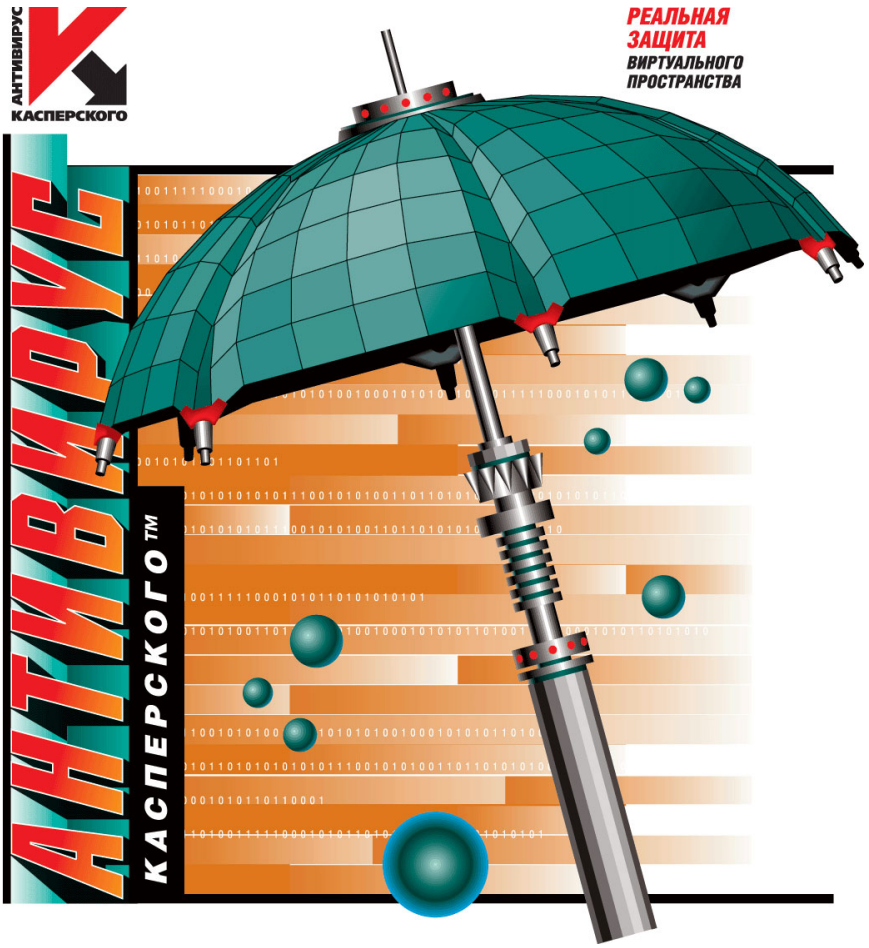
ЛАБОРАТОРИЯ КАСПЕРСКОГО



Антивирус Касперского® 5.5 для Microsoft Exchange Server 2000/2003

Руководство администратора

АНТИВИРУС КАСПЕРСКОГО® 5.5 ДЛЯ MICROSOFT EXCHANGE SERVER 2000/2003

Руководство администратора

Тел., факс: +7 (095) 797-87-00
http://www.kaspersky.ru

Дата редакции: июнь 2005 года

Содержание

ГЛАВА 1. ВВЕДЕНИЕ

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при работе с электронной почтой. Наличие почтовых приложений практически на каждом компьютере, а также то, что вредоносные программы полностью используют содержимое электронных адресных книг для выявления новых жертв, обеспечивает благоприятные условия для распространения вредоносных программ. Пользователь зараженного компьютера, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Нередки случаи, когда зараженный файл-документ по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысячам своих абонентов.

Помимо угрозы проникновения вредоносных программ существуют проблемы внешней нежелательной корреспонденции и использования интернет-ресурсов. Не являясь источником прямой угрозы, нежелательная корреспонденция, приводит к потерям рабочего времени и наносит значительные финансовые потери.

Также важно отметить, что новые вирусные программы стали использовать, так называемые, спамерские технологии для массового распространения; методы социотехники, чтобы заставить пользователя открыть письмо и т.п. Из этого следует, что возможности фильтрации спама важны не только сами по себе, но и для противодействия некоторым новым видам вирусных программ.

Сегодня всеми признается, что информация является для многих предприятий более ценным достоянием, нежели материальные и денежные активы. В то же время для извлечения прибыли из информации она должна быть доступна сотрудникам, клиентам и партнерам предприятия. Таким образом, встает вопрос об информационной безопасности и, как следствие, об одной из важных ее составляющих – защите почтовых серверов предприятия от внешних угроз, предотвращении эпидемий внутри предприятия и фильтрации корреспонденции с нежелательным содержанием.

1.1. Компьютерные вирусы и вредоносные программы

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.

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.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Также широкое распространение получили следующие потенциально опасные программы:

Программы-рекламы (*AdWare*) – программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы собирают и переправляют своему разработчику персональную информацию о пользователе, изменяют различные параметры браузера (стартовые и поисковые страницы, уровни безопасности и т.д.), а также создают неконтролируемый пользователем трафик. Все это может привести как к нарушению политики безопасности, так и к прямым финансовым потерям.

Потенциально опасное программное обеспечение (*RiskWare*) – программное обеспечение, которое не имеет какой-либо вредоносной функции, но может быть использовано злоумышленниками в качестве вспомогательных компонентов вредоносной программы, поскольку содержит бреши и ошибки. В эту категорию попадают, например, программы удаленного администрирования, IRC-клиенты, FTP-сервера, всевозможные утилиты для остановки процессов или скрытия их работы.

Программы-шпионы (*SpyWare*) – программное обеспечение, целью которого является несанкционированный доступ к данным пользователя, отслеживание действий на компьютере, сбор информации о содержании жесткого диска. Они позволяют злоумышленнику не только собирать информацию, но и контролировать чужой компьютер. Программы-шпионы, как правило, распространяются вместе с бесплатным программным обеспечением и устанавливаются на компьютер незаметно для пользователя. К таковым относятся клавиатурные шпионы, программы взлома паролей, программы сбора кониденциальной информации (например, номеров кредитных карт).

Программы автодозвона (*PornWare*) – программы, которые осуществляют модемное соединение с различными платными интернет-ресурсами, как правило, порнографического содержания.

Хакерские утилиты (*Hack Tools*) – программное обеспечение, которое используется злоумышленниками в собственных целях для проникновения на ваш компьютер. К ним относятся различные нелегальные сканеры уязвимостей, программы для взлома паролей,

прочие виды программ для взлома сетевых ресурсов или проникновения в атакуемую систему.

Основными источниками распространения вредоносных программ является электронная почта и интернет, хотя заражение может также произойти через дискету или CD-диск. Это обстоятельство предопределяет смещение акцентов антивирусной защиты с простых регулярных проверок компьютера на присутствие вирусов на более сложную задачу постоянной защиты компьютера от возможного заражения.

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. Назначение и основные функции Антивируса Касперского

Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 (далее **Антивирус Касперского**) предназначен для антивирусной защиты почтовых ящиков и общих папок на Microsoft Exchange Server 2000/2003 (далее **Microsoft Exchange Server**).
Антивирус Касперского позволяет:

- *проверять входящие и исходящие сообщения* на присутствие вредоносных объектов. При этом проверяются все атрибуты и вложения письма.
- *обрабатывать атрибуты и вложения письма.* В зависимости от настроек приложение лечит, удаляет, либо сопровождает предупреждающей информацией вредоносные объекты.
- *сохранять резервные копии объектов письма* перед лечением или удалением в специальном хранилище для последующего восстановления, что исключает возможность потери информации. Наличие настраиваемых фильтров позволяет легко находить исходные копии конкретных объектов.
- *уведомлять* отправителя, получателя и системного администратора о сообщении, содержащем вредоносный объект.
- *вести журналы событий и создавать регулярные отчеты о работе приложения и состоянии антивирусной защиты.*

Программа позволяет формировать отчеты по встроенным шаблонам с необходимой степенью детализации и периодичностью.

- *фиксировать возникновение эпидемий и уведомлять о них*. Приложение фиксирует попытки массовой рассылки зараженных сообщений как из интернета, так и с компьютеров внутри сети предприятия.

- *осуществлять настройку параметров работы приложения* в соответствии с объемом и характером проходящего трафика, а также характеристиками установленного оборудования (объем оперативной памяти, быстродействие, количество процессоров и пр.) как в ручном, так и в автоматическом режиме.

- *обновлять антивирусные базы* через интернет как автоматически, так и в ручном режиме. Ресурсом обновления баз являются ftp- и http-сервера обновлений Лаборатории Касперского.

Поиск вирусов и лечение зараженных объектов выполняются на основании записей *антивирусных баз*, содержащих описание всех известных на настоящий момент вирусов, способов лечения пораженных ими объектов, а так же описание потенциально опасного программного обеспечения.
Крайне важно поддерживать антивирусные базы в актуальном состоянии, поскольку каждый день появляются новые вирусы.
На серверах Лаборатории Касперского антивирусные базы обновляются каждый **час**. Мы рекомендуем обновлять антивирусные базы приложения с той же периодичностью (см. Глава 6 на стр. 64).

- *проверять старые (проверенные ранее) сообщения на присутствие новых вирусов каждый раз при обновлении антивирусных баз* либо по расписанию. Данная проверка выполняется в фоновом режиме и *не оказывает существенного влияния на производительность* почтового сервера.

- *формировать перечень защищаемых хранилищ*, что позволяет гибко соблюдать лицензионные ограничения по числу защищаемых почтовых ящиков.

- *управлять лицензионными ключами*.

Антивирус Касперского 5.5 для Microsoft Exchange Server состоит из следующих компонентов:

- **Сервер безопасности** обеспечивает антивирусную функциональность и обновление антивирусных баз, а также предоставляет административные сервисы для удаленного

управления, настройки, поддержания целостности приложения и хранения информации.

- **Консоль управления** предоставляет пользовательский интерфейс к административным сервисам приложения и позволяет проводить установку приложения, осуществлять настройку и управление серверной частью. Модуль управления выполнен в виде компонента расширения к Microsoft Management Console (MMC).

1.3. Что нового в версии 5.5

Отличия Антивируса Касперского 5.5 для Microsoft Exchange Server от предыдущей версии состоят в следующем:

- Полностью переработанный, удобный для использования графический интерфейс программы выполнен по стандартам Microsoft Management Console (далее **MMC**). Новый интерфейс позволяет администратору начать работу без каких-либо предварительных настроек, а также большие возможности по настройке индивидуальной среды управления приложением, максимально адаптированной к сети конкретного предприятия.

- Использование для проверки объектов расширенного набора антивирусных баз предоставляет возможность защитить почтовый сервер не только от вредоносного программного обеспечения, но и от потенциально опасного программного обеспечения, такого как программы удаленного наблюдения, программы-рекламы, программы автоматического дозвона на платные сайты, программы-взломщики, программы-шутки.

- Реализована возможность выбора уровня антивирусной защиты, что позволяет администратору регулировать уровень безопасности почтового потока и нагрузку сервера при проверке.

- Резервное копирование объектов перед лечением, удалением и переименованием позволяет восстанавливать или отправлять их на исследование специалистам Лаборатории Касперского. Возможность создания и применения пользовательских фильтров упрощает поиск необходимой информации.

- Механизм распознавания вирусных эпидемий и уведомления о них позволяет своевременно реагировать на возникающие нештатные ситуации, своевременно принимать меры по усилению антивирусной защиты почтового сервера.

- Появилась возможность масштабировать приложение в соответствии с числом процессоров компьютера защищаемого сервера. Для

увеличения производительности приложения (увеличения количества одновременно проверяемых объектов) возможен запуск и одновременная работа нескольких экземпляров антивирусного ядра.

- Расширена возможность по проверке объектов в памяти. За счет настройки параметров проверки до 8 объектов объемом до 1 МБ каждый могут проверяться параллельно в оперативной памяти без использования дисковой подсистемы, что существенно повышает производительность.
- Значительно улучшена система ведения журналов. Она предоставляет возможность настраивать полноту фиксируемой в журналах информации и уровень ее детализации. Просмотр журналов организован при помощи стандартного приложения Windows **Просмотр событий**.
- Появилась возможность создания расширенных регулярных отчетов о состоянии антивирусной защиты. Отчеты могут формироваться как в автоматическом режиме, так и по запросу администратора. Система ведения отчетов обеспечивает быстрый, удобный и унифицированный способ доступа к информации при помощи стандартных средств типа Microsoft Internet Explorer. Предусмотрена возможность отправки отчетов по электронной почте.
- Добавлена возможность уведомления пользователей по сети средствами Net Send об обнаружении зараженных и подозрительных объектов и угрозе возникновения вирусной эпидемии.

1.4. Программные требования к системе

Требования к защищаемому серверу Microsoft Exchange 2000 Server Enterprise Edition:

- Microsoft Windows 2000 Server с установленным Service Pack 4 и выше или Microsoft Windows 2000 Advanced Server Service Pack 4 и выше;
- Microsoft Exchange 2000 Server Enterprise Edition с установленным Service Pack 2 и выше.

Требования к защищаемому серверу Microsoft Exchange 2000 Server Standard Edition:

- Microsoft Windows 2000 Server с установленным Service Pack 4 и выше или Microsoft Windows 2000 Advanced Server с установленным Service Pack 4 и выше;

- Microsoft Exchange 2000 Server Standard Edition с установленным Service Pack 2 и выше.

Требования к защищаемому серверу Microsoft Exchange Server 2003 Enterprise Edition:

- Microsoft Windows 2000 Server с установленным Service Pack 4 и выше/ Microsoft Windows 2000 Advanced Server с установленным Service Pack 4 и выше/ Microsoft Windows Server 2003 Standard Edition и выше/ Microsoft Windows Server 2003 Enterprise Edition и выше;
- Microsoft Exchange Server 2003 Enterprise Edition и выше.

Требования к защищаемому серверу Microsoft Exchange Server 2003 Standard Edition:

- Microsoft Windows 2000 Server с установленным Service Pack 4 и выше/ Microsoft Windows 2000 Advanced Server с установленным Service Pack 4 и выше / Microsoft Windows Server 2003 Standard Edition и выше / Microsoft Windows Server 2003 Enterprise Edition и выше;
- Microsoft Exchange Server 2003 Standard Edition и выше.

Требования к компьютеру, с которого будет происходить управление:

- операционная система Microsoft Windows 2000 с установленным Service Pack 4 и выше / Microsoft Windows XP / Microsoft Windows 2003 вместе с MMC версии 1.2 или выше.
- Active Directory Service Interfaces (ADSI) 2.5 или Active Directory Client Extensions (Microsoft Windows 2000 и выше выполняет эти условия автоматически).

1.5. Аппаратные требования к системе

- процессор Intel Pentium 300 МГц или выше;
- около 256 МБ доступной (свободной) оперативной памяти;
- около 20 МБ свободного дискового пространства для установки приложения (без учета объема резервного хранилища и других служебных каталогов).

1.6. 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;
- лицензионный 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. Лицензионный ключ либо включен в дистрибутив, либо отправляется вам по электронной почте по факту оплаты.

1.6.1. 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-диском должен оставаться запечатанным.

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

1.6.2. 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", высылается информация о выходе новых программных продуктов.

1.7. 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.

1.8. 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.
 Примечание.	Дополнительная информация, примечания.
 Внимание!	Информация, на которую следует обратить особое внимание.
 *Чтобы выполнить действие,* 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. СХЕМА РАБОТЫ ПРИЛОЖЕНИЯ

Антивирус Касперского проверяет и, по возможности, лечит всю входящую, исходящую и хранящуюся на сервере почту. Программа проверяет тело сообщения и присоединенные к нему файлы любых форматов.

Поиск вирусов и лечение зараженных объектов выполняются на основании записей *антивирусных баз*, регулярно обновляемых Лабораторией Касперского. Антивирусные базы содержат описание и способы обезвреживания всех известных на настоящее время вредоносных программ, программ-шуток, потенциально опасных программ, а так же программ, которые не являются потенциально опасными, но могут составлять часть программного обеспечения для их разработки. Приложение использует специальный механизм проверки – эвристический анализатор, он позволяет обнаруживать в файлах еще неизвестные вирусы.

Программа проверяет в режиме реального времени все поступающие на сервер новые почтовые сообщения. До тех пор, пока новое сообщение не будет проверено, его просмотр невозможен.

Сообщения, хранящиеся на сервере, а также содержимое общих папок проверяются при каждом обновлении антивирусных баз, либо по расписанию. При проверке могут быть обнаружены новые вирусы, информация о которых отсутствовала в антивирусных базах на момент предыдущих проверок. Данная проверка осуществляется в фоновом режиме и не влияет на производительность сервера. Если пользователь запрашивает сообщение, которое еще не проверено с использованием обновленных антивирусных баз, оно будет проверено перед доставкой. Таким образом, пользователю всегда предоставляются сообщения, проверенные с использованием самой последней версии антивирусных баз, независимо от того, когда это сообщение поступило на сервер.

Каждый объект программа обрабатывает в соответствии с настройкой: лечит или удаляет зараженный объект из сообщения, заменяя соответствующим уведомлением. Администратор также может настроить режим, при котором программа пропускает сообщение с зараженным объектом пользователю, однако меняет название такого объекта, добавляя к нему информацию о вирусе, и меняет расширение объекта.

Перед обработкой программа может сохранять объект в специальном резервном хранилище для последующего восстановления или отправки для исследования специалистам Лаборатории Касперского.

Программа отправляет уведомления о вирусах администратору, получателю, отправителю зараженных сообщений, а также помещает соответствующие записи в журнал приложений Windows и в журналы приложения.

Если включен механизм распознавания вирусных эпидемий, программа фиксирует вирусную активность и отправляет уведомления об угрозе возникновения эпидемии или помещает соответствующие записи в журнал приложений Windows и в журналы приложения.

2.1. Архитектура Сервера безопасности

Серверный компонент приложения – Сервер безопасности, состоит из следующих основных подсистем:

- **Перехватчик почтовых сообщений** осуществляет перехват объектов, поступающих на Microsoft Exchange Server, и направляет в *подсистему антивирусной проверки*. Компонент встраивается в процессы Microsoft Exchange Server по технологии VSAPI 2.0 и 2.5.
- **Подсистема антивирусной проверки** осуществляет антивирусную проверку объектов. Компонент представляет собой несколько процессов, в каждом из которых находится по одному антивирусному ядру. Он также включает в себя хранилище временных объектов для проверки в оперативной памяти. Хранилище представляет собой служебный каталог **Store**. Он создается в каталоге установки приложения и должен быть исключен из проверки, установленным на компьютере Антивирусом Касперского для Windows File Servers или другими антивирусными программами.
- **Модуль внутреннего управления продуктом и контроля целостности** запускается в отдельном процессе и является службой Microsoft Windows. Данная служба запускается автоматически и не зависит от состояния Microsoft Exchange Server (запущен, остановлен), что позволяет настраивать приложение, даже если Microsoft Exchange Server остановлен. Для корректной работы программы **Модуль внутреннего управления** должен быть всегда запущен, не рекомендуется останавливать службу вручную.

2.2. Схема развертывания антивирусной защиты серверов

Для создания системы антивирусной защиты почтовых серверов при помощи Антивируса Касперского 5.5 для Microsoft Exchange Server необходимо:

1. Установить компонент **Сервер безопасности** на все защищаемые Exchange-сервера сети. Установка производится с дистрибутива на каждый сервер отдельно.
2. Установить **Консоль управления** на компьютере, входящем в состав сети предприятия. Консоль управления предоставляет централизованный доступ ко всем ресурсам сети с единого рабочего места администратора, поэтому он может быть установлен только на одном из компьютеров. Однако в случае совместной работы нескольких администраторов Консоль управления может быть установлена на компьютер каждого из них.

В случае если не установлена Консоль управления, приложение будет работать в объеме и с параметрами, предусмотренными по умолчанию (см. п. 4.6 на стр. 40). Антивирусная защита сервера будет включаться автоматически при старте Microsoft Exchange Server, отключаться при завершении его работы.

3. Сформировать список управляемых серверов (см. п. 4.3 на стр. 36).
4. Подключить Консоль управления к серверам (см. п. 4.4 на стр. 38).
5. Для каждого из серверов настроить систему антивирусной защиты:
   - Настроить параметры обновления антивирусных баз (подробную информацию содержит Глава 6 на стр. 64).
   - Проверить правильность настройки параметров и корректность работы Антивируса с помощью тестового "вируса" **EICAR** (см. п. 4.7 на стр. 42).

- Настроить систему уведомления о событиях, регистрируемых в работе приложения (см. Глава 8 на стр. 82).
- Настроить параметры журналов событий и отчетов (см. Глава 10 на стр. 100 и Глава 11 на стр. 114).
- Настроить параметры обнаружения вирусных эпидемий и оповещения об их возникновении (см. Глава 9 на стр. 91).

2.3. Поддержка системы антивирусной защиты

Поддержка созданной системы антивирусной защиты серверов в актуальном состоянии заключается в следующем:

- в регулярном обновлении антивирусных баз;
- в получении и обработке сообщений об обнаружении вирусов и угрозах возникновении эпидемий;
- в регулярной проверке отчетов о работе приложения и состоянии антивирусной защиты почтового сервера;
- в обработке и очистке резервного хранилища.

2.4. Работа приложения на кластере серверов

Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 не поддерживает кластерную технологию в полном объеме, однако корректно функционирует на кластере серверов, воспринимая каждый узел как отдельный физический Exchange-сервер.

Сообщение, поступившее на виртуальный Exchange-сервер, направляется на один из узлов кластера. Почтовые потоки для каждого из узлов могут не пересекаться. Сообщение обрабатывается Антивирусом Касперского на том узле, куда оно было направлено виртуальным Exchange-сервером.

Для каждого узла кластера результаты антивирусной проверки, а следовательно:

- содержание резервного хранилища;
- информация, представленная в отчетах;

- набор событий, зарегистрированных в журналах приложения и журнале Windows;
- значения счетчиков вирусных эпидемий;

будут приводиться только по тем сообщениям, которые были переданы виртуальным Exchange-сервером на этот узел кластера.

Для создания антивирусной защиты Microsoft Exchange Server, установленного на кластере серверов, следует:

1. Установить компонент **Сервер безопасности** на **каждый узел** кластера. Установка производится с дистрибутива на каждый сервер отдельно.

   В качестве каталога установки следует указать каталог на **локальном** диске файловой системы сервера.
   Не следует использовать **разделяемый** диск, поскольку при перемещении приложения Microsoft Exchange Server на другой узел кластера, разделяемый диск перемещается вместе с ним.

2. Установить **Консоль управления** на компьютере, входящем в состав сети предприятия.
3. Сформировать список управляемых серверов, добавив в качестве серверов **все** узлы кластера (см. п. 4.3 на стр. 36).

   При добавлении управляемых серверов и настройке подключения Консоли управления к Серверу используйте имена **физических** серверов, на которых установлен компонент Сервер безопасности.
   Использование имени **виртуального** Exchange-сервера может привести к ошибке адресации при перемещении приложения Microsoft Exchange Server на другой узел кластера.

4. Подключить Консоль управления к серверам (см. п. 4.4 на стр. 38).
5. Для каждого из серверов настроить систему антивирусной защиты с **идентичными** значениями параметров, учитывая следующие особенности:

   - В качестве каталога резервного хранилища должен быть выбран каталог на физическом сервере, где установлен компонент Сервер безопасности (см. п. 7.6 на стр. 79).
   - В качестве каталогов размещения отчетов и журналов должны быть выбраны каталоги на физическом сервере,

где установлен компонент Сервер безопасности (см. п. 10.1.1 на стр. 104 и п. 11.2 на стр. 117).

- Списки незащищаемых хранилищ на всех серверах должны совпадать (см. п. 12.6 на стр. 126).

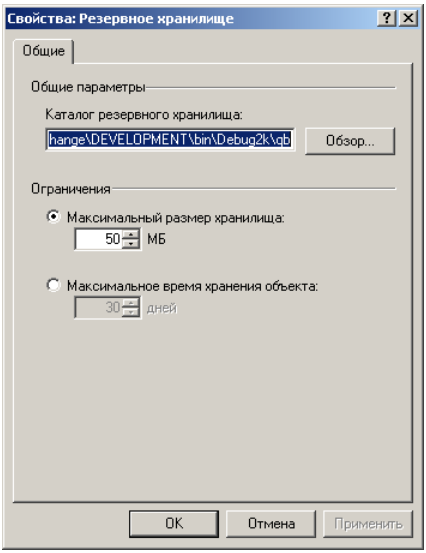


Рисунок 1. Настройка параметров резервного хранилища

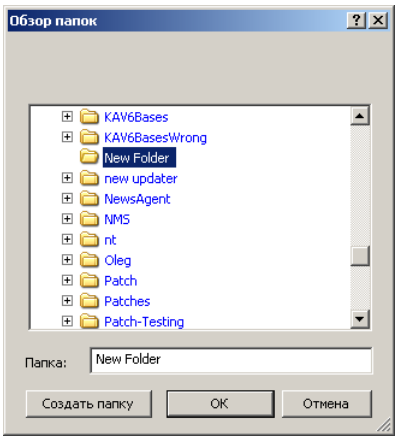


Рисунок 2. Смена каталога резервного хранилища

ГЛАВА 3. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ ПРИЛОЖЕНИЯ

Перед тем как начинать установку Антивируса Касперского, необходимо убедиться в том, что аппаратное и программное обеспечение компьютеров соответствует предъявляемым к ним требованиям. Минимально допустимая конфигурация указана в разделах 1.4 на стр. 12 и 1.5 на стр. 13.

3.1. Установка приложения

Процедура установки выполняется стандартно, как для большинства приложений Windows. Программа установки предложит установить на компьютер, где она запущена, программные компоненты приложения Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 – Сервер безопасности и Консоль управления. Такая конфигурация рекомендуется в начале создания системы защиты Exchange-серверов. Можно выбрать как полную, так и выборочную установку приложения, а также восстановить некорректную установку Антивируса Касперского.

Для установки Антивируса Касперского 5.5 для Microsoft Exchange Server 2000/2003 необходимо наличие прав локального администратора на компьютере, где осуществляется установка.

В результате установки Консоли управления на компьютере в меню **Пуск / Программы / Антивирус Касперского для Microsoft Exchange Server** появится значок для ее запуска.

Сервер безопасности будет установлен на компьютере в качестве службы со следующим набором атрибутов:

- имя – **Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003**;
- тип запуска – **автоматический**;
- учетная запись – **Локальная система**.

Просмотр свойств Сервера безопасности и наблюдение за его работой осуществляется при помощи стандартных средств администрирования Windows – **Управление компьютером** / **Службы**. Информация о работе

Сервера безопасности фиксируется и сохраняется в журнале приложений Windows на компьютере, где установлен Сервер безопасности.

3.1.1. Первая установка

Чтобы установить Антивирус Касперского на компьютер, на дистрибутивном CD-диске приложения запустите файл *setup.exe*. Установка сопровождается мастером. Он предложит провести настройку параметров установки и запустить ее. 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 установленных операционной и почтовой систем, а также Пакетов обновлений (Service Packs) программным требованиям для установки Антивируса Касперского.

В случае если на компьютере не установлен Microsoft Exchange Server или его версия не соответствует программным требованиям, вы сможете установить только один из компонентов приложения – Консоль управления. Установите Microsoft Exchange Server, соответствующий программным требованиям, после этого повторите установку Антивируса Касперского.

Если какой-либо из требуемых Пакетов обновлений для операционной или почтовой системы не установлен, проведите обновление, после чего повторите установку Антивируса Касперского.

Шаг 2. Поиск других антивирусных программ

На следующем этапе осуществляется поиск других установленных антивирусных продуктов для Microsoft Exchange Server, совместное использование с которыми Антивируса Касперского 5.5 для Microsoft Exchange Server 2000/2003 может привести к возникновению конфликтов.

При обнаружении в системном реестре некорректной регистрации антивирусного продукта для Microsoft Exchange Server, программа установки выводит предупреждающее сообщение с предложением удалить обнаруженную регистрацию.

Для продолжения установки Антивируса Касперского согласитесь с удалением некорректной регистрации.

При обнаружении на компьютере установленного антивирусного программного обеспечения для Microsoft Exchange Server другого производителя на экран будет выведено сообщение о необходимости удалить его, прежде чем устанавливать Антивирус Касперского.

Удалите указанную программу, после чего снова запустите файл *setup.exe* с дистрибутивного CD-диска приложения.

При обнаружении установленного на компьютере Антивируса Касперского для Microsoft Exchange Server более ранних версий (например, версии 4.5) на экран будет выведено сообщение, требующее удаления данного программного обеспечения, поскольку его совместное использование с Антивирусом Касперского 5.5 для Microsoft Exchange Server 2000/2003 невозможно.

Перед удалением предыдущей версии программы (Антивирус Касперского для Microsoft Exchange Server 4.5) рекомендуем сохранить используемый ранее действующий лицензионный ключ. Вы сможете использовать его в качестве ключа для Антивируса Касперского 5.5 для Microsoft Exchange Server 2000/2003.

Удалите более раннюю версию Антивируса, после чего снова запустите файл *setup.exe* с дистрибутивного компакт-диска.

При обнаружении на компьютере уже установленного Антивируса Касперского 5.5 для Microsoft Exchange Server 2000/2003 будет предложено изменить, восстановить или удалить данную копию программы.

Шаг 3. Приветствие и Лицензионное соглашение

Первые шаги установки традиционны и состоят в распаковке с дистрибутива необходимых файлов и записи их на жесткий диск компьютера. После этого открываются окно приветствия и окно, содержащее лицензионное соглашение. Внимательно прочтите текст лицензионного соглашения и примите его условия для продолжения установки.

Шаг 4. Выбор типа установки

На следующем этапе (см. рис. 3) определите тип установки: полная или выборочная.

Если компьютер, с которого осуществляется установка, является защищаемым Exchange-сервером и с него планируется управлять работой приложения, выберите полную установку. В этом случае будут установлены оба компонента приложения – Сервер безопасности и Консоль управления. Установка производится в каталог, предусмотренный по умолчанию (**Program files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server**).

Если вы хотите установить только один из компонентов приложения (Сервер безопасности или Консоль управления), либо изменить каталог установки компонентов, предусмотренный по умолчанию, воспользуйтесь выборочным типом установки.

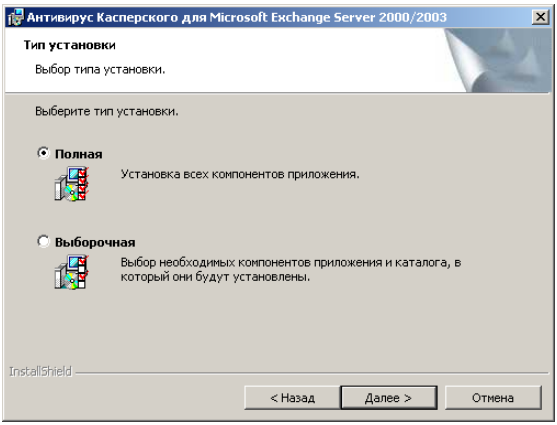


Рисунок 3. Выбор типа установки

Шаг 5. Выбор компонентов приложения для установки

Если вы используете выборочный тип установки, на следующем этапе (см. рис. 4) укажите какие компоненты приложения должны быть установлены на компьютер. Вы также можете изменить каталог для их установки, предусмотренный по умолчанию.

Если компьютер, с которого осуществляется установка, является защищаемым Exchange-сервером, выберите компонент **Сервер безопасности**.

Если компьютер является рабочим местом администратора и с него планируется управлять антивирусной защитой Exchange-серверов, выберите **Консоль управления**.

Обратите внимание, что в окне мастера приводится справочная информация о выбранном компоненте и необходимом для его установке объеме дискового пространства.

По умолчанию компоненты приложения будут установлены в каталог **Program files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server**. Если такого каталога нет, он будет создан автоматически. Смена каталога осуществляется при помощи кнопки **Обзор**.

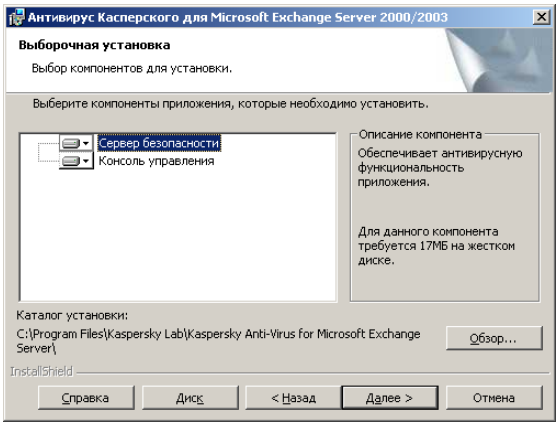


Рисунок 4. Выбор компонентов для установки

Шаг 6. Запуск установки

По окончании настройки параметров запустите установку. Для этого в окне мастера нажмите на кнопку **Установить**. После чего начнется процесс копирования файлов приложения на компьютер.

После завершения копирования вам будет предложено включить антивирусную защиту сервера автоматически сразу после завершения работы мастера (см. рис. 5), либо сделать это позже вручную, через Консоль управления Антивирусом (см. п. 5.2 на стр. 49).

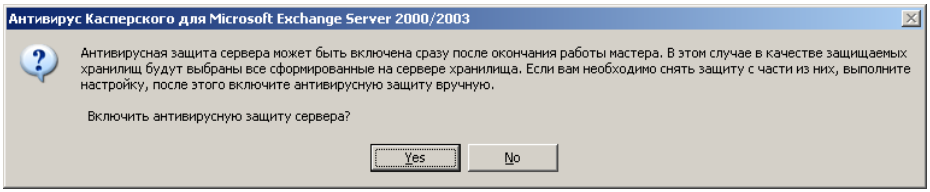


Рисунок 5. Запрос на включение антивирусной защиты

Если работа приложения в объеме и с параметрами, предусмотренными по умолчанию (см. п. 4.6 на стр. 40), подходит для вашего сервера, мы рекомендуем согласиться с автоматическим запуском антивирусной защиты после завершения работы мастера установки. Для этого нажмите на кнопку **Да**.

Следует помнить, что по умолчанию в качестве защищаемых хранилищ будут выбраны все сформированные на сервере хранилища. Если в приобретенной вами лицензии указано максимальное количество защищаемых почтовых ящиков меньшее, чем сформировано в хранилищах

сервера, перед запуском антивирусной защиты необходимо снять защиту с части из них (см. п. 12.6 на стр. 126).

Для предварительной настройки приложения, откажитесь от автоматического включения Антивирусной защиты, нажмите на кнопку **Нет**.

Шаг 7. Завершение установки

По окончании установки в заключительном окне мастера нажмите на кнопку **Готово**.

При установке компонента Сервер безопасности вам будет предложено провести установку лицензионного ключа (см. рис. 6) к приложению Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003. Вы можете установить лицензионный ключ позже через Консоль управления, однако без лицензионного ключа антивирусная функциональность приложения будет недоступна, возможен запуск только Консоли управления.

Шаг 8. Установка лицензионного ключа

На этом шаге установки приложения выполняется инсталляция лицензионного ключа Антивируса Касперского для Microsoft Exchange Server. Лицензионный ключ является вашим личным "ключом", в котором находится служебная информация, необходимая для полнофункциональной работы приложения, а именно:

- информация о поддержке (кто осуществляет и где можно ее получить);
- ограничение по количеству почтовых ящиков;
- название и номер лицензии, а также дата ее истечения.

В открывшемся окне **Установленные лицензионные ключи** (см. рис. 6) нажмите на кнопку **Добавить**. В стандартном окне выбора файлов укажите файл ключа, который необходимо установить (*.key). В результате указанный лицензионный ключ будет установлен в качестве текущего лицензионного ключа для Антивируса Касперского.

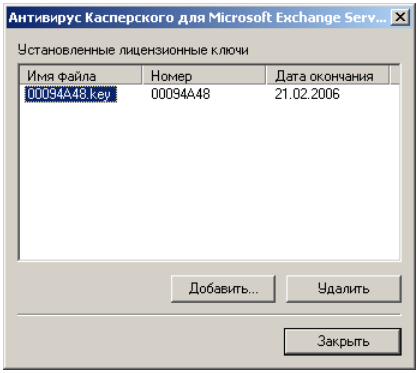


Рисунок 6. Установка лицензионного ключа

Если на компьютере был установлен Антивирус Касперского версии 4.5 и срок действия лицензионного ключа еще не закончился, вы можете использовать данный ключ в качестве лицензионного ключа к Антивирусу Касперского 5.5 для Microsoft Exchange Server 2000/2003.

Вы можете также установить резервный лицензионный ключ, который будет активирован автоматически по окончании срока действия текущего лицензионного ключа.

В случае если на момент установки приложения у вас нет лицензионного ключа (например, вы заказали его в Лаборатории Касперского через интернет, но еще не получили), вы сможете установить его позже, при первом запуске программы через Консоль управления. Помните, что без ключа вы не сможете приступить к работе с Антивирусом Касперского.

3.1.2. Повторная установка

Повторная установка Антивируса Касперского выполняется, если первая установка приложения прошла некорректно, либо при работе приложения целостность исполняемых файлов была нарушена.

*Для повторной установки приложения в открывшемся окне (см. рис. 7) выберите вариант **Исправить**.*

В этом случае будет осуществлен повтор предыдущей установки Антивируса Касперского. Так, если предыдущая установка была выборочной, то и повторная установка в режиме **Исправить** также будет выполняться выборочно.

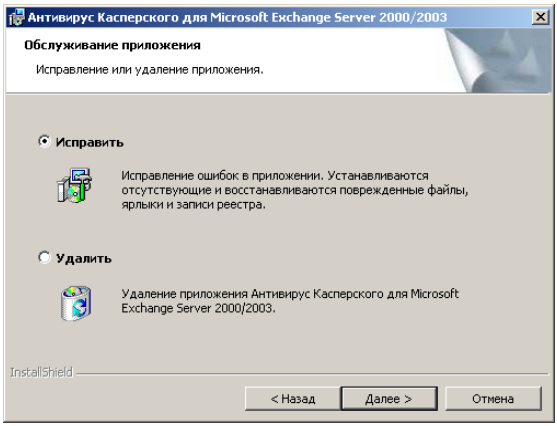


Рисунок 7. Выбор режима повторной установки приложения

3.2. Обновление версии приложения

Для обновления версии 4.x Антивируса Касперского для Microsoft Exchange Server до версии 5.5 необходимо удалить предыдущую версию и установить новую, согласно описаниям, приведенным в данном Руководстве (подробнее см. п. 3.1 на стр. 23 и п. 3.3 на стр. 31).

РЕКОМЕНДАЦИИ ПО ПЕРЕХОДУ С ВЕРСИИ 4.5 НА ВЕРСИЮ 5.5

После установки версия 5.5 начинает работать с минимальным набором параметров, основная часть которых устанавливается по умолчанию и является оптимальной, рекомендуемой специалистами Лаборатории Касперского (см. п. 4.6 на стр. 40).

Дополнительная настройка проводится вручную. Для восстановления конфигурации системы в соответствие с версией 4.5 следует внести необходимые изменения. При этом следует обратить внимание на следующее:

- Проверка архивов в версии 5.5 по умолчанию отключена. Включить проверку архивов можно на закладке **Проверка вложений** в окне **Антивирусная защита** (см. п. 5.3 на стр. 51).
- В версии 5.5 не предусмотрена группа незащищаемых пользователей. Исключение из проверки осуществляется через незащищаемые хранилища. Настройка защиты хранилищ

осуществляется на закладке **Защищаемая почта** в окне **Антивирусная защита** (см. п. 12.6 на стр. 126).

- В версии 5.5 по умолчанию уведомления не записываются в журналы событий. Настройка регистрацию уведомлений в журналах событий можно на закладке **Действия** в окне настройки параметров уведомления **Свойства: <Имя уведомления>** (см. п. 8.1 на стр. 84).
- При настройке параметров уведомлений необходимо указывать только адреса получателей. Адрес SMTP-сервера указывать не нужно, так как SMTP в версии 5.5 для рассылки уведомлений не используется. Настройка параметров оповещения осуществляется на закладке **Действия** в окне настройки параметров уведомления **Свойства: <Имя уведомления>** (см. п. 8.1 на стр. 84).

3.3. Удаление приложения

Удаление Антивируса Касперского для Microsoft Exchange Server 2000/2003 вы можете провести стандартными средствами установки и удаления программ **Windows**, либо с использованием дистрибутива приложения. При этом с компьютера будут удалены все установленные компоненты Антивируса Касперского, как Сервер безопасности, так и Консоль управления.

Для удаления Антивируса Касперского для Microsoft Exchange Server 2000/2003 с использованием дистрибутива

1. Запустите файл *setup.exe* с дистрибутивного компакт-диска. Удаление сопровождается мастером обслуживания приложения. Следуйте его указаниям.
2. В открывшемся окне (см. рис. 8) выберите вариант удаления приложения.
3. В процессе подготовки к удалению приложения выводится запрос на остановку службы Microsoft Exchange Information Store (см. рис. 9). Согласитесь с ее остановкой.

Исходное состояние службы восстанавливается программой установки после завершения выполняемой процедуры.

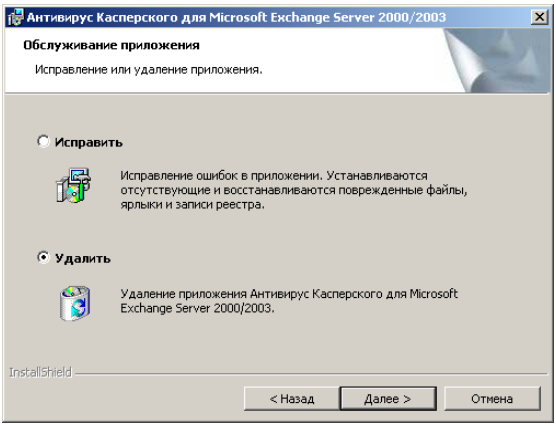


Рисунок 8. Выбор режима удаления приложения

При удалении приложения средствами установки и удаления программ **Windows**, также выводится запрос на остановку службы Microsoft Exchange Information Store (см. рис. 9). Согласитесь с ее остановкой.

Рисунок 9. Остановка службы Microsoft Exchange Information Store

ГЛАВА 4. НАЧАЛО РАБОТЫ

4.1. Запуск программы

Запуск серверной части приложения осуществляется автоматически при старте операционной системы. Если антивирусная защита сервера включена (см. п. 5.1 на стр. 47), она начинает работать сразу после запуска приложения Microsoft Exchange Server.

Управление работой Антивируса Касперского осуществляется с рабочего места администратора – компьютера, на котором установлен компонент Консоль управления.

Для запуска Консоли управления

выберите пункт **Консоль управления** в программной группе **Антивирус Касперского для Microsoft Exchange Server** стандартного меню **Пуск \ Программы**. Данная программная группа создается только на рабочих местах администраторов при установке компонента Консоль управления.

4.2. Интерфейс программы

Интерфейс управления Антивирусом Касперского обеспечивает компонент Консоль управления. Она представляет собой специализированную изолированную оснастку, интегрированную в MMC, в связи с этим интерфейс программы является стандартным для MMC.

4.2.1. Главное окно программы

Главное окно программы (см. рис. 10) содержит меню, панель инструментов, панель обзора и панель результатов. Меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе. Набор кнопок панели инструментов обеспечивает прямой доступ к некоторым наиболее популярным пунктам главного меню. Панель обзора отображает в виде дерева консоли пространство имен **Антивирус Касперского для Microsoft Exchange Server**, панель результата – список элементов выбранного в дереве объекта.

Пространство имен **Антивирус Касперского для Microsoft Exchange Server** может содержать несколько узлов с именами серверов, управляемых через консоль. Сразу после установки Консоли управления пространство имен не содержит никаких элементов.

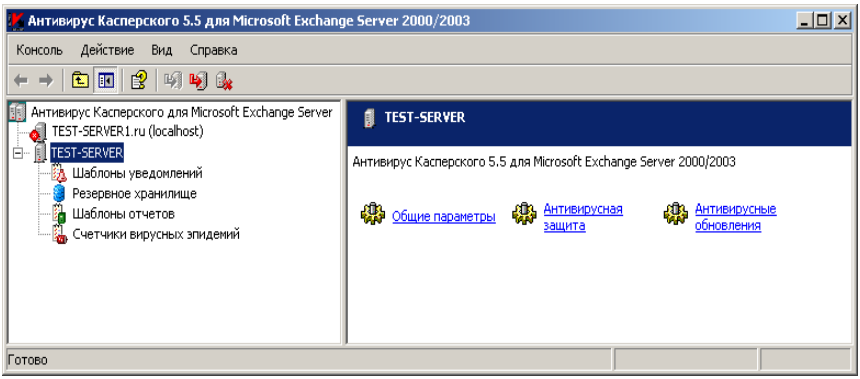


Рисунок 10. Главное окно программы

После добавления нового сервера он отображается в дереве консоли в виде узла **<Имя сервера>**. Настройка параметров и управление работой Антивируса Касперского осуществляется при помощи распложенных в панели результата гиперссылок:

- Общие параметры – просмотр общих параметров работы Антивируса Касперского, информации о лицензии и установленных лицензионных ключах, продление срока действия лицензии, а также настройка параметров диагностики работы приложения.
- Антивирусная защита – просмотр и настройка параметров антивирусной защиты управляемого сервера.
- Антивирусные обновления – настройка параметров получения обновлений антивирусных баз, обновление вручную, а также составление расписания автоматического обновления.

Если соединение с сервером установлено, в состав узла **<Имя сервера>** входят вложенные папки, каждая из которых предназначена для управления конкретной функциональностью приложения:

- **Шаблоны уведомлений**: для настройки оповещения об обнаруженных в результате антивирусной проверки зараженных и подозрительных объектах.
- **Резервное хранилище**: для работы с хранилищем резервных копий объектов; содержит список, размещенных в данном хранилище объектов.

- **Шаблоны отчетов**: для работы с отчетами; содержит список шаблонов отчетов о работе приложения и состоянии системы антивирусной защиты сервера, на основании которых формируются отчеты.
- **Счетчики вирусных эпидемий**: для настройки критериев выявления вирусных эпидемий и параметров оповещения об их возникновении.

4.2.2. Контекстное меню

В дереве консоли каждая категория объектов имеет свое контекстное меню. В нем к стандартным командам контекстного меню MMC добавлены команды, при помощи которых осуществляется работа с данным объектом. Перечень объектов и соответствующий им дополнительный набор возможных команд контекстного меню приводится в таблице.

Объект	Команда	Назначение команды
Антивирус Касперского для Microsoft Exchange Server	**Добавить сервер**	Добавить новый Exchange-сервер с установленным Сервером безопасности для управления через консоль.
<Имя сервера>	**Отключиться от сервера**	Разорвать соединение Консоли управления с установленным на данном Exchange-сервере Сервером безопасности.
	Подключиться к серверу	Установить соединение Консоли управления с установленным на данном Exchange-сервере Сервером безопасности.
	Удалить сервер из дерева консоли	Удалить Exchange-сервер из числа серверов, на которых управление работой Сервера безопасности осуществляется через консоль.
Шаблоны уведомлений	**Новый шаблон уведомлений**	Создание и настройка параметров нового шаблона уведомления об обнаруженных в результате антивирусной проверки зараженных и подозрительных объектах.

Объект	Команда	Назначение команды
Резервное хранилище	**Новый фильтр**	Создание и настройка параметров нового фильтра для поиска объектов, размещенных в хранилище резервных копий.
Шаблоны отчетов	**Новый шаблон отчетов**	Создание нового шаблона отчета.
Счетчики вирусных эпидемий	**Новый счетчик**	Создание и настройка нового критерия выявления вирусной эпидемии и параметров уведомления о ней.

Дополнительные команды контекстного меню предусмотрены также для шаблонов отчета и объектов хранилища резервных копий.

При помощи команды **Сформировать отчет** создается отчет по выбранному шаблону.

Команда **Получить файл** позволяет получать исходную копию объекта, сохраненную перед его обработкой антивирусом; **Отправить на исследование** – отправлять объект из резервного хранилища на исследование специалистам Лаборатории Касперского.

4.3. Создание списка управляемых серверов

Для того чтобы управлять Антивирусом Касперского через консоль, необходимо добавить Exchange-сервер, на котором установлен компонент Сервер безопасности, в список управляемых серверов. Вы можете добавить как локальный компьютер, так и любой Exchange-сервер из числа установленных в сети. При добавлении сервера может также сразу устанавливаться соединение Консоли управления с Антивирусом Касперского.

Чтобы добавить сервер в список управляемых серверов,

1. Выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, откройте контекстное меню и выберите команду **Добавить сервер** или воспользуйтесь

аналогичным пунктом в меню **Действие**. В результате откроется окно **Добавление сервера** (см. рис. 11).

2. Укажите компьютер, на котором установлен компонент Сервер безопасности. Если серверный компонент установлен на том же компьютере, что и Консоль управления, выберите **Локальный компьютер**. Для добавления Exchange-сервера из числа установленных в сети выберите **Удаленный компьютер** и укажите его имя в поле ввода. Вы можете ввести имя вручную: указать IP-адрес, полное доменное имя (FQDN в формате **<Имя компьютера>.<DNS-имя домена>**) или имя компьютера в сети Microsoft Windows (NetBIOS-имя), либо выбрать компьютер из списка при помощи кнопки **Обзор**.

В дальнейшем при подключении Консоли управления к Серверу безопасности программа будет устанавливать соединение с компьютером по заданному имени. Соединение производится с использованием DCOM-протокола.

Для того чтобы при добавлении сервера было сразу же установлено соединение Консоли управления с Антивирусом Касперского, установите флажок **Подключится сейчас** (подробнее см. п. 4.4 на стр. 38).

На выбранном сервере обязательно должен быть установлен серверный компонент Сервер безопасности.

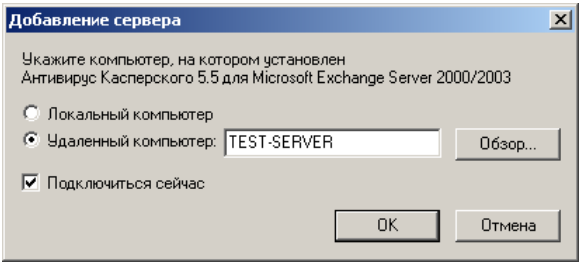


Рисунок 11. Диалоговое окно **Добавление сервера**

В результате выбранный вами сервер появляется в дереве консоли в виде узла **<Имя сервера>**. Локальный компьютер отображается под именем **<Имя сервера>(localhost)**. Если соединение с сервером успешно установлено, он будет сопровождаться значком  , и в состав узла будут входить вложенные папки **Шаблоны уведомлений**, **Резервное хранилище**, **Шаблоны отчетов** и **Счетчики вирусных эпидемий**. Если соединение не устанавливалось или не удалось установить, сервер будет

отмечен значком  . Подключиться к нему вы можете вручную (см. п. 4.4 на стр. 38).

Чтобы удалить сервер из списка управляемых серверов,

в дереве консоли выберите узел, соответствующий удаляемому серверу, раскройте контекстное меню и выберите команду **Удалить сервер из дерева консоли** или воспользуйтесь аналогичным пунктом в меню **Действие**.

В результате выбранный вами узел удаляется из дерева консоли.

4.4. Подключение Консоли управления к серверу

Для настройки и управления работой Антивируса Касперского 5.5 для Microsoft Exchange Server через консоль необходимо подключиться к установленному на сервере компоненту Сервер безопасности. Программа получает информацию с сервера и отображает ее в дереве консоли.

Для подключения к Серверу безопасности

выберите в дереве консоли узел, соответствующий нужному серверу, раскройте контекстное меню и выберите команду **Подключиться к серверу** или воспользуйтесь аналогичным пунктом в меню **Действие**.

Если соединение с сервером успешно установлено, в главном окне программы загружается отображение его параметров: узел сопровождается значком  , и в его состав входят вложенные папки **Шаблоны уведомлений**, **Резервное хранилище**, **Шаблоны отчетов** и **Счетчики вирусных эпидемий**.

Если подключиться к серверу не удалось, выводится предупреждающее сообщение (см. рис. 12) с указанием причины и предложением подключиться при следующем запуске Консоли управления. Выберите нужный вариант.

Для подключения к Серверу безопасности необходимо, чтобы пользователь обладал правами локального администратора на компьютере, к которому производится подключение.
Проверка прав осуществляется на основании Windows-аутентификации пользователя в сети.

К одному и тому же Серверу безопасности может быть подключено несколько Консолей управления. В этом случае, при параллельной работе с сервером с разных консолей необходимо регулярно обновлять информацию, представленную в каждой них. Для этого следует воспользоваться командой **Обновить** контекстного меню или аналогичным пунктом в меню **Действие**.

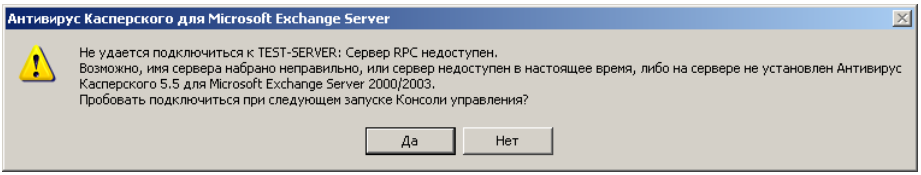


Рисунок 12. Ошибка подключения Консоли к Серверу

4.5. Минимально-необходимая настройка

После установки Антивирус Касперского начинает работать с минимальным набором параметров, основная часть которых устанавливается по умолчанию и является оптимальной, рекомендуемой специалистами Лаборатории Касперского. В случае необходимости вы можете внести нужные изменения и дополнения с учетом особенностей сети и характеристик компьютера, на котором установлен Microsoft Exchange Server.

Если подключение к интернету осуществляется через прокси-сервер, для успешного получения обновлений следует настроить параметры соединения.

Для функционирования защиты почтового сервера в полном объеме необходимо провести настройку параметров оповещения администратора или других пользователей об обнаружении зараженных и подозрительных объектов и возникновении угрозы вирусной эпидемии.

Настройка приложения производится с рабочего места администратора – компьютера, на котором установлен компонент Консоль управления. Операция может проводиться независимо от того, запущена программа Microsoft Exchange Server на сервере или нет.

4.6. Защита почтового сервера без дополнительной настройки

Антивирусная защита Exchange-сервера начинает работать сразу после установки компонента Сервер безопасности. По умолчанию предусмотрен следующий режим работы приложения:

- Антивирус выполняет проверку объектов на наличие всех известных в настоящее время вредоносных программ (установлен стандартный уровень антивирусной защиты).
- Антивирусной защите подлежат общие папки, все сформированные на Exchange-сервере хранилища и все зарегистрированные на данном почтовом сервере пользователи.
- Осуществляется антивирусная проверка всех поступающих на Exchange-сервер новых почтовых сообщений со следующими параметрами:
    - проверяется тело письма и вложенные в него объекты любых форматов, за исключением архивов и объектов-контейнеров выше 32-го уровня вложенности;
    - максимальное время проверки одного объекта составляет 180 секунд;
    - при обнаружении зараженного объекта приложение сохраняет исходную копию объекта (вложение или тело письма) в резервном хранилище, выполняет попытку лечения, если лечение невозможно, удаляет объект и заменяет текстовым файлом с информационным сообщением следующего формата:

      ```
      Обнаружен вредоносный объект %VIRUS_NAME%. Файл
      (%OBJECT_NAME%) удален Антивирусом Касперского.
      ```

      В случае обнаружения неизлечимого объекта в теле письма, оно заменяется аналогичным сообщением.
    - при обнаружении подозрительного объекта приложение сохраняет исходную копию объекта (файл или тело письма) в резервном хранилище.

      Обнаруженные в теле письма подозрительные объекты заменяются информационным сообщением следующего формата:

```
Обнаружен подозрительный объект (возможно %VI-
RUS_NAME%). Файл (%OBJECT_NAME%) удален
Антивирусом Касперского.
```

В случае обнаружения подозрительного объекта во вложенном файле приложение изменяет название и расширение вложенных объектов. Переименованные файлы будут иметь расширение *txt.*

- при обнаружении защищенного или поврежденного объекта приложение сохраняет исходную копию объекта (файл или тело письма) в резервном хранилище.

  Обнаруженные в теле письма объекты заменяются информационным сообщением следующего формата:

  ```
  Вложенный файл %OBJECT_NAME% удален Антивирусом
  Касперского. Файл был защищен паролем или
  поврежден.
  ```

  В случае обнаружения защищенного или поврежденного объекта во вложенном файле приложение изменяет название и расширение вложенных объектов. Переименованные файлы будут иметь расширение *txt.*

- Сообщения, хранящиеся на сервере, а также содержимое общих папок не проверяются.
- Не проверяется маршрутизируемый Exchange-сервером почтовый поток.
- Обновление антивирусных баз проводится каждый час через интернет с HTTP- и FTP-серверов обновлений Лаборатории Касперского.
- Уведомление администратора об обнаруженных зараженных и подозрительных объектах не производится.
- Фиксируется возникновение вирусной эпидемии: обнаружение зараженных объектов с частотой пять раз в день. Уведомление администратора не производится.
- Отчет о состоянии системы антивирусной защиты создается первого числа каждого месяца за последние 30 дней.

4.7. Проверка работоспособности приложения

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

4.7.1. Тестовый "вирус" EICAR и его модификации

Тестовый "вирус" был специально разработан организацией eicar (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 отсутствии доступа к интернету вы можете самостоятельно создать тестовый "вирус". Для этого в любом текстовом редакторе наберите следующую строку, а затем сохраните в файле с именем **eicar.com**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Файл, который вы загрузили с сайта компании **EICAR** или создали в текстовом редакторе описанным выше способом, содержит тело стандартного тестового "вируса". Антивирус Касперского обнаруживает его, присваивает тип **Зараженный** и выполняет действие, установленное администратором для объекта с таким типом.

Для того чтобы проверить реакцию Антивируса Касперского при обнаружении объектов других типов, вы можете модифицировать содержание стандартного тестового "вируса", добавив к нему один из префиксов (см. таблицу).

Вы можете проверять корректность работы Антивируса Касперского с помощью модифицированного "вируса" EICAR только при наличии антивирусных баз, датированных не ранее 24.10.2003 (кумулятивное обновление – Октябрь, 2003).

Префикс	Тип объекта
Префикс отсутствует, стандартный тестовый "вирус"	**Зараженный**. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR–	**Поврежденный**.
SUSP–	**Подозрительный** (код неизвестного вируса).
WARN–	**Подозрительный** (модифицированный код известного вируса).
ERRO–	**Не проверенный** из-за сбоя.
CURE–	**Зараженный** (излечимый). Объект подвергается лечению, при этом текст тела "вируса" изменяется на CURED.
DELE–	**Зараженный** (неизлечимый). К объекту применяется действие, установленное для неизлечимых объектов.

В первом столбце таблицы приведены префиксы, которые нужно добавить в начало строки стандартного тестового "вируса" (например, `DELE-X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`).

После добавления префикса к тестовому "вирусу" сохраните его в файл с именем, например, *eicar_dele.com* (аналогично дайте названия всем модифицированным "вирусам").

Во втором столбце описаны типы объектов, идентифицируемые антивирусной программой в результате добавления префиксов. Действия над каждым из объектов определяются значениями параметров антивирусной проверки, установленными администратором.

4.7.2. Тестирование работы приложения

После установки приложения рекомендуется произвести проверку работы Антивируса Касперского для входящей и исходящей почты, как в теле сообщения, так и во вложении.

Для проверки обнаружения вирусов в теле сообщения

1. Создайте письмо в формате **Обычный текст** с помощью установленного на компьютере почтового клиента.

   Письмо, содержащее тестовый вирус и сформированное в формате RTF и HTML, проверено не будет!

2. Поместите текст стандартного или модифицированного "вируса" в начало письма.
3. Отправите письмо на адрес администратора.
4. Ознакомьтесь с содержанием письма, поступившим на указанный адрес.

ГЛАВА 5. АНТИВИРУСНАЯ ЗАЩИТА

Главной задачей Антивируса Касперского является проверка почтового трафика и лечение зараженных почтовых сообщений с использованием информации текущей (последней) версии антивирусных баз.

В зависимости от установленного администратором уровня антивирусной защиты (см. п. 5.1 на стр. 47), приложение позволяет обнаружить:

- вредоносные объекты;
- потенциально опасные объекты;
- объекты, которые не являются потенциально опасными, но могут составлять часть программного обеспечения для их разработки.

Все поступающие на Exchange-сервер почтовые сообщения проверяются в режиме реального времени. Обрабатывается входящий и исходящий трафик, также может проверяться перенаправляемый Exchange-сервером поток. В целях уменьшения нагрузки на сервер вы можете отключать проверку транзитной почты (подробнее см. п. 5.3 на стр. 51).

В режиме проверки трафика приложение постоянно находится в оперативной памяти компьютера, при этом **Перехватчик почтовых сообщений** анализирует поступающий от Exchange-сервера почтовый поток и передает на обработку **Подсистеме антивирусной проверки**. **Подсистема антивирусной проверки** обрабатывает сообщение и в соответствии с настройкой:

- выполняет проверку объекта с помощью антивирусных баз;
- если почтовое сообщение или его часть заражены, программа обрабатывает обнаруженный объект в соответствии с настройками (подробнее см. п. 5.4 на стр. 55);
- перед обработкой копия объекта может быть сохранена в резервном хранилище.

Если антивирусная защита сервера включена (подробнее см. п. 5.2 на стр. 49), запуск и остановка проверки трафика происходит вместе с запуском и остановкой Microsoft Exchange Server.

При работе с Microsoft Exchange Server **2000** проверка входящей почты осуществляется при любом используемом почтовом клиенте и любом почтовом протоколе. Исходящие сообщения проверяются только в случае, когда для отправки почты используется клиент, совместимый с Microsoft Exchange Server (например, Microsoft Outlook) и протокол MAPI. Во всех остальных случаях исходящие сообщения не проверяются, так как они не попадают в хранилище на защищаемом сервере.

Антивирус Касперского не проверяет сообщения, создаваемые защищенными пользователями в **Общих папках** незащиненных Exchange-серверов.

Хранящиеся на сервере сообщения и содержимое общих папок также регулярно перепроверяются с использованием последней версии антивирусных баз. Проверка осуществляется в фоновом режиме и может запускаться как автоматически при обновлении антивирусных баз или по расписанию, так и вручную (подробнее см. п. 5.6 на стр. 62).

В случае работы приложения на кластере серверов, если фоновая проверка включена, она может запуститься при перемещении приложения Microsoft Exchange Server с одного узла кластера на другой.

Если фоновая проверка отключена, хранящиеся на сервере сообщения проверяются только при запросе их пользователем непосредственно перед доставкой.

Работа приложения в режиме фоновой проверки может вызвать некоторое замедление работы Microsoft Exchange Server, поэтому не рекомендуется использовать данный вид защиты постоянно.

В режиме фоновой проверки **Модуль внутреннего управления приложением** в соответствии с настройками получает от Exchange-сервера все почтовые сообщения, размещенные в общих папках и защищаемых хранилищах. Если сообщение не было проверено с использованием последней версии антивирусных баз, программа передает его на обработку **Подсистеме антивирусной проверки**. Обработка объектов в фоновом режиме проводится так же, как и в режиме проверки трафика.

Программа проверяет тело сообщения и присоединенные к нему файлы любых форматов.

Следует отметить, что Антивирус Касперского различает объект простой (тело письма, простое вложение, например, в виде исполняемого файла) и объект-контейнер (состоящий из нескольких объектов, например, архив, письмо с любым вложенным письмом).

Приложение не находит вирусы в многотомных архивах. Многотомные архивы могут быть проверены после сохранения на диске, например, установленным на компьютере Антивирусом Касперского для Windows File Servers.

В случае необходимости вы можете определять перечень объектов, не подлежащих антивирусной проверке. Из проверки могут исключаться: архивы, все объекты-контейнеры выше заданного уровня вложенности, файлы по маскам и файлы по типам (см. п. 5.3 на стр. 51).

Антивирус Касперского позволяет одновременно проверять несколько объектов. Число параллельно обрабатываемых объектов зависит от количества запущенных и параллельно работающих экземпляров антивирусного ядра. Использование режима проверки объектов в памяти позволяет проверять объекты, не сохраняя их во временном каталоге на жестком диске. За счет настройки параметров проверки до 8 объектов объемом до 1 МБ каждый могут обрабатываться параллельно в оперативной памяти без использования дисковой подсистемы (см. п. 5.5 на стр. 60).

Файлы размером более 1 МБ сохраняются для обработки в служебном каталоге **Store**. Он расположен в каталоге установки приложения. Каталог **Store**, а также хранилище временных файлов – каталог **TMP** должны быть исключены из проверки установленным на компьютере Антивирусом Касперского 5.0 для Windows File Servers и другими антивирусными программами.

5.1. Уровень антивирусной защиты

Антивирус Касперского позволяет обнаружить и предотвратить распространение через защищаемый почтовый сервер следующих категорий объектов:

- Всех известных на настоящее время вредоносных программ.
- Программ, которые не являются вредоносным кодом в традиционном понимании этого термина, но могут представлять моральную угрозу, причинять материальные убытки и способствовать воровству конфиденциальной информации. К программам этой категории относятся:
  - рекламные программы;
  - различные безвредные утилиты, которые могут использоваться вредоносными программами и злоумышленниками в своих целях;
  - программы автоматического дозвона на платные сайты;

- программы автоматического дозвона на порно-сайты;
- программы автоматической загрузки файлов с порно-содержанием;
- клавиатурные шпионы;
- программы вскрытия паролей;
- программы удаленного управления.

. Программ-шуток и странного по форме и содержанию программного обеспечения, воздействие которого на систему не может быть определено однозначно положительно. К таким программам можно отнести:

- программы, вызывающие внезапные видео- и аудио-эффекты;
- программы, вызывающие проблемы работы системы;
- симуляторы вирусов.

. Программ, которые не являются вредоносным кодом и не несут никакого ущерба их обладателю, но могу являться частью среды разработки вредоносного программного обеспечения. К программам данной категории относятся:

- программы-взломщики лицензионного программного обеспечения, генераторы ключей, генераторы номеров кредитных карточек;
- java-классы;
- программы-сборщики информации о безопасности системы (установленных антивирусах, сетевых экранах и т. д.);
- сетевые утилиты (сканеры и т. д.).

Помимо перечисленных программ к каждой категории может быть отнесено легальное программное обеспечение, работа которого может быть расценена Антивирусом, как поведение вредоносного или потенциально-опасного программного обеспечения. К таким программам, например, относятся программы удаленного управления и удаленного наблюдения.

Если через почтовый сервер передается программное обеспечение, программы данного класса следует исключить из числа проверяемых объектов (см. п. 5.3 на стр. 51).

Какие категории объектов Антивирус обнаруживает в почтовом потоке защищаемого сервера, определяется установленным уровнем

антивирусной защиты. В приложении предусмотрены следующие уровни защиты:

- **Стандартная антивирусная защита**: защита от всех известных на настоящее время вредоносных программ. Данный уровень установлен по умолчанию.
- **Расширенная антивирусная защита**: защита от всех известных на настоящее время вредоносных программ и потенциально опасных программ, перечисленных в пункте б приведенного выше списка.
- **Избыточная антивирусная защита**: защита от всех известных на настоящее время вредоносных программ и потенциально опасных программ, перечисленных в пунктах б, в и г приведенного выше списка.

5.2. Включение и отключение антивирусной защиты сервера. Выбор уровня

Если антивирусная защита сервера включена, то вместе с запуском и остановкой Microsoft Exchange Server происходит запуск антивирусной проверки почтового трафика. Если в параметрах антивирусной защиты предусмотрена фоновая проверка хранилищ, то ее запуск осуществляется либо при получении обновлений антивирусных баз, либо по расписанию (см. п. 5.6 на стр. 62).

Проверка объектов выполняется в соответствии с установленным уровнем антивирусной защиты.

Если антивирусная защита сервера отключена, ни антивирусная проверка трафика, ни фоновая проверка хранилищ не проводятся.

Следует помнить, что отключение антивирусной защиты сервера значительно повышает вероятность проникновения вредоносных программ через почтовую систему. Не рекомендуется отключать антивирусную защиту надолго.

Для того чтобы включить или отключить антивирусную защиту, либо изменить ее уровень,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.

2. В открывшемся окне Антивирусная защита (см. рис. 13) выберите закладку **Общие**.

   В группе полей **Антивирусная защита** выберите:

   - **Выключена** – для того чтобы отключить антивирусную защиту почты.
   - **Стандартная антивирусная защита**, **Расширенная антивирусная защита** или **Избыточная антивирусная защита** – для того чтобы включить антивирусную защиту почты с соответствующим уровнем.

Если вы используете расширенный или избыточный уровень антивирусной защиты, это может сказаться на скорости работы Антивируса. К тому же, ряд программных продуктов при пересылке по почте может быть отнесен к потенциально опасным программам.

Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**. Антивирусная защита будет отключена / включена через одну-две минуты.

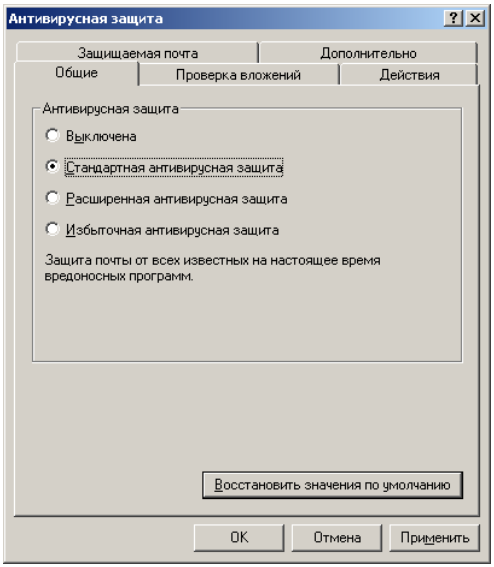


Рисунок 13. Включение антивирусной защиты

Не рекомендуется отключать антивирусную защиту путем отключения запуска службы Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 вручную через **Управление компьютером** / **Службы**.

Если все-таки возникает необходимость отключить службу Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 вручную, выполните следующие действия:

1. Отключите антивирусную защиту почты через Консоль управления.
2. Перезапустите службу Microsoft Exchange Information Store.
3. Установите для службы Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 тип запуска – **Отключено**.

Чтобы запустить Антивирус после того, как был выключен автоматический запуск службы Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003, выполните следующие действия:

1. Установите для службы Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003 тип запуска – **Авто**.
2. Перезапустите службу Microsoft Exchange Information Store.
3. Включите антивирусную защиту почты через Консоль управления.

5.3. Проверка вложений

Для уменьшения нагрузки на сервер при выполнении антивирусной проверки вы можете ограничить перечень проверяемых объектов, а также время проверки одного объекта. Ограничения на проверку используются как при проверке трафика, так и при фоновой проверке хранилищ.

Следует помнить, что тело письма проверяется всегда, ограничения касаются только вложений.

Для уменьшения нагрузки на сервер в режиме защиты трафика рекомендуется также не проверять перенаправляемую сервером почту.

Для того чтобы определить объекты, которые не будут подвергаться антивирусной проверке,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.
2. В открывшемся окне **Антивирусная защита** (см. рис. 14) выберите закладку **Проверка вложений**.
3. В группе полей **Не проверять** определите объекты, которые не будут подвергаться антивирусной проверке.
4. Для того чтобы ограничить время проверки одного объекта установите флажок **Остановить проверку, если она длится более [NN] сек.** и укажите время проверки в секундах.
5. По окончании настройки, чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

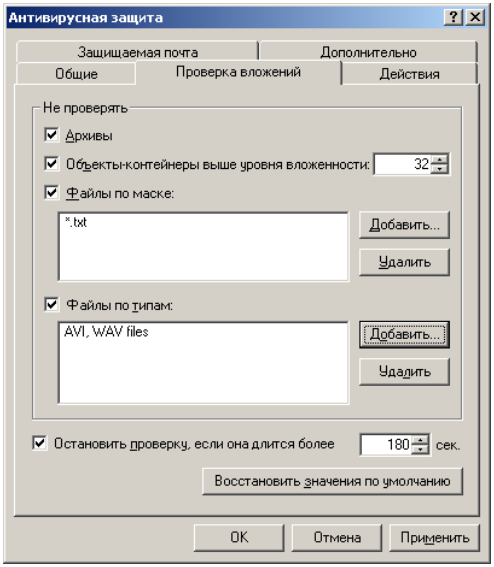


Рисунок 14. Настройка ограничений проверки вложений

Поскольку проверка архивов и объектов-контейнеров требует достаточного количества времени и ресурсов сервера, вы можете самостоятельно определять необходимость их анализа на присутствие вирусов.

Для того чтобы исключить из проверки архивы,

в группе полей **Не проверять** установите флажок **Архивы**.

Для того чтобы исключить из проверки объекты-контейнеры,

в группе полей **Не проверять** установите флажок **Объекты-контейнеры выше уровня вложенности** и определите уровень проверки. Программа проверит все вложения объекта-контейнера включая указанный уровень.

Поскольку архивы являются одной из разновидностей объектов-контейнеров, то ограничения на их проверку взаимосвязаны.
Если вы накладываете ограничения на проверку объектов-контейнеров, то и архивы будут проверяться до указанного уровня вложенности (если они не исключены из проверки явным образом).
Исключение из проверки архивов не влияет на проверку других видов объектов-контейнеров.

Существуют объекты, которые не могут быть заражены. Для снижения нагрузки на сервер при выполнении антивирусной обработки почтовых сообщений мы рекомендуем заранее определять типы и/или имена таких вложенных файлов и отсеивать их при проверке почты. Для этого следует воспользоваться настройкой исключений по маске и по типам.

Для того чтобы исключить из проверки объекты по маске,

1. В группе полей **Не проверять** установите флажок **Файлы по маске**.
2. При помощи кнопок **Добавить** и **Удалить** сформируйте список масок исключений.

   При добавлении новой маски в открывшемся окне **Добавление маски** (см. рис. 15) введите маску файла.

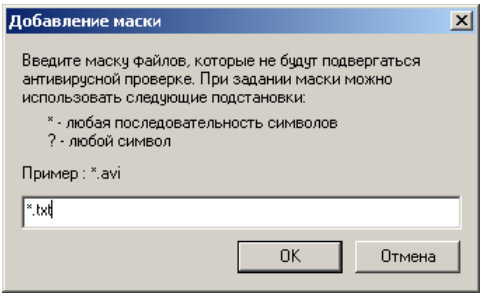


Рисунок 15. Добавление маски для файлов, исключаемых из проверки

Примеры разрешенных масок исключений:

- ***.txt** – все файлы с маской **.txt*

- ***.tx?** – все файлы с маской **.tx?*
- **test** – все файлы с именем *test*

3. Чтобы изменения вступили в силу нажмите на кнопку **Применить** или **ОК**.

Для того чтобы исключить из проверки объекты по типам,

1. В группе полей **Не проверять** установите флажок **Файлы по типам**.
2. При помощи кнопок **Добавить** и **Удалить** сформируйте список типов объектов вложений, которые не будут подвергаться антивирусной проверке.

   При добавлении типа в окне **Добавление типа** (см. рис. 16) из раскрывающегося списка выберите тип.

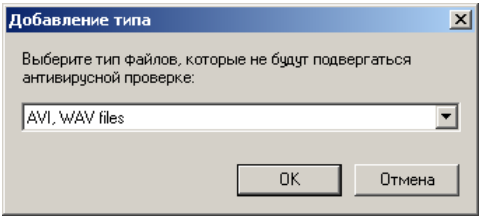


Рисунок 16. Выбор типа исключаемых из проверки файлов

3. Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

Для того чтобы исключить из проверки почту, направляемую на другие сервера,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.
2. В открывшемся окне **Антивирусная защита** (см. рис. 17) выберите закладку **Защищаемая почта**.
3. В группе полей Маршрутизируемая почта (для Microsoft Exchange Server 2003) установите флажок **Не проверять маршрутизируемую почту** (установлен по умолчанию).

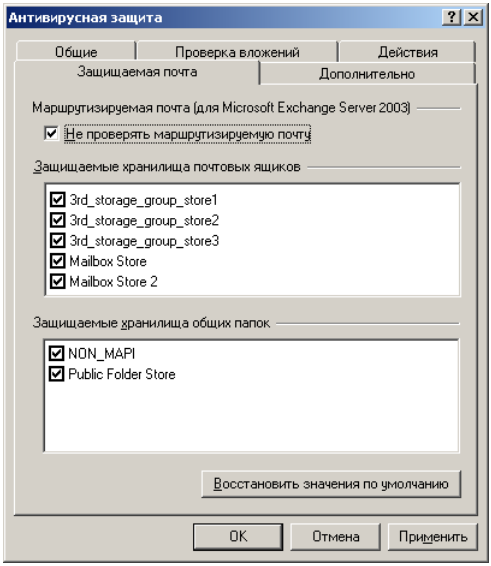


Рисунок 17. Исключение из проверки транзитного трафика

5.4. Действия над зараженным объектом

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

- **Незараженный** – не содержит вирусов.
- **Зараженный** – содержит как минимум один из известных вирусов.
- **Подозрительный** – код объекта похож на код известного или неизвестного вируса.
- **Защищенный** – объект защищен паролем.
- **Поврежденный** – объект поврежден.

В зависимости от статуса объекта к нему могут быть применены те или иные действия.

Самой важной и основной функцией приложения является *лечение* **зараженных** объектов. Лечение осуществляется на основании информации антивирусных баз и по его результатам объекту присваивается один из статусов:

- **Вылеченный** – объект успешно вылечен.
- **Невылеченный** – объект вылечить не удалось (объект неизлечим или операция лечения не применялась).

Для **невылеченных** объектов может быть задан свой порядок обработки.

К зараженным объектам, обнаруженным в теле письма, применяется действие, определенное для невылеченных объектов.

Для объектов со статусами **зараженный**, **невылеченный**, **подозрительный**, **защищенный** и **поврежденный** предусмотрены следующие действия:

- *Пропускать* – пропускать сообщение адресату без каких-либо изменений.
- *Заменять текстом тело письма и переименовывать вложения* – заменять зараженное тело письма текстом, составленным по шаблону замещения; изменять название и расширение зараженных вложенных объектов. Переименованные файлы будут иметь расширение *txt*.

Изменение имени касается только вложенных объектов, при обнаружении вируса в теле письма переименование не происходит.

- *Заменять текстом зараженные объекты* – удалять обнаруженный объект, заменяя его текстом (тело письма) или *txt*-файлом (вложение), составленным по шаблону замещения.
- *Удалять сообщение полностью* – удалить зараженное сообщение вместе со всеми вложениями (только для Microsoft Exchange Server 2003).

При лечении, замене текстом и переименовании зараженных вложений в базе данных Exchange-сервера сохраняется отдельный экземпляр сообщения для каждого получателя. Для сокращения объема базы данных Exchange-сервера мы рекомендуем регулярно проводить ее дефрагментацию.

Перед обработкой копия объекта может быть сохранена в резервном хранилище для последующего восстановления или отправки на исследование специалистам Лаборатории Касперского (см. Глава 7 на стр. 71).

Приложение может отправлять уведомление об обнаруженном объекте администратору и другим пользователям или регистрировать данное событие в журнале событий Windows (см. Глава 8 на стр. 82 и Глава 11 на стр. 114).

По умолчанию приложение пытается лечить обнаруженные **зараженные** объекты, а если лечение невозможно, заменяет объект *txt*-файлом. Для остальных статусов установлено действие **Заменять текстом тело письма и переименовывать вложения**, информационное сообщения при этом включает в себя имя обнаруженного вируса и имя зараженного объекта.

Если вложенный в сообщение объект был обработан Антивирусом Касперского (вылечен, удален, заменен), то при закрытии сообщения почтовый клиент (например, Microsoft Outlook) предложит сохранить изменения, хотя пользователь никаких изменений не проводил. Сообщение необходимо сохранить.

Для того чтобы определить порядок обработки обнаруженных в ходе антивирусной проверки объектов,

1. Выберите в дереве консоли узел, соответствующий нужному серверу и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.
2. В открывшемся окне **Антивирусная защита** (см. рис. 18) выберите закладку **Действия**.

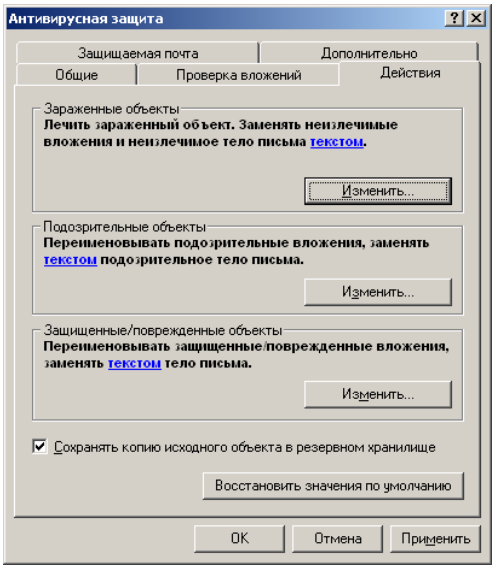


Рисунок 18. Настройка действий над зараженными объектами

На закладке отображается порядок обработки объектов отдельно для следующих статусов: **зараженный**, **подозрительный** и **защищенный/поврежденный**.

3. Определите порядок обработки объектов для каждого статуса отдельно. Для этого нажмите на кнопку **Изменить** в соответствующем разделе. В результате запускается мастер. Следуйте его указаниям.

4. В открывшемся окне (см. рис. 19) выберите действие из представленного списка.

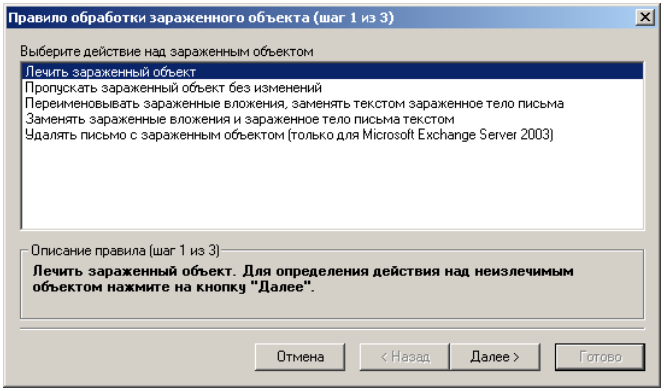


Рисунок 19. Выбор действия над зараженным объектом

В зависимости от статуса объекта, для которого осуществляется настройка, список может содержать различные значения. В нижней части окна приводится подробное описание выбранного в таблице варианта.

Дальнейшие шаги зависят от сделанного вами выбора. Для продолжения работы мастера нажмите на кнопку **Далее**.

Если дополнительной настройки параметров не требуется, будет активна кнопка **Готово**. Нажмите на нее для завершения работы мастера.

5. Если в качестве действия над зараженным объектом выбрано лечение, на следующем этапе будет предложено определить порядок обработки **невылеченных** объектов (см. рис. 20).

   Выберите нужный вариант из представленного в окне мастера списка и нажмите на кнопку **Готово** или **Далее**.

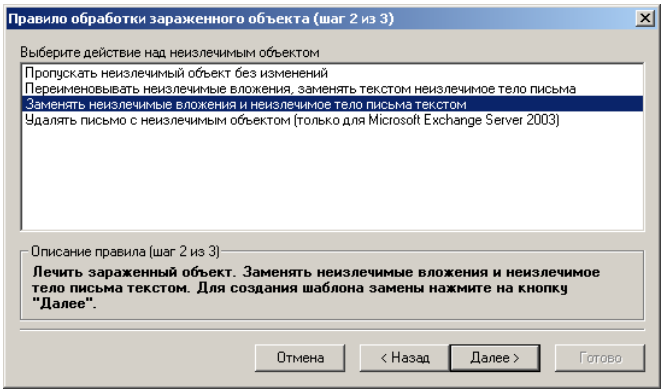


Рисунок 20. Выбор действия над невылеченным объектом

6. В случае если выбрано одно из действий замены объекта текстом, будет предложено сформировать шаблон замещения (см. рис. 21). Информационное сообщения, составленное по шаблону, записывается в тело письма и в txt-файл замещения.

   Составьте шаблон замещения. Для этого в окне мастера введите текст сообщения. В его состав может включаться информация об обнаруженном вирусе и зараженном объекте. Для этого следует добавить в шаблон соответствующие макросы подстановки, выбрав их из раскрывающегося при помощи кнопки **Макросы** списка. Подробное описание макросов содержит Приложение А на стр. 133.

   Для завершения работы мастера нажмите на кнопку **Готово**.

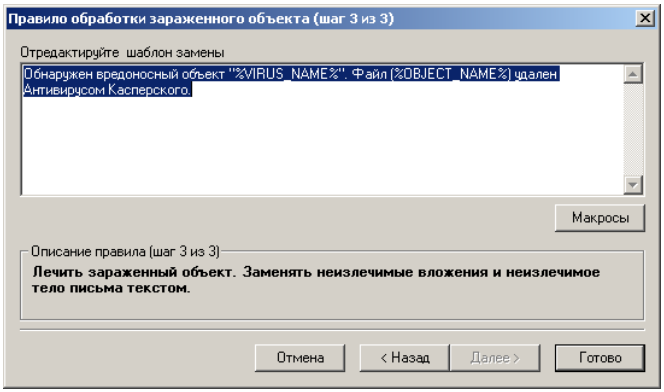


Рисунок 21. Создание шаблона замещения

7. Для того чтобы перед обработкой объекта его копия сохранялась в резервном хранилище установите флажок **Сохранять копию исходного объекта в резервном хранилище**.

8. Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

5.5. Производительность антивирусной защиты

Антивирус Касперского предоставляет возможность регулировать производительность работы приложения в зависимости от объема и характера проходящего через Exchange-сервер почтового трафика и системных характеристик компьютера: объема оперативной памяти, быстродействия, количества процессоров.

Настройка параметров производительности может осуществляться как в автоматическом режиме, так и вручную.

Для настройки параметров производительности приложения

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.

2. В открывшемся окне **Антивирусная защита** (см. рис. 22) выберите закладку **Дополнительно**.

3. В группе полей Настройка производительности выберите способ настройки: Автоматическая настройка или Ручная настройка.

4. Если вы выбрали автоматическую настройку, установите расположенный ниже ползунок в положение, соответствующее характеру проходящего через Exchange-сервер почтового трафика:

   - **Небольшой почтовый поток** предназначено для работы в условиях, когда сервер обслуживает большое количество почтовых ящиков, однако поток писем, поступающий в каждый из них, незначителен.

- **Большой почтовый поток** соответствует ситуации, когда почтовых ящиков немного, но через сервер проходит большое количество почтовых сообщений, адресованных в каждый из них.
- Среднее положение ползунка соответствует ситуации равномерного распределения потока писем по почтовым ящикам сервера.

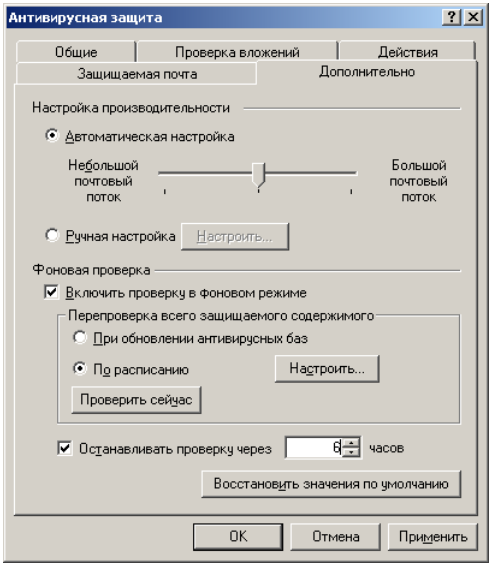


Рисунок 22. Настройка производительности антивирусной защиты и параметров фоновой проверки

5. Если вы выбрали настройку вручную, вам следует установить параметры, определяющие уровень производительности приложения. Для этого нажмите на кнопку **Настроить** и в открывшемся окне **Производительность** (см. рис. 23) укажите:
   - Количество потоков, в которых проверяются объекты (по умолчанию три). Компания Microsoft рекомендует назначать число, на единицу превышающее удвоенное количество процессоров (2*количесво_процессоров+1).
   - Количество параллельно работающих экземпляров антивирусного ядра (по умолчанию установлено значение 4).

- Будет ли программа проводить проверку объектов в оперативной памяти без предварительного сохранения их во временном каталоге. Чтобы ее разрешить, установите флажок **Проверять в памяти объекты не более** и укажите максимальный размер объекта в килобайтах. По умолчанию флажок установлен, максимальный размер объекта составляет 1024 КБ.
- Чтобы изменения вступили в силу, нажмите на кнопку **ОК**.

6. Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

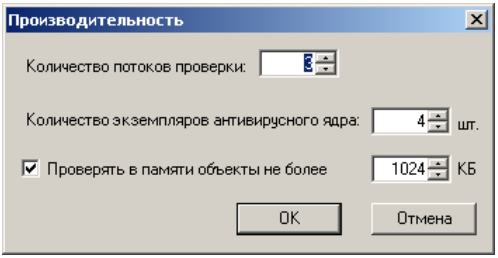


Рисунок 23. Настройка параметров производительности вручную

5.6. Фоновая проверка

Антивирус Касперского осуществляет проверку хранящейся на сервере почты и содержимого общих папок. Проверяются все общие папки и защищаемые хранилища (mailbox storages). При этом обрабатываются сообщения, которые не были проверены с использованием текущей версии антивирусных баз. Программа проверяет тело сообщения и присоединенные к нему файлы в соответствии с общими параметрами антивирусной проверки.

Если фоновая проверка хранилищ отключена, хранящиеся на сервере сообщения проверяются только при запросе их пользователем непосредственно перед доставкой.

Проверяются только почтовые ящики, расположенные в защищаемых хранилищах (см. п. 12.6 на стр. 126).

Для того чтобы Антивирус Касперского выполнял проверку хранящихся на сервере сообщений и содержимое общих папок

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**,

раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.

2. В открывшемся окне **Антивирусная защита** (см. рис. 22) выберите закладку **Дополнительно**.

3. Установите флажок **Включить проверку в фоновом режиме** (по умолчанию не установлен) и укажите режим запуска проверки, выбрав один из вариантов:

   - **При обновлении антивирусных баз** – при каждом получении новой версии антивирусных баз.
   - **По расписанию** – по сформированному расписанию.

   Если необходимо запустить проверку немедленно, нажмите на кнопку **Проверить сейчас**.

4. Если вы выбрали запуск по расписанию, сформируйте его. Для этого нажмите на кнопку **Настроить** и в открывшемся окне (см. рис. 24) укажите режим и время запуска проверки.

   Вы можете ограничить время проверки, для этого установите флажок **Останавливать проверку через [NN] часов** и укажите время в часах, по истечении которого проверка будет прекращена (по умолчанию 24 часа).

5. Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

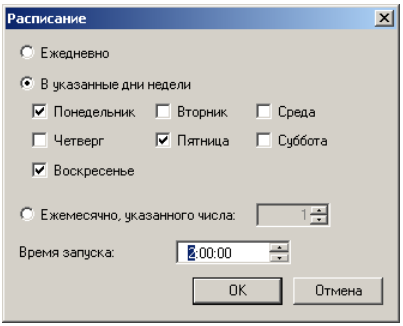


Рисунок 24. Создание расписания запуска фоновой проверки

ГЛАВА 6. ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ

Лаборатория Касперского предоставляет своим пользователям возможность обновлять антивирусные базы, используемые Антивирусом Касперского для поиска вредоносных программ и лечения зараженных объектов.

Крайне важно поддерживать антивирусные базы в актуальном состоянии, поскольку каждый день появляются новые вирусы. Мы рекомендуем вам провести обновление антивирусных баз сразу после установки приложения, поскольку базы, входящие в состав дистрибутива, к моменту установки теряют актуальность.

Приложение копирует обновления антивирусных баз через интернет с серверов обновлений Лаборатории Касперского, либо из сетевого каталога обновлений. Выбор ресурса зависит от настроек.

Загрузка обновлений происходит либо по расписанию, либо вручную. Для успешной загрузки из интернета необходимо, чтобы ваш компьютер был подключен к нему. Используя сервера обновлений, Антивирус Касперского копирует с них обновления, после чего устанавливает необходимые файлы на ваш компьютер.

Информацию об используемой приложением версии антивирусных баз и результате их последнего обновления можно посмотреть при помощи гиперссылки Антивирусные обновления в окне **Антивирусные обновления** на закладке **Общие**. Приводится следующая информация:

- дата создания антивирусных баз;
- количество записей в антивирусных базах;
- текущий статус процесса обновления.

Для обновления антивирусных баз Антивируса Касперского

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусные обновления в панели результата.
2. В открывшемся окне **Антивирусные обновления** (см. рис. 25) на закладке **Общие** определите источник получения

обновлений. Вы можете выбрать получение обновлений из интернета или из сетевого каталога (подробнее см. п. 6.1 на стр. 66 и п. 6.2 на стр. 67).

3. Для автоматического обновления сформируйте расписание получения обновлений (подробнее см. п. 6.3 на стр. 69). Если обновления необходимы немедленно, получите их вручную при помощи кнопки **Обновить сейчас** (подробнее см. п. 6.4 на стр. 70).

Перед обновлением вручную убедитесь, что настройка параметров обновления выполнена полностью и правильно.

4. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

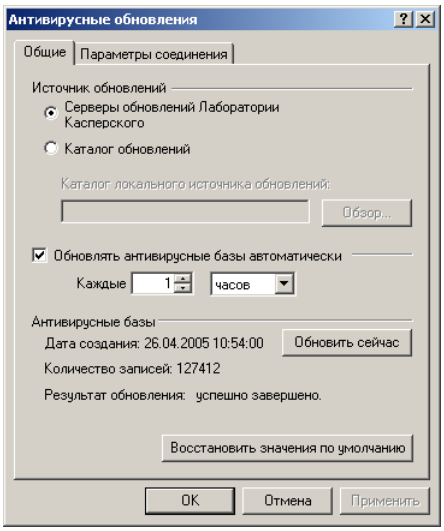


Рисунок 25. Окно настройки параметров обновления антивирусных баз. Настройка обновления из интернета

6.1. Загрузка обновлений из интернета

Для того чтобы Антивирус Касперского получал обновления антивирусных баз через интернет с HTTP-, FTP- серверов Лаборатории Касперского,

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусные обновления в панели результата.
2. В открывшемся окне **Антивирусные обновления** (см. рис. 25) на закладке **Общие** в качестве источника обновлений выберите **Серверы обновлений Лаборатории Касперского** (данный вариант установлен по умолчанию).
3. После этого настройте параметры сетевых подключений на закладке **Параметры соединения** (см. рис. 26):

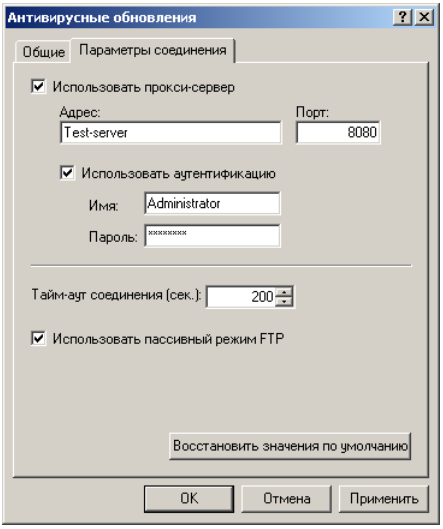


Рисунок 26. Настройка параметров сетевого подключения

- Если подключение к интернету осуществляется через прокси-сервер, установите флажок **Использовать прокси-**

сервер и определите параметры подключения: адрес и номер порта для соединения.

Если для доступа к прокси-серверу используется пароль, определите параметры аутентификации прокси-пользователя. Для этого установите флажок **Использовать аутентификацию** и заполните поля **Имя** и **Пароль**.

- В поле **Тайм-аут соединения (сек.)** задайте время, отведенное на соединение с сервером обновления. Если соединение не произошло, по истечении заданного времени предпринимается попытка соединения со следующим сервером обновлений. Перебор производится до тех пор, пока процесс соединения не завершится успешно, или пока не будут перебраны все доступные сервера обновлений.
- Установите флажок **Использовать пассивный режим FTP**, для того чтобы при обновлении по протоколу FTP использовался пассивный режим, или снимите флажок для использования активного режима. Мы рекомендуем использовать пассивный режим.

4. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

6.2. Загрузка обновлений из сетевого каталога

Если управление работой установленных на компьютерах сети приложений Лаборатории Касперского осуществляется при помощи системы централизованного управления Kaspersky Administration Kit 5.0, то получаемые Сервером администрирования обновления антивирусных баз размещаются в папке общего доступа (подробнее см. Руководство к Kaspersky Administration Kit 5.0). Вы можете использовать данную папку в качестве источника обновлений для Антивируса Касперского.

Для корректного обновления компьютер, на котором установлен Сервер безопасности, должен обладать правами на чтение из папки общего доступа.

Для того чтобы Антивирус Касперского получал обновления антивирусных баз из сетевого каталога,

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусные обновления в панели результата.

2. В открывшемся окне **Антивирусные обновления** (см. рис. 27) на закладке **Общие** в качестве источника обновлений выберите **Каталог обновлений** и в поле ввода укажите путь к сетевому или локальному каталогу. Вы можете ввести путь вручную, либо выбрать при помощи кнопки **Обзор** в стандартном окне Windows **Обзор папок** (см. рис. 28).

3. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

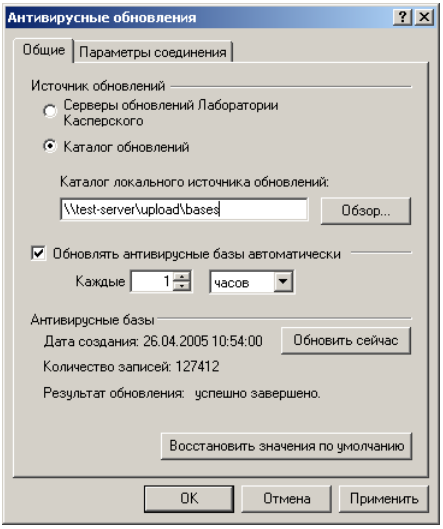


Рисунок 27. Настройка обновлений из локального каталога

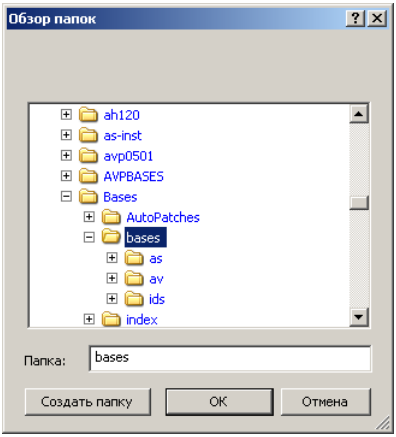


Рисунок 28. Выбор каталога обновления

6.3. Автоматическое обновление

Для того чтобы обновление антивирусных баз производилось автоматически,

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусные обновления в панели результата.
2. В открывшемся окне **Антивирусные обновления** см. рис. 25) на закладке **Общие** установите флажок **Обновлять антивирусные базы автоматически** и сформируйте расписание получения обновлений. Для этого в поле **Каждые** установите необходимую периодичность и из раскрывающегося списка выберите интервал обновления.
3. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

В результате программа будет автоматически проводить обновление антивирусных баз с заданной периодичностью в соответствии с установленными параметрами.

6.4. Обновление вручную

Для обновления антивирусных баз вручную

1. В главном окне программы выберите в дереве консоли узел **Антивирус Касперского для Microsoft Exchange Server**, раскройте его, выберите узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусные обновления в панели результата.
2. В открывшемся окне **Антивирусные обновления** см. рис. 25) на закладке **Общие** нажмите на кнопку **Обновить сейчас**.

В результате программа выполнит немедленное обновление антивирусных баз в соответствии с установленными параметрами.

ГЛАВА 7. РЕЗЕРВНОЕ КОПИРОВАНИЕ

Антивирус Касперского предоставляет возможность сохранять копию зараженного объекта перед его обработкой. Копия объекта помещается в *резервное хранилище.* В дальнейшем объект из резервного хранилища может быть:

- **восстановлен**. Эта возможность может быть полезна, например, если при лечении объекта были утеряны данные, объект был удален по ошибке, или необходимо провести повторное лечение объекта с использованием обновленной версии антивирусных баз (см. п. 7.3 на стр. 76).
- **отправлен на исследование специалистам Лаборатории Касперского**. Например, такая возможность может быть использована, если лечение зараженного объекта, оказалось не возможным. Возможно, экспертам удастся обнаружить ранее неизвестный вирус, и его описание будет включено в обновления антивирусных баз. Тогда последующая проверка объекта с использованием обновленной версии антивирусных баз позволит вылечить его и сохранить целостность содержащихся в нем данных (см. п. 7.4 на стр. 77).
- **удален** (см. п. 7.5 на стр. 78).

Резервная копия объекта создается, только если это предусмотрено значением параметров антивирусной защиты: установлен флажок **Сохранять копию исходного объекта в резервном хранилище** на закладке **Действия** окна **Антивирусная защита** (см. рис. 18) (см. п. 5.4 на стр. 55).

В резервном хранилище объект размещается в закодированном виде, что обеспечивает:

- отсутствие риска заражения (объект не доступен без расшифровки);
- экономию времени работы антивирусных программ (файлы в формате резервного хранилища не определяются как зараженные).

Объем информации в резервном хранилище может быть ограничен по одному из двух параметров: размеру резервного хранилища, или времени хранения объекта. По умолчанию ограничен размер хранилища, максимальный объем составляет 50 МБ. Администратор может изменить параметр ограничения и его значение (см. п. 7.6 на стр. 79).

Проверка соблюдения ограничений производится при записи резервной копии очередного объекта в хранилище. Приложение выполняет следующее:

- если установлено ограничение на размер хранилища и для размещения объекта недостаточно памяти, освобождает необходимый объем за счет удаления наиболее старых объектов;
- если установлено ограничение на срок хранения объекта, удаляет объекты, срок хранения которых закончился.

Фактически объект может оставаться в резервном хранилище дольше установленного срока, если в хранилище не добавляются новые объекты.

Просмотр резервного хранилища (см. п. 7.1 на стр. 72), настройка его параметров (см. п. 7.6 на стр. 79) и работа с резервными копиями объектов (см. п. 7.3 на стр. 76, п. 7.4 на стр. 77 и п. 7.5 на стр. 78) осуществляется через служебную папку **Резервное хранилище** (см. рис. 29). Данная папка входит в состав каждого узла, отображающего управляемый Exchange-сервер.

Для упрощения просмотра и поиска информации в резервном хранилище, а также ее структурирования предусмотрена возможность настройки пользовательских фильтров (см. п. 7.2 на стр. 73). Сформированные для резервного хранилища фильтры отображаются в папке **Резервное хранилище** в виде вложенных подпапок с именами, заданными администратором при их создании.

7.1. Просмотр резервного хранилища

Для просмотра резервного хранилища

выберите в дереве консоли папку **Резервное хранилище**.

После этого в панели результатов будет представлена таблица (см. рис. 29), содержащая полный перечень всех объектов, размещенных в резервном хранилище.

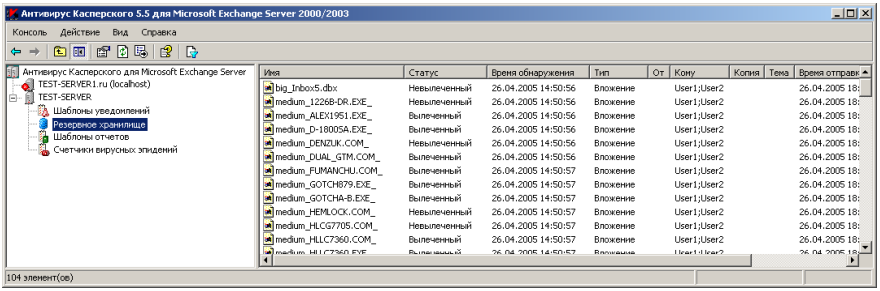


Рисунок 29. Просмотр резервного хранилища

Для каждого объекта помимо стандартных атрибутов почтового сообщения (**От**, **Кому**, **Копия**, **Тема**, **Время отправки**) в таблице отображается следующая информация:

- **Имя**. Для вложения используется его исходное имя, тело письма сохраняется под именем **<тело письма>**.
- **Статус**. Статус, присвоенный объекту в результате антивирусной проверки или по результатам лечения: **невылеченный**, **вылеченный**, **подозрительный**, **защищенный/поврежденный** (см. п. 5.4 на стр. 55).

  В резервном хранилище размещается **копия** объекта, **до того** как он был обработан Антивирусом. Поле **Статус** показывает состояние объекта **после** обработки.
- **Время обнаружения**. Точная дата и время, когда объект был обнаружен Антивирусом Касперского.
- **Тип**. Тип объекта, размещенного в резервном хранилище (**Тело письма** или **Вложение**), характеризует, где был обнаружен зараженный объект.
- **Каталог хранения**. Путь к каталогу на диске, где хранится резервная копия объекта.

Вы можете сортировать информацию в таблице по возрастанию или убыванию данных любого из столбцов.

7.2. Фильтр резервного хранилища

Использование фильтров позволяет осуществлять поиск и структурировать представленную в резервном хранилище информацию, поскольку после

применения фильтра доступной становится только информация, удовлетворяющая его параметрам. Это является весьма актуальным в связи с большим объемом хранящихся в резервном хранилище объектов. Фильтр может быть использован, например, для поиска объекта, который необходимо восстановить.

Для того чтобы создать фильтр резервного хранилища

1. Выберите в дереве консоли папку **Резервное хранилище** и воспользуйтесь командой **Фильтр** контекстного меню или аналогичным пунктом в меню **Действие**. В результате открывается окно настройки фильтра (см. рис. 30).
2. Укажите имя, под которым фильтр будет входить в состав папки **Резервное хранилище**.
3. Укажите значения параметров фильтра, по которым будет осуществлен поиск (отбор) объектов в резервном хранилище. Для настройки параметров используются следующие атрибуты объекта:
   - статус объекта (можно выбрать несколько значений);
   - имя объекта;
   - отправитель письма;
   - получатель письма;
   - тема письма;
   - временной интервал, в течение которого было отправлено письмо.
4. По окончании настройки параметров фильтра, для его создания нажмите на кнопку **Применить** или **ОК**. Чтобы отказаться от создания фильтра, нажмите на кнопку **Отмена**.

В результате в дереве консоли в папке **Резервное хранилище** создается вложенная папка с именем фильтра. При выборе фильтра в дереве консоли в панели результатов отображается только информация, удовлетворяющая критериям фильтра.

В дальнейшем вы можете изменить значения параметров фильтра или удалить фильтр при помощи команд контекстного меню и меню **Действие**.

Для изменения параметров фильтра

1. Выберите нужный фильтр в папке **Резервное хранилище** дерева консоли и воспользуйтесь командой **Свойства** контекстного меню или аналогичным пунктом в меню **Действие**. В результате открывается окно настройки фильтра (см. рис. 30).

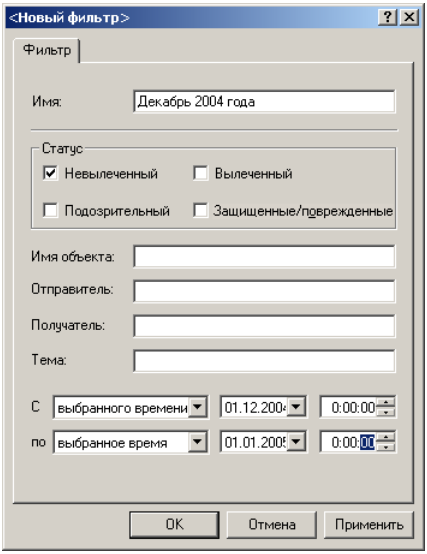


Рисунок 30. Создание фильтра

2. Внесите необходимые изменения в значения его параметров.
3. Чтобы изменения вступили в силу нажмите на кнопку **Применить** или **ОК**. Для выхода без сохранения внесенных изменений, нажмите на кнопку **Отмена**.

В результате информация, представленная в панели результатов, обновляется в соответствии с новыми значениями параметров фильтра.

Для удаления фильтра

выберите необходимый фильтр в папке **Резервное хранилище** и воспользуйтесь командой **Удалить** контекстного меню или аналогичным пунктом в меню **Действие**.

В результате фильтр удаляется из папки **Резервное хранилище**.

Удаление объектов из резервного хранилища при удалении фильтра не производится. Объекты, удовлетворявшие параметрам фильтра, по-прежнему доступны через папку **Резервное хранилище**.

7.3. Восстановление объекта из резервного хранилища

Для восстановления объекта из резервного хранилища

1. Выберите в дереве консоли папку **Резервное хранилище**.
2. В таблице, отображающей содержимое хранилища (см. рис. 29), выберите объект для восстановления. Для поиска объекта вы можете использовать фильтр (см. п. 7.2 на стр. 73).
3. Откройте контекстное меню и воспользуйтесь командой **Получить файл** или аналогичным пунктом в меню **Действие**.
4. В открывшемся окне (см. рис. 31) укажите каталог, в котором будет сохранен восстановленный объект и, если это необходимо, введите или измените имя объекта.
5. Перед сохранением выводится предупреждающее сообщение (см. рис. 32) с запросом на продолжение операции. Для восстановления объекта нажмите на кнопку **Да**.

В результате объект перемещается из резервного хранилища в указанный каталог, расшифровывается и сохраняется под заданным именем. Восстановленный объект будет иметь тот же формат, с каким объект поступил на обработку Антивирусу Касперского. После успешного восстановления объекта на экран компьютера выводится соответствующее уведомление.

Рекомендуем вам восстанавливать только объекты со статусом: **подозрительный** и **защищенный/поврежденный**. Повторная проверка таких объектов с использование обновленной версии антивирусных баз может изменить их статус: объект может быть вылечен или в нем обнаружен ранее неизвестный вирус.

Восстановление других объектов может привести к заражению вашего компьютера!

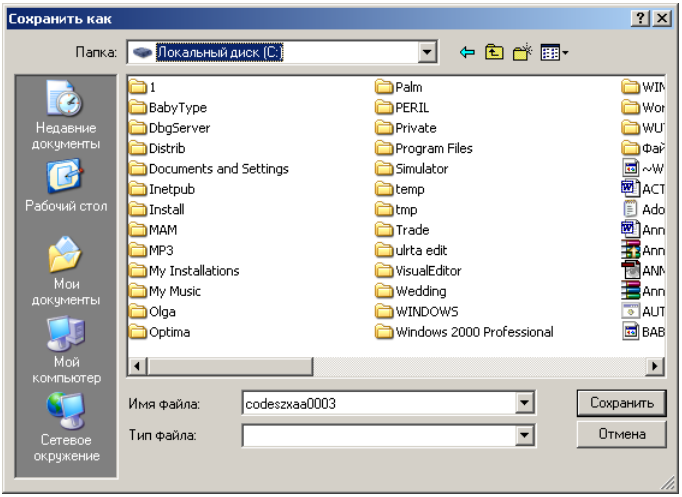


Рисунок 31. Восстановление объекта из резервного хранилища

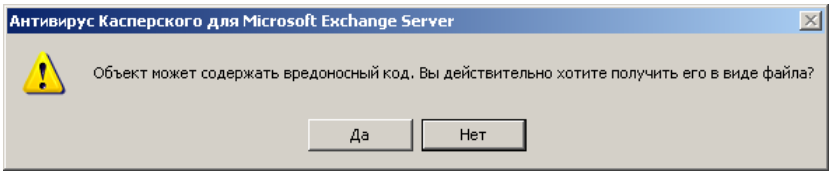


Рисунок 32. Подтверждение восстановления объекта

7.4. Отправка объекта на исследование

Чтобы отправить объект из резервного хранилища на анализ специалистам Лаборатории Касперского,

1. Выберите в дереве консоли папку **Резервное хранилище**.
2. В таблице, отображающей содержимое хранилища (см. рис. 29), выберите объект для отправки. Для поиска объекта вы можете использовать фильтр (см. п. 7.2 на стр. 73).
3. Откройте контекстное меню и воспользуйтесь командой **Отправить файл на исследование** или аналогичным пунктом в меню **Действие**.

В результате на компьютере, где установлен управляемый Exchange-сервер, автоматически формируется почтовое сообщение с вложенным объектом и отправляется в Лабораторию Касперского.
После отправки сообщения на экран компьютера, с которого осуществляется управление, выводится уведомление об отправке (см. рис. 33).

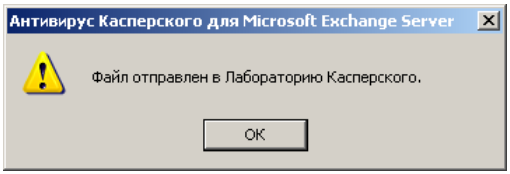


Рисунок 33. Уведомление об отправке объекта на исследование

7.5. Удаление объекта из резервного хранилища

Из резервного хранилища автоматически удаляются следующие объекты:

- наиболее старые объекты, если установлено ограничение на размер хранилища и для размещения нового объекта недостаточно места на диске. При этом будет удалено столько старых объектов, сколько потребуется для освобождения нужного объема диска.
- объекты, срок хранения которых закончился, если установлено ограничение на срок хранения объекта.

Предусмотрена также возможность удаления объекта из резервного хранилища вручную. Она может быть полезна для удаления успешно восстановленных или отправленных на исследование объектов, а также для принудительного освобождения резервного хранилища, если не подходят автоматические способы удаления объектов.

Чтобы удалить объект из резервного хранилища вручную,

1. Выберите в дереве консоли папку **Резервное хранилище**.
2. В таблице, отображающей содержимое хранилища (см. рис. 29), выберите объект для удаления. Для поиска объекта вы можете использовать фильтр (см. п. 7.2 на стр. 73).

3. Откройте контекстное меню и воспользуйтесь командой **Удалить** или аналогичным пунктом в меню **Действие**.

В результате объект удаляется из таблицы, отображающей содержимое резервного хранилища.

7.6. Настройка параметров резервного хранилища

Резервное хранилище создается при установке компонента Сервер безопасности. Значения параметров хранилища определяются по умолчанию и могут быть изменены администратором.

Чтобы изменить значения параметров резервного хранилища,

1. Выберите в дереве консоли папку **Резервное хранилище**.
2. Откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**.
3. В открывшемся окне **Свойства: Резервное хранилище** (см. рис. 34) установите необходимые значения параметров.

   Чтобы изменить каталог размещения резервного хранилища, в поле **Каталог резервного хранилища** введите вручную или укажите при помощи кнопки **Обзор** путь к новому каталогу и его имя (см. рис. 35).

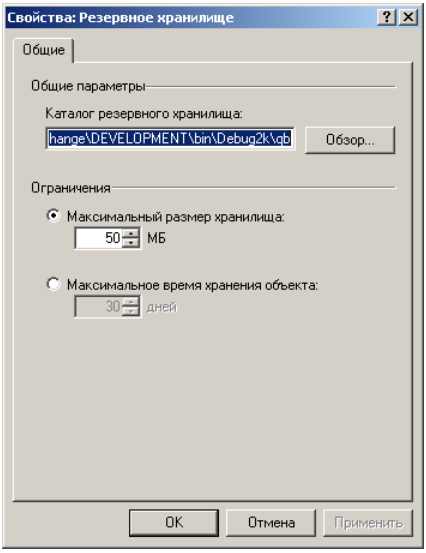


Рисунок 34. Настройка параметров резервного хранилища

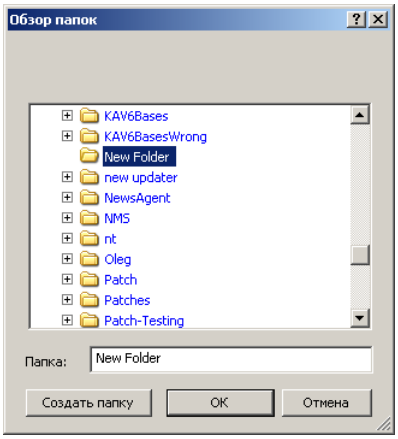


Рисунок 35. Смена каталога резервного хранилища

По умолчанию резервная копия объекта сохраняется в каталоге **qb**. Это служебный каталог программы, он создается в каталоге установки приложения при установке компонента Сервер безопасности. При смене каталога резервного хранилища ранее созданные резервные копии объектов останутся в том каталоге, где они были изначально размещены. Удаление объектов из

всех каталогов осуществляется автоматически, в соответствии с установленным ограничением.

Чтобы установить ограничение, в разделе **Ограничения** выберите один из вариантов и введите нужное значение параметра:

- **Максимальный размер хранилища** – если вы хотите ограничить общий размер объектов, хранящихся в резервном хранилище (выбран по умолчанию); в поле ввода укажите необходимый объем (по умолчанию он составляет 50 МБ). При подсчете учитывается суммарный размер всех объектов, не зависимо от каталога их размещения.
- **Максимальное время хранения объекта** – если вы хотите ограничить срок хранения объектов в резервном хранилище (по умолчанию не ограничен); в поле ввода укажите необходимое количество дней (по умолчанию предлагается 30 дней).

4. Чтобы изменения вступили в силу нажмите на кнопку **Применить** или **ОК**. Для выхода без сохранения внесенных изменений нажмите на кнопку **Отмена**.

ГЛАВА 8. УВЕДОМЛЕНИЯ

Приложение Антивирус Касперского предоставляет возможность оповещать об обнаруженных при антивирусной проверке зараженных объектах.

Предусмотрено уведомление о событиях следующих типов:

- **обнаружен зараженный объект**;
- **обнаружен подозрительный объект**;
- **обнаружен поврежденный объект**.

Для каждого типа событий формируется уведомление соответствующего типа:

- **О зараженном объекте**.
- **О подозрительном объекте**.
- **О поврежденном объекте**.

Уведомление может производиться несколькими способами:

- рассылкой сообщений по электронной почте;
- рассылкой сообщений по сети средствами Net Send;
- регистрацией события в системном журнале **Windows** на компьютере, где установлен компонент Сервер безопасности.

  В этом случае доступ к информации осуществляется при помощи стандартного инструмента **Windows** просмотра и управления журналами **Просмотр событий**.

Предусмотрена возможность оповещения отправителя и получателя сообщения о зараженном объекте.

Получатели скрытых копий сообщения не оповещаются о зараженном объекте.

Порядок уведомления, способ распространения и текст рассылаемых сообщений формируются администратором в виде шаблона уведомления.

На основании сформированного шаблона в случае возникновения события соответствующего типа автоматически производится оповещение о нем.

Может быть сформировано несколько шаблонов уведомлений одного типа с различными значениями параметров, что позволяет настроить различные

по содержанию и способу рассылки уведомления для администратора, отправителя, получателя или службы безопасности.

По умолчанию уведомление об обнаруженных зараженных объектах не производится. Однако при установке Сервера безопасности формируется встроенный шаблон уведомления. На основании этого шаблона может быть настроено уведомление.

Шаблоны уведомлений размещаются в служебной папке **Шаблоны уведомлений**. Данная папка входит в состав каждого узла, отображающего управляемый Exchange-сервер.

Перечень сформированных шаблонов уведомлений представлен в панели результатов в виде таблицы (см. рис. 36). Для каждого шаблона таблица отображает имя шаблона и тип уведомления.

Подробно с параметрами шаблона уведомления можно ознакомиться, вызвав окно настройки при помощи команды контекстного меню **Свойства** (см. п. 8.1 на стр. 84).

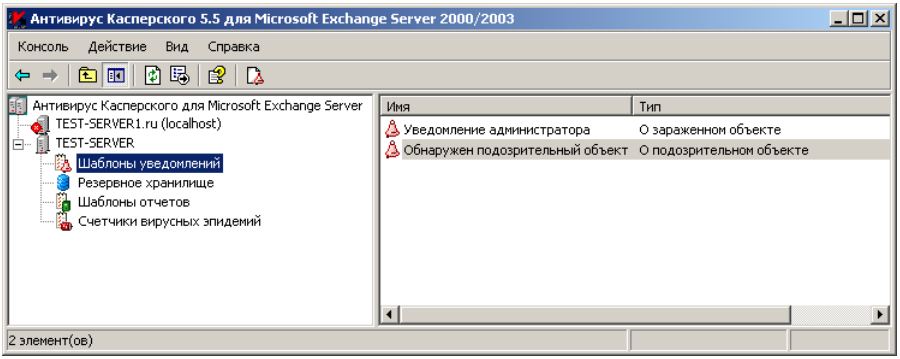


Рисунок 36. Папка **Шаблоны уведомлений**

Администратор может создавать новые шаблоны, просматривать и редактировать параметры существующих, переименовывать и удалять их при помощи команд контекстного меню.

Для того чтобы выполнялось уведомление об обнаруженных при антивирусной проверке зараженных объектах,

1. Создайте шаблон уведомления (см. п. 8.2 на стр. 86) или выберите существующий и настройте его параметры (см. п. 8.1 на стр. 84).
2. Установите флажок **Уведомлять о событии** на закладке **Общие** окна настройки шаблона уведомления (см. рис. 37).

8.1. Просмотр и изменение параметров уведомления

Чтобы просмотреть или изменить параметры уведомления,

1. Выберите в дереве консоли папку **Шаблоны уведомлений**.
2. В таблице, отображающей перечень сформированных шаблонов (см. рис. 29), выберите необходимый шаблон уведомления.
3. Откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**.
4. В результате открывается окно настройки шаблона уведомления **Свойства: <Имя шаблона>** (см. рис. 37). Окно состоит из закладок: **Общие**, **Текст**, **Действие** и полностью аналогичное окну **<Новый шаблон уведомлений>** (см. рис. 40). Изменение параметров уведомления выполняется так же, как их установка при создании (см. п. 8.2 на стр. 86).

   На закладке **Общие** (см. рис. 37) вы можете посмотреть и изменить имя шаблона, описание и тип уведомления, а так же определить выполняется оповещение по данному шаблону или нет. Если флажок **Уведомлять о событии** установлен, оповещение проводится, если снят – не проводится.

   На закладке **Текст** (см. рис. 38) вы можете ознакомиться с шаблоном сообщения, которое направляется в качестве уведомления, и изменить значения его параметров.

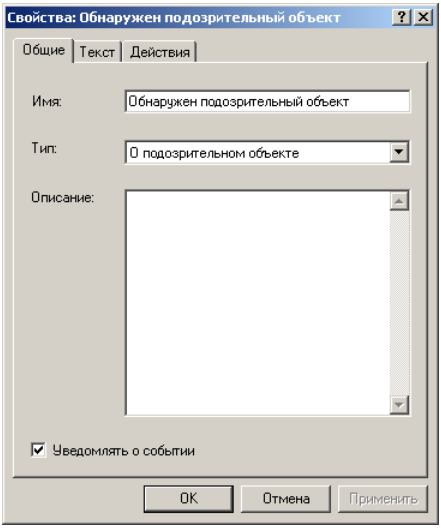


Рисунок 37. Изменение шаблона уведомления. Закладка **Общие**

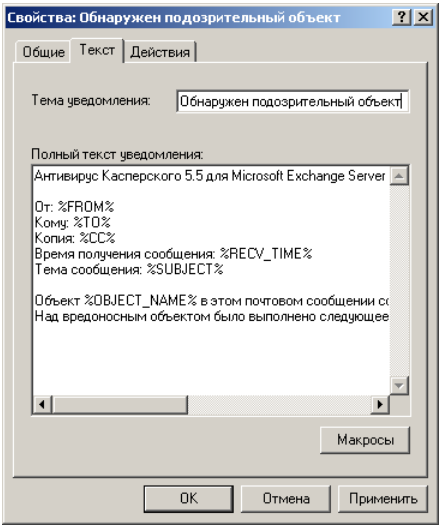


Рисунок 38. Изменение шаблона уведомления. Закладка **Текст**

На закладке **Действия** (см. рис. 39) представлены способы уведомления, указаны адресанты и перечислены компьютеры-получатели сообщений (если выбраны соответствующие

варианты уведомления). Вы можете установить другие способы уведомления и изменить значения параметров.

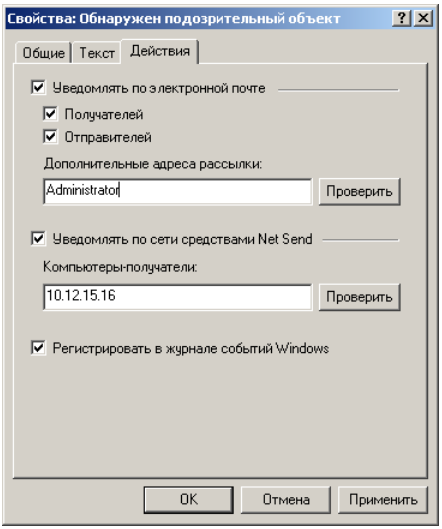


Рисунок 39. Изменение шаблона уведомления. Закладка **Действия**

5. После внесения изменений, чтобы новые значения параметров вступили в силу, нажмите на кнопку **Применить** или **ОК**. Для выхода без сохранения изменений нажмите на кнопку **Отмена**.

8.2. Создание шаблона уведомления

Для создания нового шаблона уведомления,

1. Выберите в дереве консоли папку **Шаблоны уведомлений**.
2. Откройте контекстное меню и воспользуйтесь командой **Новый шаблон уведомлений** или аналогичным пунктом в меню **Действие**.
3. В результате открывается окно настройки нового шаблона уведомления **<Новый шаблон уведомлений>** (см. рис. 40). Установите необходимые значения для параметров, представленных на закладках окна.

На закладке **Общие** (см. рис. 40) выполните следующие действия:

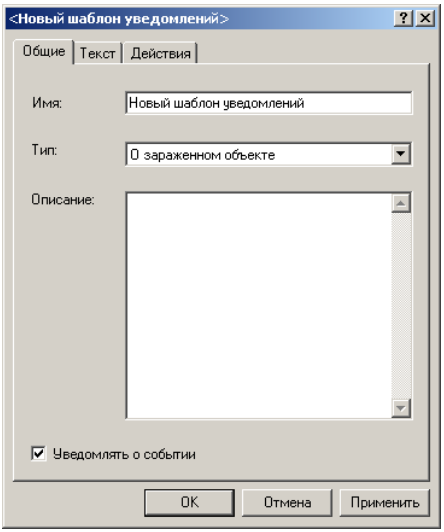


Рисунок 40. Шаблон уведомления. Закладка **Общие**

- Введите имя шаблона в поле **Имя**.
- Укажите тип уведомления. Он должен соответствовать событию, при возникновении которого будет формироваться уведомление.

  Для этого в поле **Тип** выберите необходимое значение из раскрывающегося списка. В списке представлены следующие значения:

  - **О зараженном объекте**.
  - **О подозрительном объекте**.
  - **О поврежденном объекте**.
- Если необходимо, введите более подробное описание уведомления в поле **Описание**.
- Определите, будут формироваться уведомления на основании данного шаблона или нет.

  Для этого установите или снимите флажок **Уведомлять о событии**.

На закладке **Текст** (см. рис. 41) создайте шаблон сообщения, которое будет направляться в качестве уведомления:

- Введите краткое описание уведомления в поле **Тема уведомления**. Эта строка будет использоваться в качестве заголовка письма.
- Сформируйте текст сообщения в поле **Полный текст уведомления**. В состав сообщения может включаться информация о зарегистрированном событии. Для этого следует вставить в шаблон соответствующие макроподстановки, выбрав необходимые из раскрывающегося при помощи кнопки **Макросы** списка. Полный перечень макроподстановок содержит Приложение А на стр. 133.

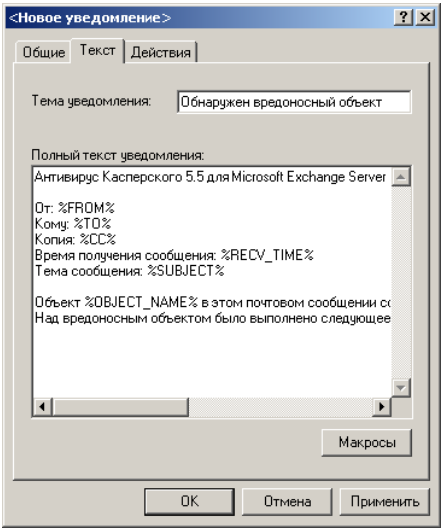


Рисунок 41. Шаблон уведомления. Закладка **Текст**

На закладке **Действия** (см. рис. 42) выберите способы уведомления и определите соответствующие им значения параметров. Допускается выбор нескольких способов.

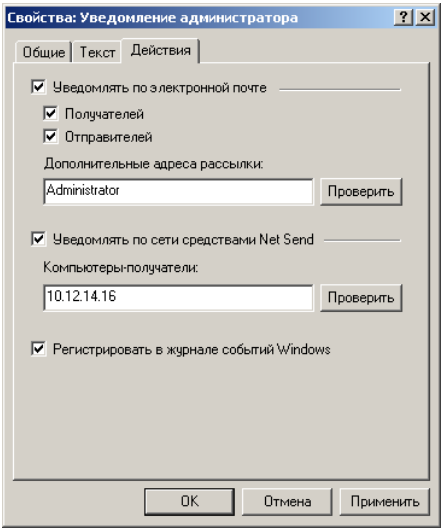


Рисунок 42. Шаблон уведомления. Закладка **Действие**

- Для отправки сообщений через почтовый сервер установите флажок **Уведомлять по электронной почте** и укажите адресатов рассылки.
  - Чтобы информировать отправителей и получателей зараженного сообщения об обнаруженном объекте, установите флажки **Получателей** и **Отправителей**.
  - Для уведомления других пользователей, например, администратора, введите его электронный адрес в поле **Дополнительные адреса рассылки**.

    Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

    Допускается ввод нескольких электронных адресов, разделенных точкой с запятой.
- Для отправки сообщений по сети с помощью службы Net Send установите флажок **Уведомлять по сети средствами Net Send** и укажите адреса компьютеров-получателей в поле **Компьютеры-получатели**.

  В качестве адреса также можно использовать IP-адрес или NetBIOS-имя компьютера.

Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

Допускается ввод нескольких адресов, разделенных запятой или точкой с запятой.

- Для регистрации события в системном журнале **Windows** установите флажок **Регистрировать в журнале событий Windows**.

4. По окончании настройки параметров нажмите на кнопку **Применить** или **ОК**.

В результате шаблон уведомления добавляется в папку **Шаблоны уведомлений**, отображается в таблице панели результатов и, если на закладке **Общие** установлен флажок **Уведомлять о событии**, по данному шаблону производится уведомление.

ГЛАВА 9. ПРЕДОТВРАЩЕНИЕ ЭПИДЕМИЙ

Антивирус Касперского позволяет фиксировать повышение вирусной активности на защищаемом Exchange-сервере и уведомлять об этом администратора и других пользователей. Эта возможность имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Вирусная активность определяется на основании данных антивирусной защиты сервера и позволяет фиксировать события следующих типов:

- **Обнаружен зараженный объект**.
- **Обнаружен подозрительный объект**.
- **Обнаружен поврежденный объект**.
- **Один и тот же вирус обнаружен несколько раз**.

Администратор устанавливает **порог вирусной активности** – максимально-допустимое количество событий заданного типа в течение ограниченного временного интервала. Если вирусная активность превышает установленный порог, осуществляется уведомление.

Уведомление может выполняться несколькими способами:

- рассылкой сообщений по электронной почте;
- рассылкой сообщений по сети средствами Net Send;
- регистрацией события в системном журнале **Windows** на компьютере, где установлен компонент Сервер безопасности.

  В этом случае доступ к информации осуществляется при помощи стандартного инструмента **Windows** просмотра и управления журналами **Просмотр событий**.

Порог вирусной активности, порядок уведомления, способ распространения и текст рассылаемых сообщений определяются администратором в параметрах *счетчика эпидемии*.

На основании параметров счетчика эпидемии в случае превышения установленного порога вирусной активности автоматически производится оповещение о возникновении угрозы вирусной эпидемии. По истечении заданного временного интервала значение счетчика обнуляется.

Значения всех счетчиков эпидемий обнуляются в случае перезагрузки компонента Сервер безопасности или операционной системы сервера, где установлен компонент.

Для каждого типа событий может быть создано несколько счетчиков эпидемий с различными значениями параметров.

По умолчанию уведомление о повышении вирусной активности не производится. Однако при установке Сервера безопасности формируется встроенный счетчик эпидемии. На основании счетчика может быть настроено уведомление об эпидемии.

Счетчики эпидемий размещаются в служебной папке **Счетчики вирусных эпидемий**. Данная папка входит в состав каждого узла, отображающего управляемый Exchange-сервер.

Перечень сформированных счетчиков эпидемий представлен в панели результатов в виде таблицы (см. рис. 43). Для каждого счетчика таблица отображает его имя и тип. Тип счетчика соответствует типу событий, отслеживаемых счетчиком

Подробно с параметрами счетчика эпидемии можно ознакомиться, вызвав окно настройки при помощи команды контекстного меню **Свойства** (см. п. 9.1 на стр. 93).

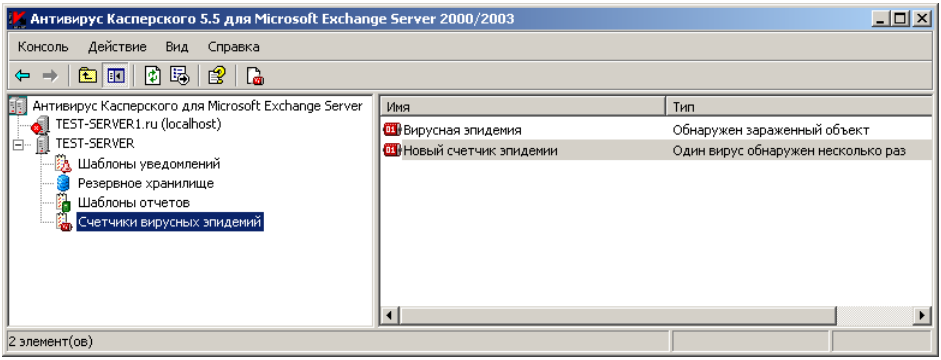


Рисунок 43. Папка **Счетчики вирусных эпидемий**

Администратор может создавать новые счетчики, просматривать и редактировать параметры существующих, переименовывать и удалять их при помощи команд контекстного меню.

Для того чтобы выполнялось уведомление о повышении вирусной активности,

1. Создайте счетчик эпидемии (см. п. 9.2 на стр. 95) или выберите существующий и настройте его параметры (см. п. 9.1 на стр. 93).
2. Установите флажок **Уведомлять об эпидемии** на закладке **Общие** окна настройки параметров счетчика эпидемии (см. рис. 44).

9.1. Просмотр и изменение параметров уведомления об эпидемии

Чтобы просмотреть или изменить параметры уведомления о вирусной эпидемии,

1. Выберите в дереве консоли папку **Счетчики вирусных эпидемий**.
2. В таблице, отображающей перечень сформированных счетчиков (см. рис. 43), выберите необходимый счетчик эпидемии.
3. Откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**.
4. В результате открывается окно настройки счетчика эпидемии **Свойства: <Имя счетчика>** (см. рис. 44).

   Окно состоит из закладок: **Общие**, **Текст**, **Уведомления** и полностью аналогично окну **<Новый счетчик>** (см. рис. 47). Изменение параметров уведомления выполняется так же, как и установка при создании (см. п. 9.2 на стр. 95).

   На закладке **Общие** (см. рис. 44) вы можете включить или отключить механизм распознавания вирусной активности на основании параметров счетчика, а также посмотреть и изменить:

   - имя счетчика;
   - тип события, возникновение которого отслеживает счетчик;
   - значение порога вирусной активности;
   - подробное описание счетчика.

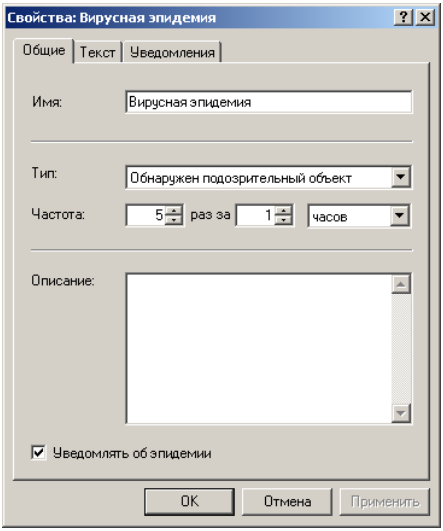


Рисунок 44. Изменение счетчика эпидемии. Закладка **Общие**

На закладке **Текст** (см. рис. 45) вы можете ознакомиться с шаблоном сообщения, которое направляется в качестве уведомления, и изменить значения его параметров.

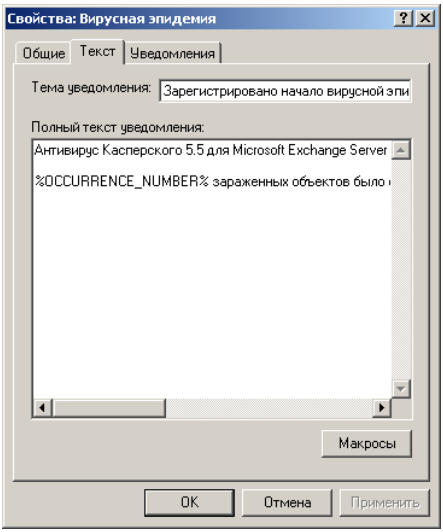


Рисунок 45. Изменение счетчика эпидемии. Закладка **Текст**

На закладке **Уведомления** (см. рис. 46) представлены способы уведомления, указаны адресанты и перечислены компьютеры-получатели сообщений (если выбраны соответствующие варианты уведомления). Вы можете указать другие способы уведомления и изменить значения параметров.

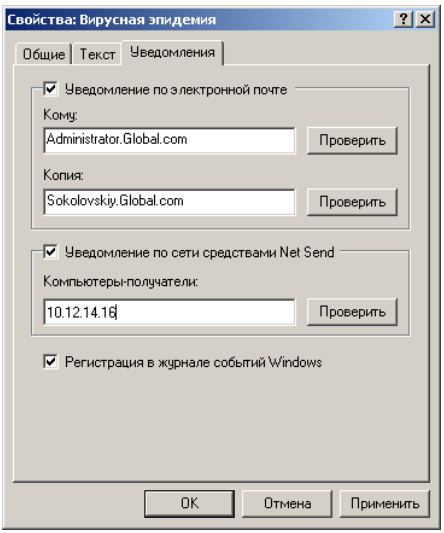


Рисунок 46. Изменение счетчика эпидемии. Закладка **Уведомления**

5. После внесения изменений, чтобы новые значения параметров вступили в силу, нажмите на кнопку **Применить** или **ОК**. Для выхода без сохранения изменений нажмите на кнопку **Отмена**.

9.2. Создание нового счетчика эпидемии

Для создания нового счетчика эпидемии,

1. Выберите в дереве консоли папку **Счетчики вирусных эпидемий**.
2. Откройте контекстное меню и воспользуйтесь командой **Новый счетчик** или аналогичным пунктом в меню **Действие**.

3. В результате открывается окно настройки нового счетчика эпидемии **<Новый счетчик>** (см. рис. 47). Установите необходимые значения для параметров, представленных на закладках окна.

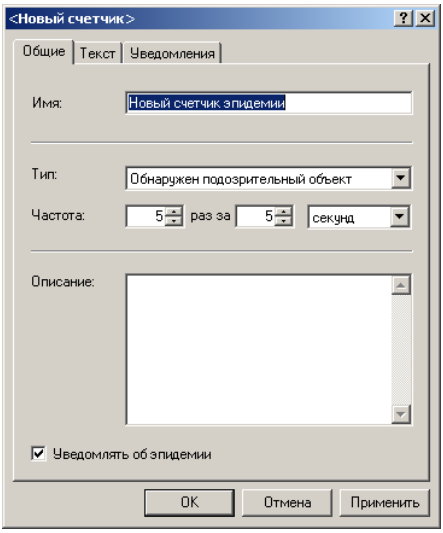


Рисунок 47. Счетчик эпидемии. Закладка **Общие**

На закладке **Общие** (см. рис. 47) выполните следующие действия:

- Введите имя счетчика в поле **Имя**.
- Укажите тип события, возникновение которого будет фиксировать счетчик.

  Для этого в поле **Тип** выберите необходимое значение из раскрывающегося списка. В списке представлены следующие значения:

  - **Обнаружен зараженный объект**.
  - **Обнаружен подозрительный объект**.
  - **Обнаружен поврежденный объект**.
  - **Один и тот же вирус обнаружен несколько раз**.
- Определите значение порога вирусной активности. Для этого в группе полей **Частота** установите значения параметров в следующей последовательности:

- максимально-допустимое количество событий заданного типа;
- временной интервал, в течение которого события должны быть зафиксированы;
- выберите единицу измерения времени: **секунды**, **минуты** или **часы**.

- Если необходимо, введите более подробное описание счетчика эпидемии в поле **Описание**.
- Укажите, будут формироваться уведомления на основании параметров данного счетчика или нет.

  Установите флажок **Уведомлять об эпидемии**, для того чтобы в случае превышения порога вирусной активности по событиям указанного типа уведомление выполнялось. Чтобы уведомление не производилось, снимите флажок.

На закладке **Текст** (см. рис. 48) создайте шаблон сообщения, которое будет направляться в качестве уведомления:

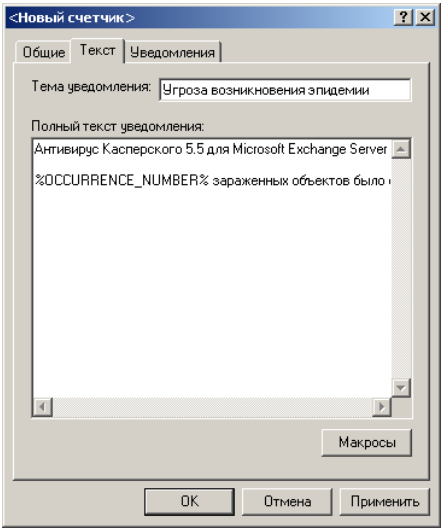


Рисунок 48. Счетчик эпидемии. Закладка **Текст**

- Введите краткое описание уведомления в поле **Тема уведомления**. Эта строка будет использоваться в качестве заголовка письма.

- Сформируйте текст сообщения в поле **Полный текст уведомления**. В состав сообщения может включаться информация о зарегистрированном событии. Для этого следует вставить в шаблон соответствующие макроподстановки, выбрав необходимые из раскрывающегося при помощи кнопки **Макросы** списка. Полный перечень макроподстановок содержит Приложение А на стр. 133.

На закладке **Уведомления** (см. рис. 49) выберите способы уведомления и определите соответствующие им значения параметров. Допускается выбор нескольких способов.

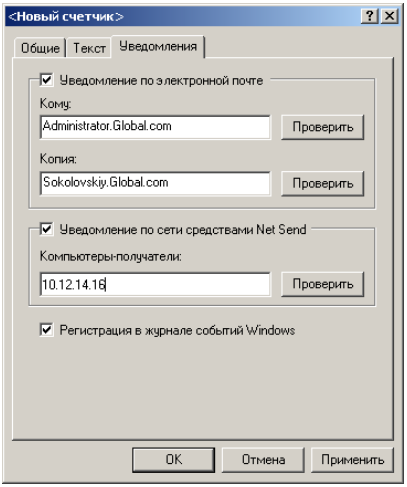


Рисунок 49. Счетчик эпидемии. Закладка **Уведомления**

- Для отправки сообщений через почтовый сервер установите флажок **Уведомление по электронной почте** и укажите электронные адреса получателей сообщения в полях **Кому** и **Копия**.

  Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

  Допускается ввод нескольких электронных адресов, разделенных точкой с запятой.

- Для отправки сообщений по сети с помощью службы Net Send установите флажок **Уведомление по сети**

средствами Net Send и укажите адреса компьютеров-получателей в поле **Компьютеры-получатели**.

В качестве адреса также можно использовать IP-адрес или NetBIOS-имя компьютера.

Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

Допускается ввод нескольких адресов, разделенных запятой или точкой с запятой.

- Для регистрации эпидемии в системном журнале **Windows** на компьютере, где установлен Сервер безопасности, установите флажок **Регистрация в журнале событий Windows**.

4. По окончании настройки параметров нажмите на кнопку **Применить** или **ОК**.

В результате:

- счетчик эпидемии добавляется в папку **Счетчики вирусных эпидемий** и отображается в таблице панели результатов;
- если на закладке **Общие** установлен флажок **Уведомлять об эпидемии**, будет осуществляться мониторинг вирусной активности по событиям заданного типа;
- в случае превышения установленного порога вирусной активности будет выполняться уведомление об угрозе возникновения вирусной эпидемии.

ГЛАВА 10. ОТЧЕТЫ

Антивирус Касперского предоставляет возможность получать отчеты о результатах антивирусной проверки сервера.

Отчет содержит информацию, зафиксированную в течение заданного отчетного периода, и предоставляет сведения:

- об обнаруженных зараженных объектах;
- об обнаруженных вирусах;
- об отправителях зараженных сообщений;
- о производительности антивирусной проверки:
    - общее количество обработанных объектов;
    - средняя скорость обработки объектов;
    - максимальная скорость обработки объектов;
    - интенсивность поступления зараженных объектов.

Отчет формируется автоматически, в соответствии с расписанием, или по запросу и может быть сохранен в каталоге, а также отправлен по электронной почте. Информация, представленная в отчете, сохраненном на диске и отправленном по почте, полностью совпадает, однако отличаются форматы отчетов, структура и способ просмотра.

Сохраняемый отчет создается в формате *htm-страницы* и имеет фреймовую структуру. Он размещается в каталоге, в состав которого входит предопределенный набор файлов, поддерживающих фреймовую структуру отчета и обеспечивающих его просмотр (см. п. 10.2 на стр. 109). Каталог создается с именем, отображающим дату и время создания отчета в формате **<ДД.ММ.ГГГГ ЧЧ-ММ-СС>**. Хранилищем отчетов на сервере по умолчанию является каталог **Reports**. Он создается в каталоге установки приложения при установке компонента Сервер безопасности. В качестве хранилища отчета может быть задан любой другой каталог по выбору администратора (см. п. 10.1.1 на стр. 104 и п. 10.1.2 на стр. 106). Срок хранения отчетов на сервере и размер хранилища отчетов не ограничены. Удаление отчетов осуществляется вручную через файловую систему.

Отправляемый по почте отчет является файлом формата *htm* и отсылается по электронной почте в виде вложения в сообщение. Сообщение содержит пояснительный текст: *Письмо создано приложением Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003. Присоединенный*

файл содержит отчет об антивирусной проверке за период с: <ДД.ММ.ГГГГ ЧЧ:ММ:СС> по: <ДД.ММ.ГГГГ ЧЧ:ММ:СС>.

Для просмотра отчетов используется браузер, установленный в системе по умолчанию.

Отчеты создаются на основании сформированных администратором **шаблонов отчетов**. В шаблоне задаются: отчетный период, расписание создания и формат отчета.

При установке Сервера безопасности создается встроенный шаблон отчета. На основании этого шаблона отчет о результатах антивирусной проверки сервера формируется первого числа каждого месяца за прошедшие 30 дней.

Шаблоны отчетов размещаются в служебной папке **Шаблоны отчетов**. Данная папка входит в состав каждого узла, отображающего управляемый Exchange-сервер.

Перечень сформированных шаблонов отчетов отображается в панели результатов в виде таблицы (см. рис. 50).

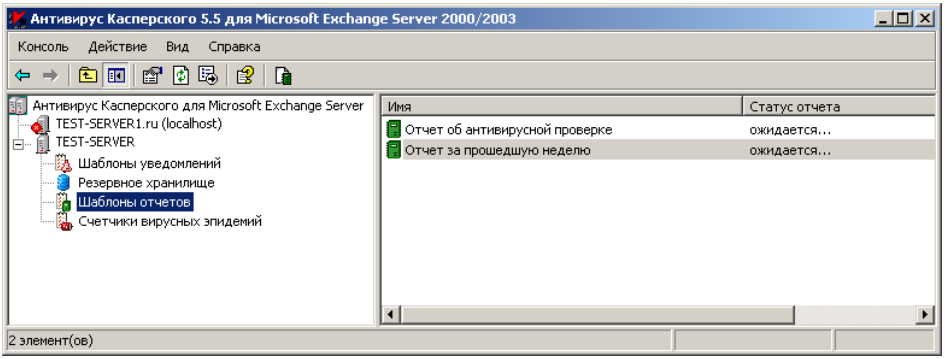


Рисунок 50. Папка **Шаблоны отчетов**

Для каждого шаблона таблица помимо имени содержит информацию о статусе отчета, формируемого по шаблону. В зависимости от того, на каком этапе находится создание отчета, статус отчета может иметь одно из следующих значений:

- **создается** – идет создание очередного отчета, запущенное по расписанию или по запросу;
- **ожидается** – ожидается создание очередного отчета в соответствии с расписанием;

- **не создавался** – ни одного отчета не было создано по данному шаблону (шаблон только что сформирован, создание отчетов по шаблону отключено).

Подробно с параметрами шаблона отчета можно ознакомиться, вызвав окно его настройки при помощи команды контекстного меню **Свойства** (см. п. 10.1.1 на стр. 104).

Администратор может создавать новые шаблоны, просматривать и редактировать параметры существующих, переименовывать и удалять их при помощи команд контекстного меню.

10.1. Получение отчета

Для получения отчета о результатах антивирусной проверки сервера

1. Создайте шаблон отчета (см. п. 10.1.2 на стр. 106) или выберите существующий и настройте его параметры (см. п. 10.1.1 на стр. 104).
2. Установите флажок **Формировать отчет** на закладке **Общие** окна настройки шаблона отчета (см. рис. 52).

В результате, в соответствии с заданной в расписании периодичностью формируется отчет.

Чтобы ознакомиться с результатами антивирусной проверки, следует просмотреть отчет за соответствующий отчетный период (см. п. 10.2 на стр. 109).

Предусмотрена возможность получения отчета по запросу, вне установленного расписанием времени, что может быть полезным для получения оперативной информации о состоянии системы антивирусной защиты сервера, например, в периоды вирусных эпидемий.

Для получения отчета о результатах антивирусной проверки сервера по запросу

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. В таблице, отображающей перечень сформированных шаблонов (см. рис. 50), выберите необходимый шаблон отчета.
3. Откройте контекстное меню и воспользуйтесь командой **Сформировать отчет** или аналогичным пунктом в меню **Действие**.

Отчет будет создан, только если формирование по шаблону отчета включено: установлен флажок **Формировать отчет** на закладке **Общие** окна настройки шаблона отчета (см. рис. 40).

Отчет формируется на основании сохраняемой приложением информации о результатах антивирусной проверки сервера. Сохраняются все результаты проверки: результаты проверки трафика, транзитной почты и фоновой проверки хранилищ. Для сокращения объема хранимой информации может быть ограничен срок ее хранения. По умолчанию он составляет один год.

Чтобы ограничить срок хранения информации о результатах антивирусной проверки сервера,

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. Откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**.
3. В открывшемся окне **Свойства: Шаблоны отчетов** (см. рис. 51):

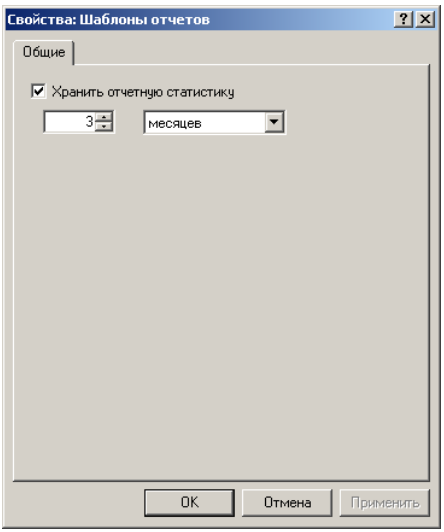


Рисунок 51. Настройка параметров отчета

- Установите флажок **Хранить отчетную статистику**.

- Укажите период хранения информации и выберите единицу измерения времени.

4. После внесения изменений, чтобы новые значения параметров вступили в силу, нажмите на кнопку **Применить** или **ОК**. Изменение значений произойдет в течение часа с момента применения. Для выхода без сохранения нажмите на кнопку **Отмена**.

10.1.1. Просмотр и настройка шаблона отчета

Чтобы просмотреть или изменить параметры шаблона отчета,

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. В таблице, отображающей перечень сформированных шаблонов (см. рис. 50), выберите необходимый шаблон отчета.
3. Откройте контекстное меню и воспользуйтесь командой **Свойства** или аналогичным пунктом в меню **Действие**.
4. В результате открывается окно настройки шаблона отчета **Свойства: <Имя шаблона>** (см. рис. 52).

   Окно состоит из закладок: **Общие**, **Параметры**, **Действия** и полностью аналогично окну **<Новый шаблон отчетов>** (см. рис. 55). Изменение параметров шаблона осуществляется так же, как и установка при создании (см. п. 10.1.2 на стр. 106).

   На закладке **Общие** (см. рис. 52) вы можете включить или отключить формирование отчета по шаблону, а также посмотреть и изменить имя шаблона и его подробное описание.

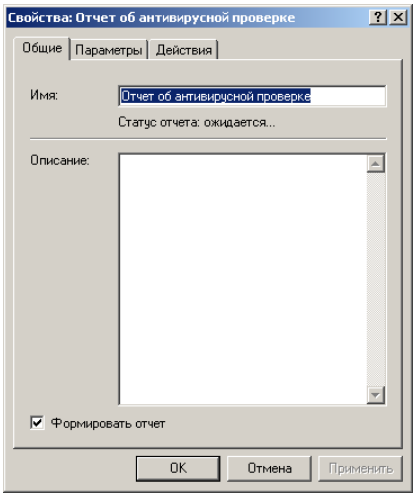


Рисунок 52. Изменение шаблона отчета. Закладка **Общие**

На закладке **Параметры** (см. рис. 53) вы можете посмотреть и изменить отчетный период и параметры расписания создания отчета.

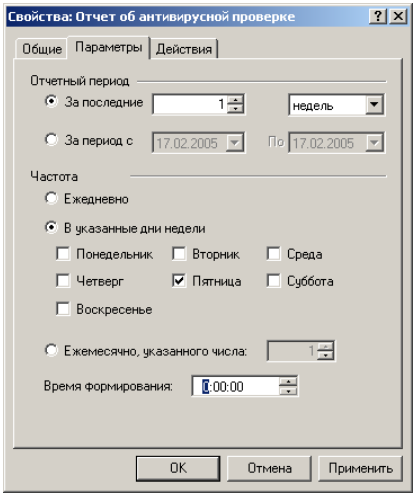


Рисунок 53. Изменение шаблона отчета. Закладка **Параметры**

На закладке **Действия** (см. рис. 54) указаны формы создания отчета, адрес каталога хранения отчета и адреса получателей

отчета по электронной почте (если выбраны соответствующие формы отчета). Вы можете выбрать другие формы создания отчета и изменить значения представленных параметров.

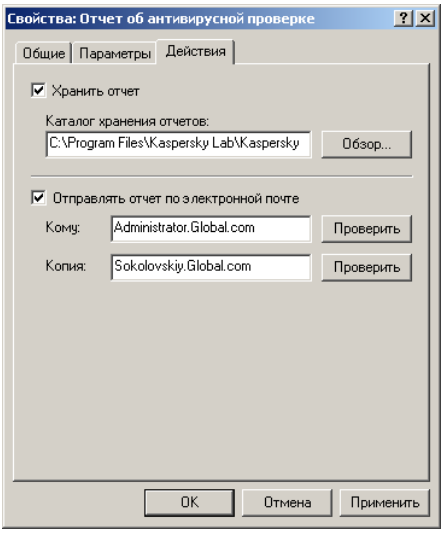


Рисунок 54. Изменение шаблона отчета. Закладка **Действия**

10.1.2. Создание шаблона отчета

Для создания нового шаблона отчета,

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. Откройте контекстное меню и воспользуйтесь командой **Новый шаблон отчетов** или аналогичным пунктом в меню **Действие**.
3. В результате открывается окно настройки шаблона отчета **<Новый шаблон отчетов>** (см. рис. 55), состоящее из закладок: **Общие**, **Параметры**, **Действия**. Установите необходимые значения для параметров, представленных на закладках.

   На закладке **Общие** (см. рис. 47) выполните следующие действия:

   - Введите имя шаблона в поле **Имя**.

- Если необходимо, введите более подробное описание отчета, который будет создаваться по шаблону, в поле **Описание**.
- Укажите, будут формироваться отчеты на основании данного шаблона или нет. Для этого установите или снимите флажок **Формировать отчет**.

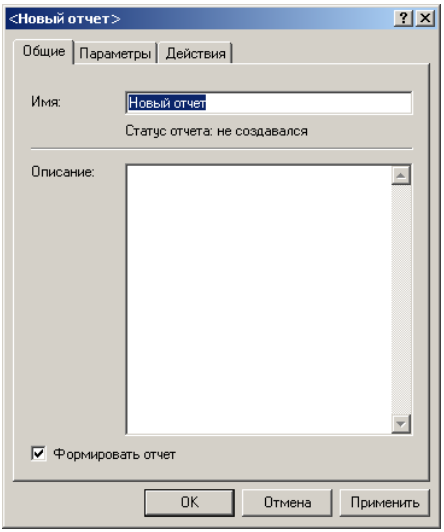


Рисунок 55. Шаблон отчета. Закладка **Общие**

На закладке **Параметры** (см. рис. 56) укажите отчетный период и установите параметры расписания создания отчета.

- При установке отчетного периода вы можете выбрать один из вариантов:
  - указать продолжительность временного интервала. В этом случае в отчете будет представлена информация за указанный период, начиная с даты и времени создания отчета. Для этого в группе полей **Отчетный период** выберите вариант **За последние** и укажите величину интервала и единицу измерения времени (часы, дни, недели, месяцы).
  - определить точные даты начала и конца отчетного периода. Для этого в группе полей **Отчетный период** выберите вариант **За период** и установите необходимые даты в полях **С** и **по**.

- Для создания расписания в разделе **Частота**:
  - Выберите частоту формирования отчета: **Ежедневно**, **В указанные дни недели** или **Ежемесячно, указанного числа**. Настройте параметры расписания, в соответствии с выбранной периодичностью.
  - Определите, в какое время будет запускаться создание отчета в поле **Время формирования**.

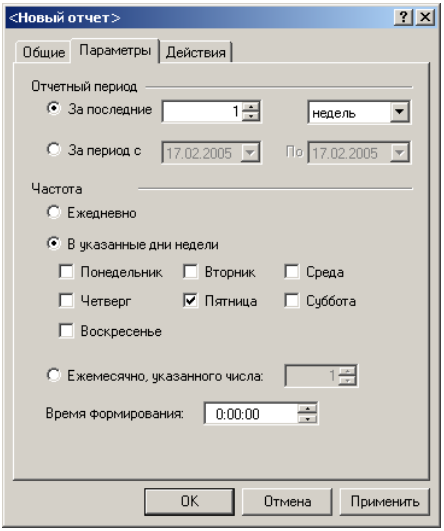


Рисунок 56. Шаблон отчета. Закладка **Параметры**

На закладке **Действия** (см. рис. 57) определите, в каком формате будет создаваться отчет, укажите каталог хранения отчетов и адреса рассылки.

- Для создания отчета и сохранения его на диске файловой системы сервера, установите флажок **Хранить отчет**.

  После этого укажите каталог, в котором сформированный отчет будет сохранен. По умолчанию это каталог **Reports**, расположенный на сервере в каталоге установки приложения. Вы можете указать другой каталог вручную, либо выбрав при помощи кнопки **Обзор**.

- Для создания отчета и отправки через почтовый сервер установите флажок **Отправлять отчет по электронной почте** и укажите электронные адреса получателей в полях **Кому** и **Копия**.

Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

Допускается ввод нескольких электронных адресов, разделенных точкой с запятой.

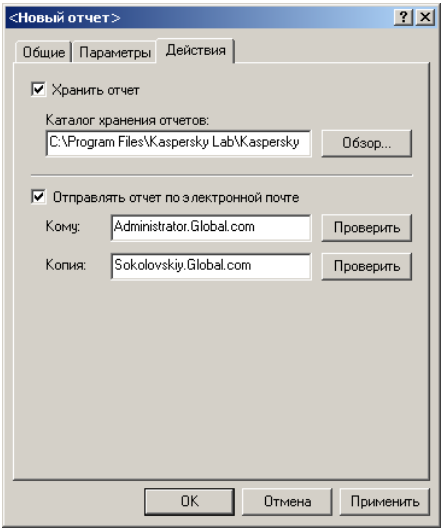


Рисунок 57. Шаблон отчета. Закладка **Действие**

4. По окончании настройки параметров нажмите на кнопку **Применить** или **ОК**.

В результате:

- Шаблон отчета добавляется в папку **Шаблоны отчетов** и отображается в таблице панели результатов;
- Если на закладке **Общие** установлен флажок **Формировать отчет**, на основании шаблона формируется отчет в заданное расписанием время и с установленной периодичностью. Отчет может быть также создан по запросу администратора.

10.2. Просмотр отчета

В соответствии с настройками шаблона сформированный отчет:

- сохраняется в виде каталога;

- отправляется по почте в виде вложенного в сообщение файла.

Для просмотра отчета, сохраненного в виде каталога

1. Зайдите в каталог размещения журналов. По умолчанию это каталог **Reports**, расположенный на сервере в каталоге установки приложения.
2. Выберите подкаталог, с именем, соответствующем дате и времени создания отчета в формате **<ДД.ММ.ГГГГ ЧЧ-ММ-СС>**.
3. Запустить файл *index.htm*, расположенный в выбранном подкаталоге.

В результате загружается браузер, установленный в системе по умолчанию. В главном окне браузера представлен отчет о результатах антивирусной проверки сервера (см. рис. 58). Сразу после загрузки отчет отображает общие результаты проверки. Отчетный период указан в заголовке.

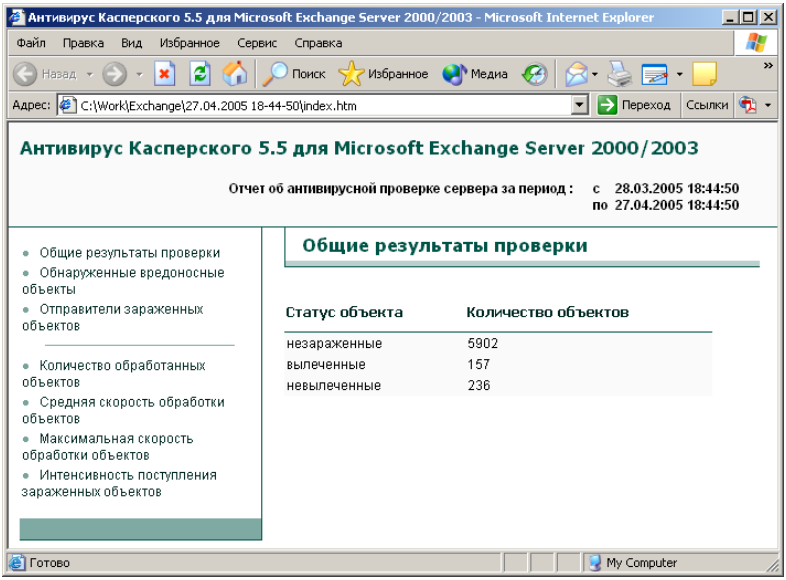


Рисунок 58. Просмотр отчета, сохраненного в виде каталога

Отчет имеет фреймовую структуру. В левой части отображается перечень разделов отчета – оглавление, в правой части – заголовок и содержание выбранного раздела.

Для просмотра раздела следует выбрать его в оглавлении, в результате содержание раздела загружается в правой части экрана.

Перечень разделов отчета и описание представленной в каждом из них информации приводится в таблице.

Название раздела	Содержание раздела
Общие результаты проверки	Количество объектов, обнаруженных в результате антивирусной проверки, для каждого статуса отдельно.
Обнаруженные вредоносные объекты	Список различных вирусов, обнаруженных в зараженных объектах, и количество обнаружений каждого из них.
Отправители зараженных объектов	Электронные адреса отправителей сообщений, в которых были обнаружены зараженные объекты и общее количество вирусов, поступивших с каждого адреса.
Количество обработанных объектов	Общее количество объектов, проверенных Антивирусом Касперского в течение отчетного периода.
Средняя скорость обработки объектов	Среднее за отчетный период количество объектов, проверявшихся в секунду.
Максимальная скорость обработки объектов	Максимальная скорость проверки объектов в секунду достигавшаяся в течение отчетного периода.
Интенсивность поступления зараженных объектов	Среднее за отчетный период количество зараженных объектов, обнаруженных в секунду.

Для просмотра отчета, доставленного по почте

откройте вложенный в сообщение файл *index.htm.*

В результате загружается браузер, установленный в системе по умолчанию. В главном окне браузера представлен отчет о результатах антивирусной проверки сервера (см. рис. 59).

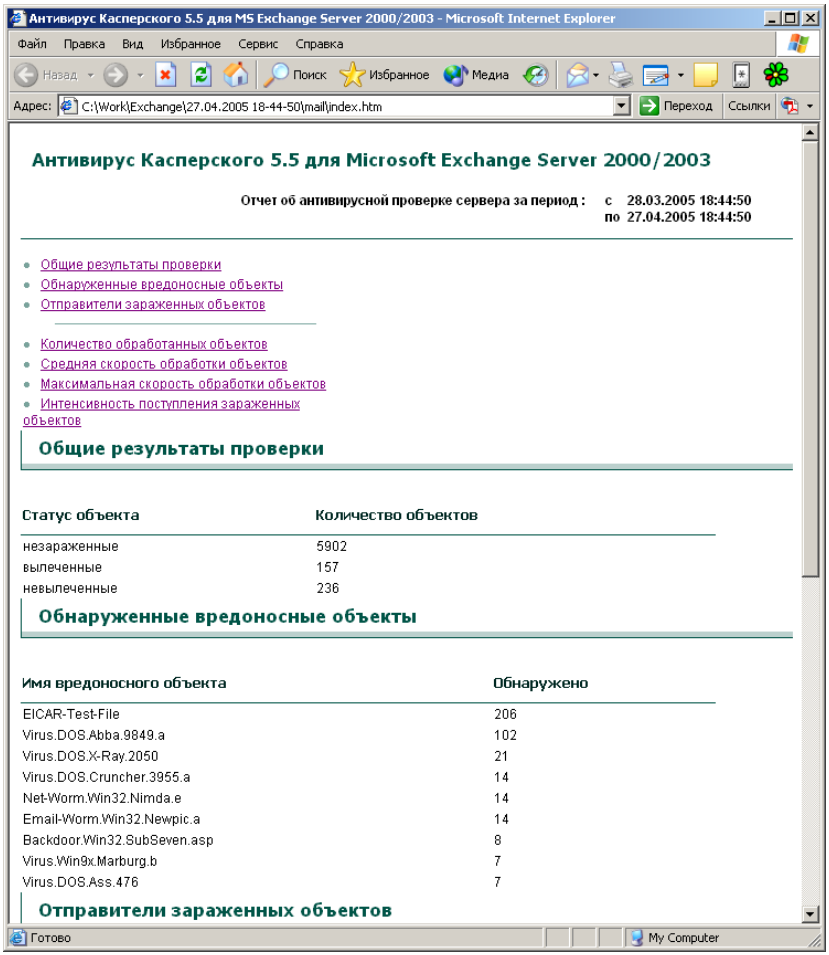


Рисунок 59. Просмотр отчета, отправленного по почте

В верней части отчета представлен список разделов – оглавление. За ним следуют разделы с входящей в их состав информацией. Разделы расположены последовательно, в порядке, соответствующем оглавлению.

Состав разделов и представленная в них информация те же, что и в отчете, сохраненном на диске.

Для последовательного просмотра отчета используйте полосу прокрутки.

Чтобы переместиться в начало нужного раздела, выберите его в оглавлении.

ГЛАВА 11. ЖУРНАЛЫ СОБЫТИЙ ПРИЛОЖЕНИЯ

Антивирус Касперского позволяет проводить полную диагностику своей работы и регистрировать зафиксированные события в журнале приложений операционной системы Windows и собственных журналах приложения.

Полнота информации, выводимой в журналы, зависит от установленных в параметрах приложения уровней диагностики (см. п. 11.1 на стр. 115).

Просмотр событий, зарегистрированных в журнале приложений Windows, осуществляется при помощи стандартного сервиса Windows **Просмотр событий**. В графе **Источник** для Антивируса Касперского прописывается строка **KAVE**.

Для корректного отображения событий, зарегистрированных в журнале приложений Windows, необходимо чтобы в параметрах сервиса Windows **Язык и региональные стандарты** в качестве **Языка программ, не поддерживающих Юникод** был выбран язык, совпадающий с языковой версией Антивируса.

Журналы событий Антивируса Касперского ведутся в двух форматах и в зависимости от формата имеют следующую структуру имен:

kavscmesrvДАТА.log – основной журнал событий приложения. В качестве *ДАТА* в названии файла приводится дата его создания в формате ***ГГГГММДД***. Например: *kavscmesrv20050410.log*.

Если в момент заполнения журнала он недоступен для записи, например, открыт администратором на редактирование, Антивирус Касперского сформирует новый файл с дополнительным постфиксом к его имени. Например: *kavscmesrv 20040410_1.log*.

kavscmesrv.rawДАТА.log и *store.rawДАТА.log* – журналы, содержащие информацию в неотформатированном виде. Событие регистрируется в *raw*-журнале, если по каким-либо причинам его не удалось записать в основной журнал.

Новый журнал по умолчанию создается раз в месяц. Срок хранения журналов не ограничен, однако, ограничено количество журналов одного формата. По умолчанию одновременно может храниться не более 5 журналов одинакового формата. При создании нового журнала, если установленное ограничение превышено, удаляется наиболее старый журнал такого же формата. Периодичность создания журналов и ограничение на их количество могут быть изменены (см. п. 11.2 на стр. 117).

Запись информации в журнал событий Антивируса Касперского производится в конец самого нового файла. Размер журналов не ограничен.

Просмотр журналов событий Антивируса Касперского осуществляется через файловую систему.

Хранилищем журналов по умолчанию является каталог **Log**. Он создается на сервере в каталоге установки приложения при установке компонента Сервер безопасности. В качестве хранилища журналов может быть задан любой другой каталог по выбору администратора (см. п. 11.2 на стр. 117).

Настройка параметров журналов Антивируса Касперского осуществляется на закладке **Диагностика** окна настройки параметров приложения **Общие параметры** (см. рис. 60). Чтобы открыть окно, следует воспользоваться гиперссылкой Общие параметры.

11.1. Настройка уровня диагностики

Объем и полнота информации, выводимой в журналы, зависит от установленных в параметрах приложения уровней диагностики для каждого из модулей программы. Если модуль состоит из нескольких компонентов, уровень диагностики устанавливается для каждого компонента отдельно.

Предусмотрены следующие уровни диагностики:

- **Не выводить**: не записывать в журналы никакой информации.
- **Минимальный**: фиксировать в журналах только основные события.
- **Средний**: записывать помимо основных событий ряд дополнительных, характеризующих работу Антивируса более детально.
- **Максимальный**: выводить в журналы максимально полную информацию о работе модуля, за исключением отладочных сообщений.
- **Отладочный**: записывать в журналы всю информацию, в том числе и отладочную.

Для настройки уровней диагностики

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.

2. В открывшемся окне **Общие параметры** выберите закладку **Диагностика** (см. рис. 60).

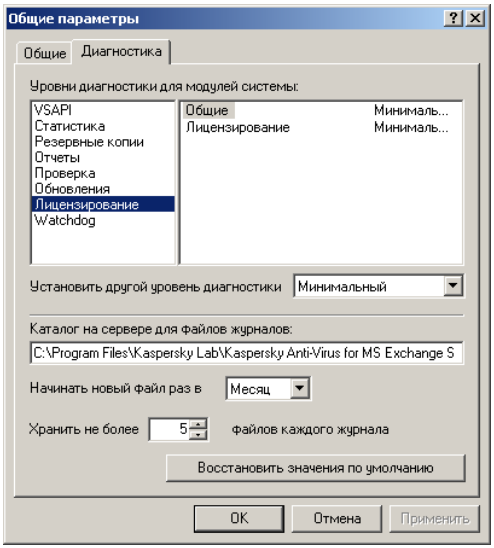


Рисунок 60. Закладка **Диагностика**

3. На закладке в разделе **Уровни диагностики для модулей системы** представлена таблица. В левой части таблицы приведены все модули, входящие в состав программы. В правой части таблицы входящие в состав выбранного модуля компоненты и уровень диагностики для каждого из них.

   Выберите в левой части таблицы модуль, после этого в правой части нужный компонент. Установите необходимый уровень диагностики при помощи раскрывающегося списка.

   Установите нужные уровни диагностики для каждого модуля.

4. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

11.2. Настройка параметров журнала

Для настройки параметров журнала

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.
2. В открывшемся окне **Общие параметры** выберите закладку **Диагностика** (см. рис. 60).
3. В поле **Каталог на сервере для файлов журналов** введите путь к новому каталогу.
4. Установите периодичность создания журналов в поле **Начинать новый файл раз в**, выбрав нужное значение из раскрывающегося списка.
5. Укажите, какое количество файлов журналов одного формата может храниться. Для этого установите нужное значение в поле **Хранить не более [NN] файлов каждого журнала**.
6. По окончании настройки нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

ГЛАВА 12. ЛИЦЕНЗИОННЫЕ КЛЮЧИ

При покупке Антивируса Касперского между вами и Лабораторией Касперского заключается лицензионное соглашение. На его основании вам предоставляется право использовать данное программное обеспечение в течение определенного периода для защиты указанного количества почтовых ящиков.

Защите подлежат как почтовые ящики, так и общие папки. Таким образом, при работе в среде Microsoft Exchange Server не требуется приобретение отдельной лицензии на защиту общих папок.

В течение лицензионного периода 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.

Приложение устанавливает наличие лицензионного соглашения по **лицензионному ключу**, который является неотъемлемой частью любого продукта Лаборатории Касперского.

Без лицензионного ключа Антивирус Касперского НЕ РАБОТАЕТ!

У приложения может быть только один действующий лицензионный ключ. В нем содержатся ограничения на использование Антивируса Касперского, которые могут быть проверены специальными механизмами приложения. В случае обнаружения нарушений лицензионного соглашения:

- ограничивается функциональность приложения;

- в журналы событий заносится запись о зафиксированном нарушении;
- если настроены параметры оповещения, производится уведомление о нарушении по электронной почте (см. п. 12.3 на стр. 123).

Количество объектов, непроверенных в период ограничения функциональности из-за нарушения условий лицензии, можно посмотреть в разделе отчета **Общие результаты проверки** (см. п. 10.2 на стр. 109). Для проверки этих объектов мы рекомендуем после восстановления антивирусной функциональности приложения (установки нового лицензионного ключа) запустить фоновую проверку.

При превышении установленного лицензией ограничения по количеству защищаемых почтовых ящиков отключается антивирусная функциональность приложения. Доступны только сервисы управления, обеспечивающие настройку параметров приложения, в частности, установку лицензионных ключей и выбор защищаемых хранилищ.

Регулировать количество защищаемых почтовых ящиков возможно исключением из проверки хранилищ, почтовые ящики которых не будут проверяться (см. п. 12.6 на стр. 126).

Предварительное уведомление о лицензионном ограничении по почтовым ящикам производится, когда количество ящиков на почтовом сервере достигает 90% от установленного в лицензии ограничения.

Мы рекомендуем приобрести дополнительные лицензии для защиты всех почтовых ящиков, поскольку наличие незащищенных хранилищ увеличивает вероятность проникновения и распространения вирусов через почтовую систему.

По окончании действия коммерческой лицензии функциональность Антивируса Касперского сохраняется за исключением возможности обновления антивирусных баз. Приложение по-прежнему осуществляет антивирусную проверку трафика и фоновую проверку хранилищ, но при лечении зараженных объектов используются устаревшие версии антивирусных баз. В такой ситуации сложно гарантировать стопроцентную антивирусную защиту от новых вирусов, которые появятся после окончания действия лицензии Антивируса.

За две недели до истечения срока действия лицензии во время работы приложения отсылается предупреждающее уведомление. В нем содержится информация о дате окончания установленного лицензионного ключа.

Мы рекомендуем вам своевременно продлевать лицензию на использование Антивируса Касперского.

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

Чтобы продлить лицензию, вам необходимо приобрести и установить новый лицензионный ключ для Антивируса Касперского. Для этого:

1. Свяжитесь с компанией, у которой вы купили продукт, и приобретите лицензионный ключ на использование Антивируса Касперского 5.5 для Microsoft Exchange Server 2000/2003.

или:

Приобретите лицензионный 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 лицензионный ключ по электронному адресу, который был указан вами в форме заказа.

2. Установите лицензионный ключ (см. п. 12.4 на стр. 124).

Вы можете установить два ключа: текущий и резервный. Текущий ключ действует на данный момент времени. В программе не может быть больше одного ключа со статусом "текущий". Резервный ключ активируется автоматически сразу после окончания срока действия текущего.

В некоторых случаях, например, при расторжении договора о продаже, или изменении лицензионных ограничений, Лаборатория Касперского прерывает заключенное лицензионное соглашение. В этом случае серийный номер лицензионного ключа помещается в список аннулированных ключей, так называемый "черный список".

Если текущий лицензионный ключ, обнаружен в "черном списке", резервный ключ не активизируется, из всей функциональности приложения будут доступны только сервисы управления и обновления антивирусных баз.

12.1. Информация о лицензии

Для просмотра информации о лицензии

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.

2. В открывшемся окне **Общие параметры** выберите закладку **Общие** (см. рис. 61).

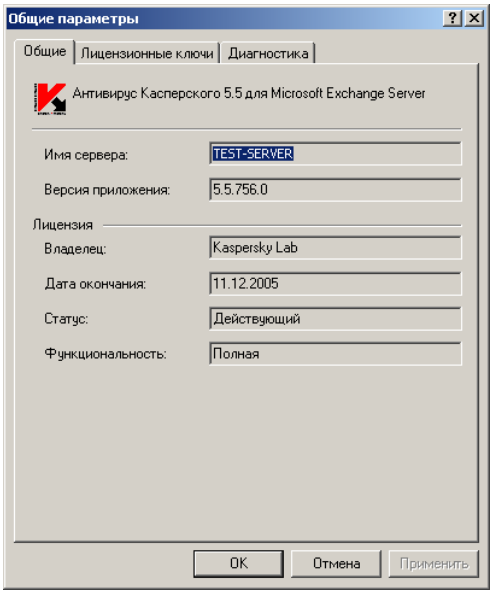


Рисунок 61. Просмотр информации о лицензии

На закладке представлена следующая информация:

- имя Exchange-сервера, на котором установлен компонент Антивируса Касперского Сервер безопасности;
- номер установленной версии приложения;
- информация о владельце лицензии;
- дата окончания лицензии;
- статус текущего лицензионного ключа;
- объем доступной функциональности приложения, соответствующий текущему лицензионному ключу:
  - **Полная**. Приложение работает в объеме, предусмотренном лицензионным соглашением.
  - **Не доступно обновление**. Не доступно обновление антивирусных баз. Приложение выполняет антивирусную проверку и лечит обнаруженные зараженные объекты на основании устаревшей версии

антивирусных баз. Возможно, истек срок действия лицензии.

- **Только управление**. Доступны только сервисы управления, обеспечивающие настройку параметров приложения, в частности установку лицензионных ключей и выбор защищаемых хранилищ. Возможно, превышено лицензионное ограничение по количеству защищаемых почтовых ящиков, или закончился срок действия пробного лицензионного ключа (trial).
- **Только обновление**. Доступны только функция обновления антивирусных баз. Возможно, базы были повреждены, поэтому антивирусная проверка осуществляться не может.

12.2. Информация о лицензионных ключах

Для просмотра информации об установленных для приложения лицензионных ключах

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.
2. В открывшемся окне **Общие параметры** выберите закладку **Лицензионные ключи** (см. рис. 62).

   На закладке представлена подробная информация об установленных для приложения текущем и резервном лицензионных ключах, а также параметры лицензионных уведомлений.

   В разделе **Текущий лицензионный ключ** отображаются данные о текущем лицензионном ключе:

   - Статус.
   - Тип, установленного лицензионного ключа, например, **коммерческий**, **пробный**.
   - Информация о владельце лицензии.
   - Дата окончания срока действия.
   - Серийный номер.

- Максимальное количество защищаемых почтовых ящиков.

В разделе **Резервный лицензионный ключ** отображаются данные о резервном лицензионном ключе:

- Дата окончания срока действия.
- Серийный номер.
- Максимальное количество защищаемых почтовых ящиков.

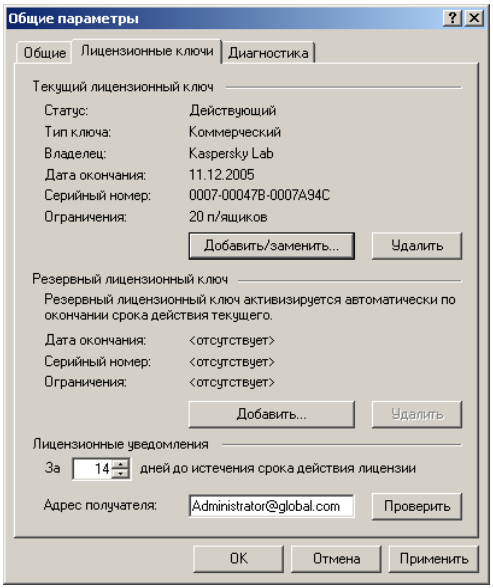


Рисунок 62. Просмотр информации о лицензионных ключах. Настройка лицензионных уведомлений

12.3. Лицензионные уведомления

Приложение выполняет проверку соблюдения условий лицензии периодически и после каждого обновления антивирусных баз.

По результатам проверки в случаях если:

- срок действия текущего лицензионного ключа истекает через несколько дней;
- срок действия лицензионного ключа истек;
- текущий лицензионный ключ находится в "черном списке";

- количество ящиков на почтовом сервере составляет 90% от установленного в лицензии ограничения;
- количество ящиков на почтовом сервере превышает установленное в лицензии ограничение;

заносится запись в журналы приложения и, если настроены параметры уведомления, отправляется сообщение по электронной почте.

По умолчанию уведомление осуществляется за 14 дней до истечения срока действия лицензии. Вы можете установить более ранний или более поздний срок уведомления.

Для настройки лицензионных уведомлений

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.
2. В открывшемся окне **Общие параметры** выберите закладку **Лицензионные ключи** (см. рис. 62).

   В разделе **Лицензионные уведомления** укажите:

   - за сколько дней до истечения срока действия лицензии выполнять лицензионные уведомления;
   - электронный адрес получателя лицензионный уведомлений.

   Проверить корректность адреса можно при помощи кнопки **Проверить**. На указанный адрес будет отправлено сообщение.

   Допускается ввод нескольких электронных адресов, разделенных точкой с запятой.
3. После ввода адреса и его проверки нажмите на кнопку **Применить** или **ОК**.

12.4. Установка лицензионного ключа

В приложении одновременно может быть установлено два лицензионных ключа: текущий и резервный. Резервный лицензионный ключ становится текущим автоматически по окончании срока действия текущего лицензионного ключа.

Если текущий лицензионный ключ обнаружен в "черном списке", резервный ключ не активируется. Необходимо заменить текущий лицензионный ключ. Вы можете установить резервный ключ в качестве текущего вручную.

Предусмотрена возможность замены текущего лицензионного ключа, что исключает возможность ограничения функциональности приложения, если замена выполняется как последовательное удаление и установка нового ключа.

Если для приложения не установлено ни одного ключа, возможна установка только текущего лицензионного ключа.

Для установки или замены лицензионного ключа

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.
2. В открывшемся окне **Общие параметры** выберите закладку **Лицензионные ключи** (см. рис. 62).
3. На закладке Лицензионные ключи:
   - если вы устанавливаете или заменяете текущий лицензионный ключ, в разделе **Текущий лицензионный ключ** нажмите на кнопку **Добавить/ заменить**.
   - если вы устанавливаете или заменяете резервный лицензионный ключ, в разделе **Текущий лицензионный ключ** нажмите на кнопку **Добавить**.
4. В открывшемся окне выбора файла укажите файл ключа, который необходимо установить (*.key).

   По истечении срока действия пробного лицензионного ключа вы не сможете установить второй пробный лицензионный ключ.

   В результате информация об установленном лицензионном ключе отображается в полях соответствующего раздела.
5. Закройте окно **Общие параметры** при помощи кнопки **Применить** или **ОК**.

12.5. Удаление лицензионного ключа

При удалении текущего лицензионного ключа автоматически удаляется установленный резервной ключ.

Для удаления лицензионного ключа

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Общие параметры в панели результата.
2. В открывшемся окне **Общие параметры** выберите закладку **Лицензионные ключи** (см. рис. 62).
3. На закладке Лицензионные ключи:
   - если вы удаляете резервный лицензионный ключ, в разделе **Резервный лицензионный ключ** нажмите на кнопку **Удалить**.
   - если вы удаляете текущий лицензионный ключ, в разделе **Текущий лицензионный ключ** нажмите на кнопку **Удалить**.
4. Подтвердите удаление лицензионного ключа в открывшемся предупреждающем сообщении.

   В результате информация в полях соответствующего раздела обновляется.
5. Закройте окно **Общие параметры** при помощи кнопки **Применить** или **ОК**.

12.6. Незащищаемые хранилища

Программа рассчитана на защиту того количества почтовых ящиков, которое указано в приобретенной вами лицензии. Если этого количества недостаточно, вам придется выбрать, с каких почтовых ящиков снять защиту и разместить их в хранилища, которые не будут подвергаться антивирусной проверке.

По умолчанию защите подлежать все общие папки, сформированные на защищаемом почтовом сервере. Вы можете снять защиту с общих папок, если считаете, что их проверка избыточна.

Для того чтобы снять антивирусную защиту с хранилища или общей папки,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой Антивирусная защита в панели результата.
2. В открывшемся окне **Антивирусная защита** выберите закладку **Защищаемая почта** (см. рис. 63).

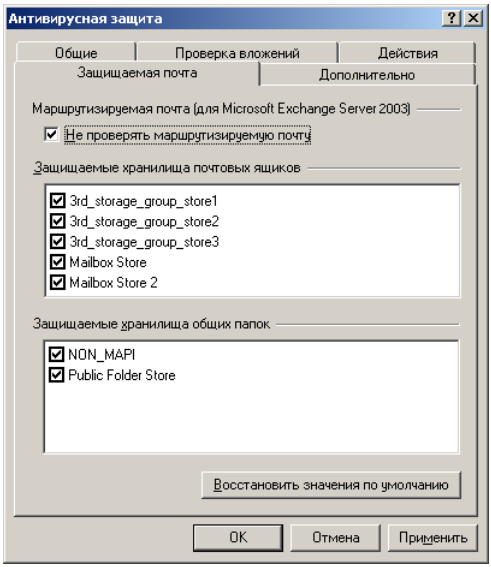


Рисунок 63. Выбор незащищенных хранилищ

- В разделе **Защищаемые хранилища почтовых ящиков** снимите флажки рядом с именами хранилищ, почтовые ящики которых не будут проверяться на присутствие вирусов.

  Представленный список содержит полный перечень сформированных на защищаемом Exchange-сервере хранилищ. По умолчанию все они подлежат антивирусной защите.

Отправляемые с почтовых ящиков незащищаемых хранилищ, поступающие и хранящиеся в них сообщения не будут проверяться на присутствие вирусов.

- В разделе **Защищаемые хранилища общих папок** снимите флажки рядом с именами хранилищ общих папок, содержимое которых не будет проверяться на присутствие вирусов.

  Представленный список содержит полный перечень созданных на защищаемом Exchange-сервере хранилищ общих папок. По умолчанию все они подлежат антивирусной защите.

3. Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **ОК**.

Восстановить значения параметров, предусмотренные по умолчанию, вы можете при помощи кнопки **Восстановить значения по умолчанию**.

В результате почтовые ящики, размещенные в незащищенных хранилищах, не будут учитываться при проверке соблюдения лицензионных ограничений.

ГЛАВА 13. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В данной главе мы осветим наиболее распространенные вопросы пользователей 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?

Детектирование 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), Лаборатория Касперского считает, что задача Антивируса – обеспечивать реальную антивирусную безопасность пользователей.

Антивирус Касперского позволяет опытному пользователю ускорить антивирусную проверку путем отключения антивирусной проверки различных типов файлов. Однако не стоит забывать, что это приводит к снижению уровня безопасности.

Антивирус Касперского распознает более семисот форматов архивированных и сжатых файлов. Это очень важно для антивирусной безопасности, поскольку каждый из распознаваемых форматов может содержать исполняемый вредоносный код.

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

Без лицензионного ключа Антивирус Касперского не работает.

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

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

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

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

Вопрос: мой Антивирус не работает.

Что мне делать?

Прежде всего, убедитесь, не описан ли метод решения вашей проблемы в данной документации, в частности в этом разделе, или на нашем сайте.

Также мы рекомендуем обратиться к фирме, где вы приобрели Антивирус Касперского или написать письмо в Службу технической поддержки (support@kaspersky.com) или по адресу, указанному в информации о лицензионном ключе.

Чтобы ваш запрос был обработан как можно скорее:

1. В заголовке сообщения укажите операционную систему вашего компьютера, название продукта Лаборатории Касперского, который вы используете, и проблему. Например: **Microsoft Windows 2000, Антивирус Касперского 5.5 для Microsoft Exchange Server 2000/2003, не работает обновление антивирусных баз**.
2. Пишите сообщения в виде plain text.

3. В начале сообщения укажите:
   - версию операционной системы и установленного пакета обновлений;
   - версию Microsoft Exchange Server и установленного пакета обновлений;
   - версию дистрибутива Антивируса Касперского и номер вашей лицензии.
4. Кратко, но наиболее понятно опишите проблему. Помните, что Служба поддержки на момент чтения вашего письма ещё ничего не знает о вашей проблеме и сможет помочь вам, только полностью поняв и воспроизведя ее.
5. Отправьте в Службу технической поддержки следующие данные, предварительно запаковав их в один архив:
   - текущие журналы событий приложения с уровнем диагностики для каждого из модулей приложения **Отладочный**;
   - лицензионный ключ.
6. Обязательно укажите в письме информацию о наличии:
   - очень старого или нового процессора, нескольких процессоров;
   - памяти меньше, чем 256 МБ или больше 2 ГБ.
7. Укажите примерный размер дневного трафика и бывают ли пики нагрузки.

Вопрос: Зачем нужны ежедневные 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 бессилен перед новой угрозой. Для того чтобы не стать жертвой новых вирусов, необходимо обновлять антивирусные базы ежедневно.

Лаборатория Касперского с каждым годом увеличивает частоту обновления антивирусных баз. Сейчас они обновляются каждый час.

Дополнительной функцией является задача обновления программных модулей Антивируса, в которых исправляются обнаруженные уязвимости или предоставляются новые функциональные возможности.

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, и дата баз – более поздняя, чем день окончания лицензии на использование продукта, Антивирус Касперского не будет использовать такие базы.

Вопрос: я использую прокси-сервер и у меня не работает обновление. Что делать?

Недоступность получения обновлений при работе через прокси-сервер может быть вызвана следующими причинами:

- Неправильные сетевые настройки.

  При настройке сервиса обновления есть два пути установки сетевых настроек: использование настроек Microsoft Internet Explorer или использование индивидуальных настроек. Сервис обновления не всегда корректно использует настройки Microsoft Internet Explorer, а именно в случаях:

  - на компьютере не настроен интернет;
  - настройки Microsoft Internet Explorer не доступны, если не залогинен ни один пользователь;
  - прокси-сервер требует авторизации.

  Во всех случаях следует задавать сетевые настройки непосредственно в настройках сервиса обновления.

- Использование прокси-сервера, тип которого не поддерживается сервисом обновления Антивируса Касперского.

  Сервис обновления не работает через Kerio WinRoute, так как WinRoute не полностью реализует протокол http 1.0. В данном случае рекомендуется использовать любой другой прокси-сервер.

ПРИЛОЖЕНИЕ А. ТАБЛИЦА МАКРОПОДСТАНОВОК

Макрос	Значение макроса
%OCURRENCE_NUMBER%	общее количество зарегистрированных событий
%PERIOD_LENGTH%	продолжительность периода
%PERIOD_TYPE%	единицы измерения временного периода (секунды, минуты, часы, дни)
%VIRUS_NAME%	имя обнаруженного вируса (в уведомлениях о вирусных эпидемиях заполняется только для события **Один и тот же вирус обнаружен несколько раз**)
%ACTION%	действие, которое было выполнено над объектом при антивирусной проверке
%AVBASES_LAST_UPDATE%	дата последнего обновления антивирусных баз
%CC%	список получателей копий сообщения.
%CONTENT_CODEPAGE%	кодовая страница содержимого объекта сообщения
%CONTENT_LENGTH%	размер объекта
%CONTENT_TYPE%	информация о MIME-типе объекта
%DATABASE_NAME%	имя базы данных Microsoft Exchange Server 2000, в которой обнаружен объект
%FROM%	отображаемое имя отправителя
%MAILBOX_NAME%	имя почтового ящика, в котором обнаружен объект
%MESSAGE_URL_NAME%	полное имя сообщения, в котором обнаружен объект

Макрос	Значение макроса
%OBJECT_NAME%	имя вложения, для OLE-объектов и писем – не определено
%OBJECT_TYPE%	тип объекта: письмо, файл, OLE-объект
%RECV_TIME%	время получения сообщения
%SCANNER_VERSION%	номер версии приложения
%SCANNER_VENDOR%	имя компании производителя приложения – Лаборатория Кассперского
%SENT_REPRESENTING_NAME%	отображаемое имя для пользователя обмена сообщениями, предоставленное отправителем
%SERVER_NAME%	имя сервера, на котором обнаружен объект (при работе приложения на кластере серверов имя виртуального сервера, а в уведомлениях о вирусных эпидемиях имя узла кластера)
%SUBJECT%	тема сообщения
%SUBMIT_TIME%	время отправки сообщения
%TO%	список получателей сообщения

ПРИЛОЖЕНИЕ В. ГЛОССАРИЙ

В документации встречаются термины и понятия, специфичные для области антивирусной защиты. Глоссарий представляет собой словарь определений данных понятий. Для удобства пользования статьи глоссария представлены в алфавитном порядке.

А

Антивирусные базы – базы данных, формируемые специалистами Лаборатории Касперского и содержащие подробное описание всех существующих на текущий момент вирусов, способов их обнаружения и лечения. Базы постоянно обновляются в Лаборатории Касперского по мере появления новых вирусов. Это требует от администратора проведения регулярного обновления антивирусных баз, используемых приложением.

В

Восстановление – перемещение резервной копии объекта из *резервного хранилища* в указанный администратором каталог, расшифровка и сохранение под заданным именем. Восстановленный объект имеет тот же формат, с каким объект поступил на обработку Антивирусу Касперского.

З

Зараженный (инфицированный) объект – объект, внутри которого содержится вредоносный код. Мы не рекомендуем работать с такими объектами, поскольку это может привести к заражению компьютера.

К

Консоль управления – компонент Антивируса Касперского. Предоставляет пользовательский интерфейс к административным сервисам приложения и позволяет осуществлять настройку и управление серверной частью. Модуль управления выполнен в виде компонента расширения к Microsoft Management Console (MMC).

Л

Лечение объектов – способ обработки *зараженных объектов*, в результате которого происходит полное или частичное восстановление данных, либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей *антивирусных баз*. В случае если лечение является первичным действием над объектом (самое первое действие над объектом сразу после его обнаружения), то перед его

выполнением создается *резервная копия* объекта. В процессе лечения часть данных может быть утеряна. Для восстановления объекта до первоначального состояния может быть использована резервная копия объекта.

Лицензионный ключ – файл с расширением **.key*, который является вашим личным "ключом", необходимым для работы с Антивирусом Касперского. Лицензионный ключ включен в поставку продукта, если вы приобрели его у дистрибьюторов Лаборатории Касперского, или присылается по почте, если продукт был приобретен в интернет-магазине. Без лицензионного ключа Антивирус Касперского НЕ РАБОТАЕТ.

Н

Неизвестный вирус – новый вирус, информации о котором нет в *антивирусных базах*. Как правило, неизвестные вирусы обнаруживаются Антивирусом Касперского в объектах при помощи *эвристического анализатора кода*, и таким объектам присваивается статус *подозрительных*.

О

Обновление антивирусных баз – процедура замены/добавления новых антивирусных баз, получаемых приложением с серверов обновлений Лаборатории Касперского или из сетевого каталога.

Объект-контейнер – объект антивирусной проверки, состоящий из нескольких объектов, например, архив, письмо с любым вложенным письмом. См. также **простой объект**.

П

Подозрительный объект – объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока неизвестный Лаборатории Касперского.

Порог вирусной активности – максимально-допустимое количество событий заданного типа в течение ограниченного временного интервала, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Проверка трафика – антивирусная проверка поступающих на Exchange-сервер почтовых сообщений в режиме реального времени с использованием информации текущей (последней) версии антивирусных баз.

Проверка хранилищ – см. **Фоновая проверка**.

Простой объект – объект антивирусной проверки: тело письма или простое вложение, например, в виде исполняемого файла. См. также **объект-контейнер**.

Р

Рабочее место администратора – компьютер, на котором установлен компонент Антивируса Касперского Консоль управления. С него осуществляется настройка и управление серверной частью приложения – компонентом Сервер безопасности.

Резервное копирование – создание резервной копии объекта перед его обработкой и размещение этой копии в резервном хранилище. В дальнейшем объект из резервного хранилища может быть восстановлен, отправлен на исследование в Лабораторию Касперского или удален.

Резервный лицензионный ключ – лицензионный ключ, установленный для работы Антивируса Касперского, но не активизированный. Резервный ключ начинает действовать по окончании срока действия лицензии текущего ключа.

Резервное хранилище (BACKUP) – специальное хранилище, предназначенное для сохранений резервных копий объектов перед лечением, удалением или заменой. Представляет собой служебный каталог и создается в каталоге установки приложения при установке компонента Сервер безопасности.

С

Сервер безопасности – серверный компонент приложения Антивирус Касперского. Обеспечивает антивирусную функциональность и обновление антивирусных баз, а также предоставляет административные сервисы для удаленного управления, настройки, поддержания целостности приложения и хранения информации.

Сервера обновлений Лаборатории Касперского – список http- и ftp-сайтов Лаборатории Касперского, откуда Антивирус Касперского копирует антивирусные базы и обновления приложения на компьютер.

Срок действия лицензии – период времени, в течение которого предоставляется возможность использовать полную функциональность Антивируса Касперского. Срок действия лицензии определяется лицензионным ключом, и, как правило, составляет календарный год со дня установки ключа. После окончания действия лицензии функциональность приложения сокращается.

Счетчик вирусной эпидемии – шаблон, на основании которого проводится оповещение об угрозе возникновении вирусной эпидемии. Счетчик вирусной эпидемии содержит набор

параметров, определяющих порог вирусной активности, способ распространения и текст рассылаемых сообщений.

У

Удаление объекта – способ обработки объекта, при котором происходит его физическое удаление с компьютера. Такой способ обработки рекомендуется применять к зараженным объектам. В случае если удаление является первичным действием над объектом, то перед его выполнением создается *резервная копия*. Вы можете ее использовать для восстановления оригинального объекта.

Ф

Фоновая проверка – повторная антивирусная проверка хранящихся на сервере сообщений и содержимого общих папок с использованием последней версии антивирусных баз. Проверяются все общие папки и защищаемые хранилища (mailbox storage). При проверке могут быть обнаружены новые вирусы, информация о которых отсутствовала в антивирусных базах на момент предыдущих проверок.

Ч

"Черный список" – база данных, содержащая информацию о лицензионных ключах, владельцы которых нарушили условия Лицензионного соглашения, и о ключах, которые были выписаны, но по какой-либо причине не были проданы. Содержимое файла "черного списка" обновляется ежедневно.

Ш

Шаблон замены – шаблон, на основании которого формируется текстовое сообщение об обнаруженных зараженных объектах или об угрозе возникновении вирусной эпидемии.

Шаблон отчета – шаблон, на основании которого формируются отчеты о результатах антивирусной проверки сервера. Шаблон отчета содержит набор параметров, определяющих отчетный период, расписание создания и формат отчета.

Шаблон уведомления – шаблон, на основании которого проводится оповещение об обнаруженных при антивирусной проверке зараженных объектах. Шаблон уведомления содержит набор параметров, определяющих порядок уведомления, способ распространения и текст рассылаемых сообщений.

K

Kaspersky Administration Kit – приложение, входящее в состав продуктов Антивирус Касперского Business Optimal и Kaspersky Corporate Suite и предназначенное для централизованного решения

основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе приложений Лаборатории Касперского.

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, Бенилюксе, 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 двухсотпятидесяти высококвалифицированных специалистов, девять из которых имеют дипломы MBA, пятнадцать – степени кандидатов наук и двое являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками 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 шлюзов, межсетевых экранов и 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. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

С.1. Другие разработки Лаборатории Касперского

Антивирус Касперского® Personal

Антивирус Касперского® Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное ПО. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

- **Постоянная защита компьютера** – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
- **Проверка компьютера по требованию** – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Антивирус Касперского Personal теперь не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию. Такая организация работы **заметно повышает скорость работы программы**.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах.

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их

содержимого, а также удаление вредоносного кода из архивных файлов формата **ZIP, CAB, RAR, AFJ**.

Простота настройки программы осуществляется за счет возможности выбора одного из трех предопределенных уровней: **Максимальная защита**, **Рекомендуемая защита** и **Максимальная скорость**.

Обновления антивирусных баз осуществляется каждые три часа, при этом обеспечивается их гарантированная доставка при разрыве или смене соединений с интернетом.

Антивирус Касперского® Personal Pro

Пакет разработан специально для полномасштабной антивирусной защиты домашних компьютеров, работающих под управлением операционных систем Windows 98/ME, Windows 2000/NT, Windows XP с бизнес-приложениями из состава Microsoft Office 2000. Антивирус Касперского® Personal Pro включает программу загрузки ежедневных обновлений антивирусной базы и программных модулей. Уникальная система эвристического анализа данных второго поколения эффективно нейтрализует неизвестные вирусы. Простой и удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского® Personal Pro обеспечивает:

- **антивирусную проверку по требованию пользователя** локальных дисков;
- **автоматическую проверку в масштабе реального времени** на присутствие вирусов всех используемых файлов;
- **почтовый фильтр**, осуществляющий проверку входящих и исходящих почтовых сообщений в фоновом режиме;
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов.

Kaspersky® Anti-Hacker

Программа Kaspersky® Anti-Hacker представляет собой персональный межсетевой экран, обеспечивающий полномасштабную защиту компьютера, работающего под управлением операционной системы Windows, от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети и интернета.

Kaspersky® Anti-Hacker отслеживает сетевую активность по протоколу TCP/IP для всех приложений на вашем компьютере. При обнаружении подозрительных действий какого-либо приложения программа информирует вас об этом, и, при необходимости, блокирует сетевой доступ этому

приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере.

Благодаря технологии SmartStealth™ значительно затрудняется обнаружение компьютера извне: режим невидимости вашего компьютера обеспечивает защиту от хакерских атак, не оказывая никакого негативного влияния на вашу работу в интернете. Программа обеспечивает стандартную прозрачность и доступность информации.

Kaspersky® Anti-Hacker также блокирует наиболее распространенные сетевые хакерские атаки, отслеживает попытки сканирования портов.

Программа поддерживает упрощенное администрирование по пяти режимам безопасности. По умолчанию используется режим самообучения, который позволяет настроить систему безопасности в зависимости от вашей реакции на различные события. Данный режим позволяет сконфигурировать межсетевой экран под конкретного пользователя и конкретный компьютер.

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на КПК, работающих под управлением Palm OS или Windows CE, а также информации, переносимой с PC или любой карты расширения, ROM файлы и базы данных, В состав программы входит оптимальный набор средств антивирусной защиты:

- **антивирусный сканер**, обеспечивающий проверку информации (хранимой как на PDA, так и на картах расширения любого типа) по требованию пользователя;
- **антивирусный монитор**, осуществляющий перехват вирусных программ, передаваемых в процессе синхронизации с использованием технологии HotSync™ или с другими КПК.

Программа также обеспечивает защиту данных, хранящихся на карманном компьютере, от несанкционированного доступа путем шифрования доступа к самому устройству и ко всей информации, хранящейся на портативном компьютере и картах расширения.

Антивирус Касперского® Business Optimal

Программный комплекс представляет собой уникальное конфигурируемое решение антивирусной защиты для предприятий малого и среднего бизнеса.

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту[1]:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *почтовых систем* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; Microsoft ISA Server.

Антивирус Касперского® Business Optimal также включает систему централизованной установки и управления – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite – это интегрированная система, обеспечивающая информационную безопасность вашей корпоративной сети независимо от ее сложности и размера. Программные компоненты, входящие в состав комплекса, предназначены для защиты всех узлов сети компании. Они совместимы с большинством используемых сегодня операционных систем и программных приложений, объединены системой централизованного управления и обладают единым пользовательским интерфейсом. Программный комплекс обеспечивает создание системы защиты, полностью совместимой с системными требованиями вашей сети.

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstations и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.

[1] В зависимости от типа поставки

- *интернет-шлюзов*: CheckPoint Firewall –1; Microsoft ISA Server.
- *карманных компьютеров*, работающих под управлением Windows CE и Palm OS.

Kaspersky® Corporate Suite также включает *систему централизованной установки и управления* – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

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 RBL-списки и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознать 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 базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal предназначен для защиты пользователей почтовых клиентов Microsoft Outlook и Microsoft Outlook Express от нежелательных писем (спама).

Программный пакет Kaspersky Anti-Spam Personal представляет собой мощный инструмент для обнаружения спама в потоке входящей электронной почты, поступающей по протоколам POP3 и IMAP4 (только для Microsoft Outlook).

Во время фильтрации проверяются все возможные атрибуты письма: адреса отправителя и получателя, его заголовки. Также используется *контентная фильтрация*, то есть анализируется содержание самого письма (включая заголовок *Subject*) и файлов вложений. Применяются уникальные лингвистические и эвристические алгоритмы.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

C.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, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700	
Экстренная круглосуточная помощь	+7 (095) 797-8707 support@kaspersky.com	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com
Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	
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 (095) 797-8700	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (095) 797-8700	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.com	