссылкой [Карантин почтовых сообщений](#), расположенной в разделе **Карантин** в панели результатов консоли Антивируса Касперского (см. рис. 10).

Правая часть окна карантина оформлена в виде таблицы, в которой содержится следующая информация:

- **Отправитель** – адрес отправителя задержанного объекта почтового сообщения.
- **Тема** – тема письма.

Любой объект в карантине почтовых сообщений представляет собой документ, содержащий следующие данные:

- **Отправитель** – адрес отправителя задержанного объекта почтового сообщения.
- **Получатели** – адрес получателей объекта почтового сообщения.
- **Тема** – тема письма.
- **Сервер** – имя защищаемого сервера.
- **Результат проверки** – статус объекта после антивирусной проверки (например, *Не проверен из-за сбоя*).
- **Выполнено действие** – действие, произведенное над объектом в соответствии с параметрами проверки.
- **Вложение** – исходное имя вложенного объекта, а также результат его проверки Антивирусом Касперского.



Иногда в почтовое сообщение вложено несколько объектов с одинаковыми именами. В этом случае при отображении результатов проверки оригинальное имя будет сохранено только для одного из вложений, а для прочих будут отражены их уникальные системные имена.

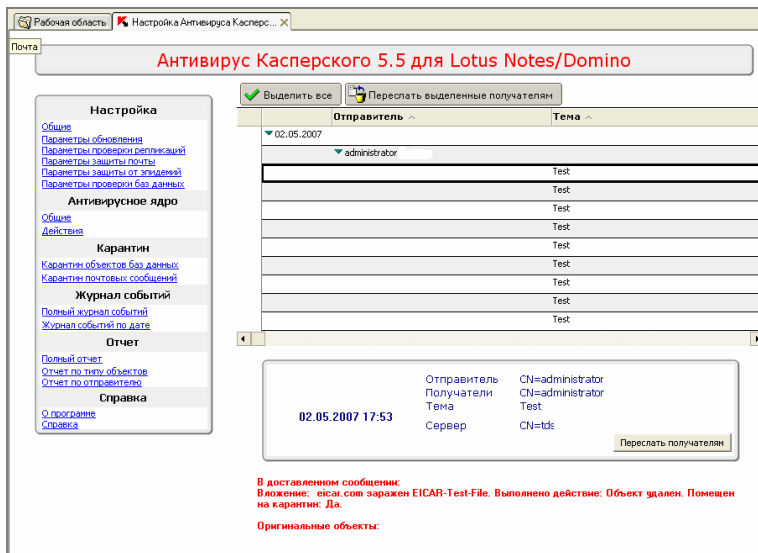


Рисунок 10. Закладка **Карантин почтовых сообщений**

В дальнейшем почтовое сообщение из карантина можно:

- **Переслать получателю** в целях получения информации, содержащейся в сообщении.
- **Удалить**. Удаление почтового сообщения проводится аналогично процедуре удаления объекта из карантинного хранилища баз данных (подробнее об этом см. п. 5.1.1 на стр. 38).



Для пересылки получателю объектов почтового сообщения из карантина:

- В таблице, отображающей содержимое хранилища, выберите объект для восстановления.
- Нажмите на кнопку **Переслать получателю**.
- Перед отправкой сообщения выводится предупреждение с запросом на подтверждение операции. Для восстановления письма из карантина нажмите на кнопку **ОК**.

В результате объект будет отправлен из хранилища карантина указанному адресату.



Сообщение MIME-типа может быть перенесено в карантин несколькими частями.

В процессе проверки Антивирус Касперского разделяет MIME-сообщения на части и если время проверки превысит максимально-допустимое значение, все части будут отправлены в карантин отдельно.

Особый случай возникает при восстановлении из карантина объекта реплицируемой базы почтовых сообщений.

Если вам будет прислано зараженное письмо, Антивирус Касперского автоматически выполнит над ним действие, указанное в настройках (например, заменит инфицированную часть вылеченной) и реплицирует сообщение в соответствующую базу на другом сервере. Инфицированная часть будет помещена на карантин. Однако если возникнет необходимость восстановления зараженного объекта из карантина, письмо будет вновь перехвачено при попытке репликации и повторно передано на карантин.



Таким образом, правило проверки репликаций запрещает восстановить объект из карантина. Если вам необходимо извлечь зараженную часть письма, временно снимите флажок **Проверять следующие объекты:** в окне **Параметры защиты репликаций** группы **Настройка**.

5.2. Журнал событий

Информация о событиях, возникающих при работе Антивируса Касперского, фиксируется в **Журнале событий** приложения (см. рис. 11). Все записи в журнале можно просматривать, группируя их следующим образом:

- [Полный журнал событий](#) – список записей без группировки.
- [Журнал событий по дате](#) – список записей, сгруппированных по дате возникновения события.

Сообщения в базе отмечаются специальными графическими значками и могут быть следующих видов:

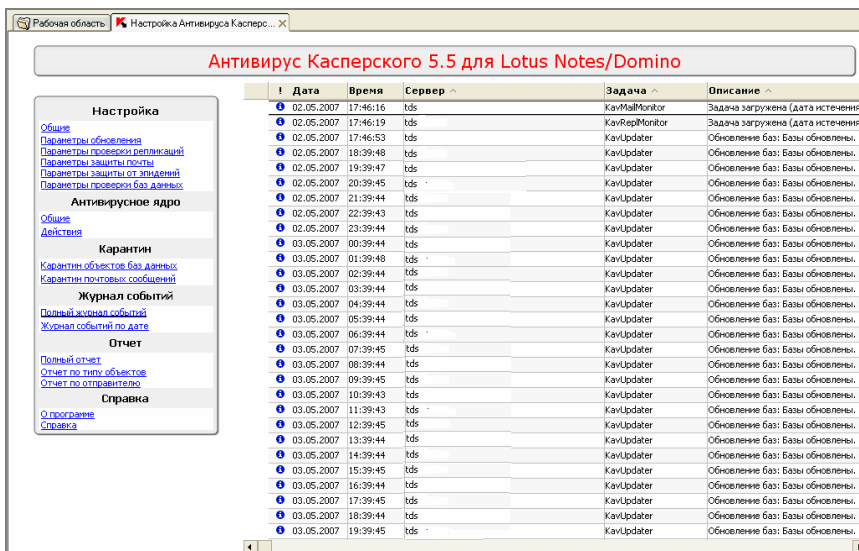
-  – информационное сообщение;
-  – сообщение о происшествии, на которое рекомендуется обратить внимание;

-  – сообщение о критическом событии в работе программы.

Просмотреть журнал событий можно, нажав на соответствующую ссылку в разделе **Журнал событий** панели результатов консоли Антивируса Касперского (см. рис. 11).

Структура записей для любой группы представляет собой таблицу с графами:

- **Дата** – дата формирования записи в журнале.
- **Время** – время формирования записи в журнале.
- **Сервер** – имя сервера, от которого пришло уведомление о событии.
- **Задача** – название модуля, при работе которого произошло событие.
- **Описание** – в окне содержится полное описание события.



The screenshot shows the configuration window for Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino. The left sidebar contains navigation options: Настройка (Общие, Обновления, Репликация, Защита почты, Проверка баз данных), Антивирусное ядро (Общие, Действия), Карантин (Объекты, Почтовые сообщения), Журнал событий (Полный журнал, По дате), Отчет (Полный отчет, По типу объектов, По администратору), and Справка (О программе, Справка). The main area displays a table of events.

Дата	Время	Сервер	Задача	Описание
02.05.2007	17:46:16	tds	KavMailMonitor	Задача загружена (дата истечения)
02.05.2007	17:46:19	tds	KavRepMonitor	Задача загружена (дата истечения)
02.05.2007	17:46:53	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	18:39:48	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	19:39:47	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	20:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	21:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	22:39:43	tds	KavUpdater	Обновление баз: Базы обновлены.
02.05.2007	23:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	00:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	01:39:48	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	02:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	03:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	04:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	05:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	06:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	07:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	08:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	09:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	10:39:43	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	11:39:43	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	12:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	13:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	14:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	15:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	16:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	17:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	18:39:44	tds	KavUpdater	Обновление баз: Базы обновлены.
03.05.2007	19:39:45	tds	KavUpdater	Обновление баз: Базы обновлены.

Рисунок 11. Полный журнал событий








5.3. Отчеты о работе приложения

Результаты антивирусной проверки объектов фиксируются в отчетах о работе приложения (см. рис. 12). Отчеты можно просматривать, группируя их следующим образом:

- [Полный отчет](#) – список записей без группировки.
- [Отчет по типу объектов](#) – список записей, сгруппированных по статусам проверенных объектов.
- [Отчет по отправителю](#) – список записей, сгруппированных по адресу отправителя (только для почтовых сообщений).

Просмотреть отчеты можно выбрав соответствующую ссылку в разделе **Отчет** панели результатов консоли Антивируса Касперского.

Структура записей в базе отчетов аналогична журналу событий и содержит следующие поля:

- Графический значок, отображающий результаты антивирусной проверки объекта:
 -  – объект не заражен;
 -  – объект был заражен и успешно вылечен;
 -  – объект заражен;
 -  – объект подозревается на заражение;
 -  – объект поврежден;
 -  – объект не может быть проверен;
 -  – объект не проверен из-за системного сбоя или настроек фильтрации.
- **Дата** – дата записи отчета об антивирусной проверке конкретного объекта в базу.
- **Время** – время записи отчета об антивирусной проверке конкретного объекта в базу.
- **Сервер** – имя сервера, на котором выполнялась проверка.
- **Задача** – название модуля, результаты работы которого зафиксированы в отчете.

- **Описание** – имя вируса, если проверенный объект заражен. Если объект не заражен, в графе будет указано его имя и статус после антивирусной проверки.
- **Отправитель** – электронный адрес, с которого были отправлены проверенные объекты.

Дата	Время	Сервер	Задача	Описание
02.05.2007	17:53:17	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:53:56	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:53:58	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:00	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:01	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:02	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:04	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:05	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:07	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	17:54:08	CN	KavMailMonitor	EICAR-Test-File
02.05.2007	18:00:28	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:28	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
02.05.2007	18:00:29	CN	KavOBScanner	EICAR-Test-File
03.05.2007	15:28:01	CN	KavOBScanner	EICAR-Test-File

Рисунок 12. Зкладка **Полный отчет**

Обратите внимание, что формирование отчета об обнаружении объекта определенной статуса задается в разделе **Действия** группы настроек **Антивирусное ядро**.

5.4. Работа с ключами

Возможность использования Антивируса Касперского определяется наличием *ключа*. Ключ входит в поставку продукта и дает вам право использовать программу со дня приобретения и установки ключа.

По окончании действия ключа функциональность программы сохраняется за исключением возможности обновления антивирусных баз. Вы по-прежнему можете выполнять проверку, но только на антивирусных базах, актуальных на дату окончания ключа. Следовательно, «Лаборатория Касперского» не гарантирует вам стопроцентную защиту от новых вирусов, которые появятся после окончания действия ключа программы.

В приложении предусмотрено ограничение работы по сроку его использования (как правило, это срок в один год со дня приобретения). **За две недели** до истечения срока действия ключа во время работы приложения отсылается предупреждающее уведомление. В нем содержится информация о дате окончания установленного ключа.

Чтобы избежать заражения новыми вирусами, мы рекомендуем вам продлить ключ на использование Антивируса Касперского.

В течение срока действия ключа вам предоставляются следующие возможности:

- использование антивирусной функциональности приложения;
- обновление антивирусных баз каждый час;
- обновление приложения (patch);
- получение новых версий приложения (upgrade);
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного приложения, оказываемые круглосуточно по телефону и электронной почте;
- возможность переслать обнаруженные зараженные и подозрительные объекты в «Лабораторию Касперского» для исследования.

У приложения может быть только один действующий ключ. В нем содержатся ограничения на использование Антивируса Касперского, которые могут быть проверены специальными механизмами приложения.

5.4.1. Продление ключа

Продление ключа на использование Антивируса Касперского дает вам право на восстановление полной функциональности приложения.



«Лаборатория Касперского» регулярно проводит акции, позволяющие продлить ключ на использование наших продуктов со значительными скидками. Следите за акциями на сайте «Лаборатории Касперского» в разделе **Продукты → Акции и спецпредложения**.



Чтобы продлить ключ Антивируса Касперского, вам необходимо:

Связаться с компанией, у которой вы купили продукт, и приобрести новый ключ на использование Антивируса Касперского 5.5 для Lotus Notes/Domino.

или:

Приобрести ключ непосредственно в «Лаборатории Касперского», написав запрос в Отдел продаж (sales@kaspersky.com) или заполнив соответствующую форму на нашем сайте (www.kaspersky.ru). По факту оплаты вам будет отправлен ключ по электронному адресу, который был указан вами в форме заказа.

Приобретенный ключ необходимо установить с помощью модуля **Kavmailmonitor**.



Чтобы установить новый ключ вам необходимо:

- Остановить работу модуля **kavmailmonitor**. Для этого в командной строке введите:

```
tell kavmailmonitor quit
```

- Скопируйте файл ключа на сервер.
- Запустите установку ключа. Для этого в командной строке введите:

```
load kavmailmonitor <полный-путь-к-файлу-ключа>
```

Информация о ключе отображается при запуске приложения.

Если вы хотите установить новый ключ до истечения срока действия активного ключа, вы можете установить его в качестве резервного. Резервный ключ становится активным начиная с даты окончания срока действия предыдущего ключа.



Чтобы установить резервный ключ в командной строке введите:

```
tell kavmailmonitor addreservekey <полный-путь-к-файлу-ключа>
```

После этого при запуске приложения на консоль сервера будет выводиться информация как об активном, так и о резервном ключах.



Чтобы удалить резервный ключ в командной строке введите:

```
tell kavmailmonitor removereservekey
```

5.5. Работа с программой из командной строки

Вы можете работать с Антивирусом Касперского посредством командной строки. Любая введенная команда должна иметь следующий синтаксис:

```
tell <имя_задачи> <строка>
```

где

имя задачи – название модуля, выполняющего данную задачу;

строка – системная команда.



Чтобы просмотреть установленную версию приложения, в командной строке введите:

```
tell kavmailmonitor version
```



Чтобы просмотреть серийный номер установленного ключа, в командной строке введите:

```
tell kavmailmonitor keyinfo
```



Чтобы остановить проверку баз данных, в командной строке введите:

```
tell kavdbscanner stop
```



Чтобы просмотреть время, в которое будет запущена следующая антивирусная проверка, в командной строке введите:

```
tell kavdbscanner shownext
```



Чтобы удалить информацию о результатах предыдущих проверок баз, в командной строке введите:

```
tell kavdbscanner rlsd
```



Чтобы запустить обновление антивирусных баз, в командной строке введите:

```
tell kavupdater start
```



Чтобы просмотреть время, в которое будет запущено следующее обновление антивирусных баз, в командной строке введите:


```
tell kavupdater shownext
```



Настоятельно рекомендуем вам не использовать для остановки проверки почтовых сообщений команду **tell kavmailmonitor quit**. В результате выполнения данной команды доставка писем через сервер будет блокирована.

ГЛАВА 6. ПРОВЕРКА КОРРЕКТНОСТИ РАБОТЫ ПРИЛОЖЕНИЯ

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить правильность настроек и корректность работы программы с помощью тестового «вируса» и его модификаций.

Тестовый «вирус» был специально разработан организацией  (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ ВИРУСОМ и не содержит программного кода, который может навредить вашему компьютеру, при этом большинство продуктов антивирусных компаний-производителей идентифицируют его как вирус.



Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!

Загрузить тестовый «вирус» можно с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

При попытке загрузки тестового «вируса» Антивирус Касперского обнаруживает его, идентифицирует как зараженный объект, не подвергающийся лечению, и выполняет действие, установленное администратором для такого объекта.



Рекомендуется произвести проверку работы Антивируса для входящей и исходящей почты, как в теле сообщения, так и во вложении. Для проверки обнаружения вирусов в теле сообщения, поместите текст стандартного или модифицированного «вируса» в тело сообщения.

ПРИЛОЖЕНИЕ А.

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В данной главе мы осветим наиболее часто задаваемые пользователями вопросы по установке, настройке и работе Антивируса Касперского и постараемся ответить на них наиболее подробно.



Вопрос: возможно ли использование Антивируса Касперского с антивирусными продуктами других производителей?

Во избежание конфликтов мы рекомендуем удалять антивирусные продукты сторонних производителей до установки Антивируса Касперского.



Вопрос: почему Антивирус Касперского вызывает определенное снижение производительности компьютера и ощутимо нагружает процессор?

Обнаружение вирусов является вычислительной (математической) задачей, связанной с анализом структур, подсчетом контрольных сумм и математическими преобразованиями данных. Поэтому основным ресурсом, который потребляется Антивирусом в процессе работы, является процессорное время. При этом каждый новый вирус, добавленный в антивирусную базу, увеличивает общее время проверки.

В отличие от других антивирусов, сокращающих время проверки путем исключения из антивирусных баз более сложных в обнаружении или более редких (например, в географическом отношении) вирусов, а также более сложных в анализе форматов файлов (например, pdf), Антивирус Касперского включает в свои базы всю доступную информацию обо всех известных вирусах. В зависимости от желаемой степени безопасности, пользователь может ускорить проверку путем отключения антивирусной проверки различных типов файлов.

Антивирус Касперского распознает более 1200 форматов архивированных и упакованных файлов, а файлы четырех форматов лечит. Это очень важно для антивирусной безопасности. Тем не менее, благодаря оптимизации работы различных модулей программы и улучшению алгоритмов распознавания вирусов, новая версия продукта работает быстрее, чем предыдущая.



Вопрос: зачем нужен ключ? Может ли мой Антивирус работать без него?

Без ключа Антивирус Касперского не работает.

Если вы еще не решились на приобретение Антивируса Касперского, мы можем предоставить вам пробный ключ (trial-key), который будет работать в течение двух недель или месяца. По истечении данного срока ключ будет заблокирован.



Вопрос: что произойдет, когда истечет ключ на использование приложения?

По истечении срока действия ключа на использование Антивируса Касперского приложение будет продолжать работу, но использование новых антивирусных баз станет невозможным. Антивирус по-прежнему будет выполнять лечение зараженных объектов, но с использованием старых антивирусных баз.

Если на вашем сервере была установлена пробная версия Антивируса (версия с пробным ключом или ключом для бета-тестирования), по истечении срока действия ключа антивирусная проверка производится не будет.

При возникновении данной ситуации проинформируйте вашего системного администратора или обратитесь за продлением ключа в компанию, где был приобретен Антивирус Касперского, либо непосредственно в ЗАО «Лаборатория Касперского».



Вопрос: Зачем нужны ежечасные обновления?

Еще несколько лет назад вирусы передавались на дискетах и для защиты компьютера достаточно было установить антивирусную программу и изредка обновлять антивирусные базы. Но последние вирусные эпидемии распространялись по миру всего за несколько часов, и установленный Антивирус со старыми базами может оказаться бессильным перед новой угрозой.

«Лаборатория Касперского» с каждым годом увеличивает частоту обновления антивирусных баз. Сейчас они обновляются ежечасно. Мы рекомендуем вам обновлять антивирусные базы на вашем компьютере также ежечасно, для того чтобы не стать жертвой новых вирусов.

Дополнительной функцией является обновление программных модулей Антивируса, при исправлении обнаруженных уязвимостей или с добавлением новых функциональных возможностей.



Вопрос: может ли злоумышленник подменить антивирусные базы?

Все антивирусные базы имеют уникальную подпись, и при обращении к базам Антивирус Касперского проверяет ее. Если подпись не соответствует присвоенной в «Лаборатории Касперского» или дата баз – более поздняя, чем день окончания ключа на использование продукта, Антивирус Касперского не будет использовать такие базы.



Вопрос: после установки Антивируса почта помещается в системный почтовый ящик, но не проверяется. Почему?

Убедитесь, что после установки приложения запустился модуль **kavmailmonitor**. Для этого в командной строке введите:

```
show tasks
```

В выведенном на экран списке задач проверьте наличие модуля **kavmailmonitor**. Если задача отсутствует, запустите задачу самостоятельно с помощью строки:

```
load kavmailmonitor
```

Если задача не запустилась, отправьте письмо с описанием проблемы в Службу технической поддержки.



Вопрос: в настройках задано удаление зараженных объектов, вложенных в почтовое сообщение. Однако сообщения по-прежнему доставляются с вложенным файлом. Почему?

Особенности архитектуры Lotus Notes/Domino не позволяет удалить вложенный файл целиком. Однако если в настройках Антивируса Касперского администратором задано удаление зараженных вложенных объектов, то любое инфицированное вложение будет заменено вложением-шаблоном. Шаблон вложения – текстовый файл **kavdumtmy.txt**, находящийся в папке Domino установленного сервера. Файл помещается в папку при установке Антивируса Касперского и по умолчанию содержит слово **EMPTY**.



Вопрос: мой Антивирус не работает. Что мне делать?

Мы рекомендуем обратиться к фирме, продавшей вам Антивирус Касперского или написать письмо в Службу технической поддержки.

ПРИЛОЖЕНИЕ В. КОДЫ ВОЗВРАТА МОДУЛЯ KAVUPDATER

В процессе работы модуль **Kavupdater** фиксирует свое состояние с помощью кодов возврата, записываемых в логи приложения. Рассмотрим значение некоторых кодов, знание которых может быть полезно.

Код	Значение
0	Обновление прошло успешно.
1	Невозможно создать папку для хранения обновлений.
2	Недостаточно прав на выполнение операции.
3	Обрыв сетевого соединения.
4	Базы не требуют обновления.
6	Источник обновления не содержит всех необходимых файлов.
10	Базы актуальны, обновления не требуется.
11	Обновлены не все модули.
17	Ошибка проверки подписи файла.
19	Операция отменена пользователем.
20	Невозможно обновить антивирусные базы.

Код	Значение
21	Повреждена более ранняя версия антивирусных баз.
28	Сетевая ошибка при загрузке файлов обновления.
29	Сетевое соединение разорвано.
30	Превышено время ожидания ответа от сервера обновлений.
31	Ошибка авторизации на FTP.
32	Ошибка авторизации на прокси-сервере.
33	Не найден источник обновления.
38	Ошибка при подключении к источнику обновления.
41	Ошибка при подключении к прокси-серверу.
42	Невозможно обновить антивирусные базы. Ошибка при определении имени прокси-сервера.

ПРИЛОЖЕНИЕ С. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ЗАО «Лаборатория Касперского» была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более четырехсот пятидесяти высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

С.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

Программа Новостной Агент предназначена для оперативной доставки новостей «Лаборатории Касперского», оповещения о «вирусной погоде» и появлении свежих новостей. С заданной периодичностью программа считывает с новостного сервера «Лаборатории Касперского» список доступных новостных каналов и содержащуюся в них информацию.

Новостной Агент также позволяет:

- визуализировать в системной панели состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в браузере. Таким образом, пользователи могут максимально оперативно получать ответ на вопросы,

связанные с заражением вредоносными программами. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется непосредственно в браузере. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- лечить обнаруженные зараженные объекты;
- сохранять отчеты о результатах проверки в форматах txt и html.

Антивирус Касперского® 6.0

Антивирус Касперского 6.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP – для исходящих) независимо от используемой почтовой программы, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно запустить анализ на присутствие вирусов только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе.* Программа позволяет создавать список приложений, компонентный состав которых будет

контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.

- *Наблюдение за процессами в оперативной памяти.* Антивирус Касперского 6.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.
- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.
- *Блокирование опасных макросов* Visual Basic for Applications в документах Microsoft Office.
- *Восстановление системы* после вредоносного воздействия программ-шпионов за счет фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 6.0

Kaspersky Internet Security 6.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;
- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы*: антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;
- *проактивную защиту*: программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные

изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных скриптов на веб-страницах, всплывающих окон и рекламных баннеров). Функция *блокирования автоматического дозвола на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и блокировать их работу.

Kaspersky Internet Security 6.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На *основе заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим невидимости *предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского® Mobile

Антивирус Касперского Mobile обеспечивает антивирусную защиту мобильных устройств, работающих под управлением операционных систем Symbian OS и Microsoft Windows Mobile. Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- *проверку по требованию* памяти мобильного устройства, карт памяти, отдельной папки либо конкретного файла. При обнаружении зараженного объекта он помещается на карантин или удаляется;
- *постоянную защиту*: автоматически проверяются все входящие или изменяющиеся объекты, а также файлы при попытке доступа к ним;

- *защиту от sms- и mms-спама.*

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare, Linux и Samba от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux File Server.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени:* все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- *предотвращение вирусных эпидемий;*
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- *восстановление системы после заражения;*
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *соблюдение баланса загрузки системы;*
- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуются их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;

- *оповещения о событиях* в работе программного продукта администратора системы;
- *ведение детальных отчетов*;
- *автоматическое обновление баз* программного продукта.

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Kaspersky Open Space Security включает в себя четыре продукта:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Рассмотрим подробнее каждый продукт.

Kaspersky WorkSpace Security – это продукт для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- целостная защита от вирусов, шпионских программ, хакерских атак и спама;
- *проактивная защита* от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- отмена вредоносных изменений в системе;
- защита от фишинг-атак и нежелательной почтовой корреспонденции;
- динамическое перераспределение ресурсов при полной проверке системы;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;

- *поддержка Cisco® NAC (Network Admission Control);*
- проверка электронной почты и интернет-трафика в режиме реального времени;
- блокирование всплывающих окон и рекламных баннеров при работе в интернете;
- безопасная работа в сетях любого типа, включая Wi-Fi;
- *средства для создания диска аварийного восстановления, позволяющего восстановить систему после вирусной атаки;*
- развитая система отчетов о состоянии защиты;
- автоматическое обновление баз;
- полноценная поддержка 64-битных операционных систем;
- *оптимизация работы программного продукта на ноутбуках (технология Intel® Centrino® Duo для мобильных ПК);*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™).*

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и безопасность доступа пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC (Network Admission Control);*
- защита рабочих станций и файловых серверов от всех видов интернет-угроз;
- использование технологии iSwift для исключения повторных проверок в рамках сети;
- распределение нагрузки между процессорами сервера;
- *изоляция подозрительных объектов* рабочих станций в специальном хранилище;

- отмена вредоносных изменений в системе;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- проверка электронной почты и интернет-трафика в режиме реального времени;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- защита при работе в беспроводных сетях Wi-Fi;
- технология самозащиты антивируса от вредоносных программ;
- изоляция подозрительных объектов в специальном хранилище;
- автоматическое обновление баз.

Kaspersky Enterprise Space Security

Программный продукт включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- защита рабочих станций и серверов от вирусов, троянских программ и червей;
- защита почтовых серверов Sendmail, Qmail, Postfix и Exim;
- проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;
- обработка сообщений, баз данных и других объектов серверов Lotus Domino;
- защита от фишинг-атак и нежелательной почтовой корреспонденции;
- предотвращение массовых рассылок и вирусных эпидемий;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- безопасная работа в беспроводных сетях Wi-Fi;
- *проверка интернет-трафика* в режиме реального времени;
- отмена вредоносных изменений в системе;
- динамическое перераспределение ресурсов при полной проверке системы;
- изоляция подозрительных объектов в специальном хранилище;
- *система отчетов* о состоянии системы защиты;
- автоматическое обновление баз.

Kaspersky Total Space Security

Решение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама* на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;
- защита почтовых серверов и серверов совместной работы;

- *проверка интернет-трафика* (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- блокирование доступа с зараженных рабочих станций;
- предотвращение вирусных эпидемий;
- централизованные отчеты о состоянии защиты;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC* (Network Admission Control);
- поддержка аппаратных прокси-серверов;
- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- использование технологии iSwift для исключения повторных проверок в рамках сети;
- динамическое перераспределение ресурсов при полной проверке системы;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- безопасная работа пользователей в сетях любого типа, включая WiFi;
- защита от фишинг-атак и нежелательной почтовой корреспонденции;
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™);
- отмена вредоносных изменений в системе;
- технология самозащиты антивируса от вредоносных программ;
- полноценная поддержка 64-битных операционных систем;
- автоматическое обновление баз.

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в

себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Антивирус Касперского для Lotus Notes/Domino.
- Антивирус Касперского для Microsoft Exchange.
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *фильтрация нежелательной почтовой корреспонденции;*
- *проверка входящих и исходящих почтовых сообщений и вложений;*
- *антивирусная проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino;*
- *фильтрация сообщений по типам вложений;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления программным продуктом;*
- *предотвращение вирусных эпидемий;*
- *мониторинг состояния системы защиты с помощью уведомлений;*
- *система отчетов о работе приложения;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- Kaspersky Administration Kit.
- Антивирус Касперского для Proxy Server.
- Антивирус Касперского для Microsoft ISA Server.
- Антивирус Касперского для Check Point FireWall-1.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *проверка интернет-трафика (HTTP/FTP) в режиме реального времени;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления;*
- *система отчетов о работе приложения;*
- *поддержка аппаратных прокси-серверов;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая списки DNS Black List и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознавать и уничтожить до девяноста пяти процентов нежелательного трафика.

Kaspersky® Anti-Spam представляет собой фильтр, который устанавливается на «входе» в сеть предприятия и проверяет входящий поток писем на предмет обнаружения спама. Продукт совместим с любой почтовой системой, используемой в сети заказчика, и может быть установлен как на уже существующий почтовый сервер, так и на выделенный.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации

образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

Антивирус Касперского® для MIMESweeper обеспечивает высокоскоростную антивирусную проверку трафика на серверах, использующих Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

С.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700, +7 (495) 645-79-39
Экстренная круглосуточная помощь:	+7 (495) 797-8707, +7 (495) 645-79-29
Поддержка пользователей персональных продуктов и Business Optimal:	+7 (495) 797-8707, +7 (495) 645-79-29 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка пользователей Corporate Suite:	Телефоны и электронный адрес предоставляются при покупке Corporate Suite в зависимости от пакета технической поддержки.
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-8700, +7 (495) 645-79-39 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700, +7 (495) 645-79-39 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru