ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky® Corporate Suite

ОПИСАНИЕ ПРОДУКТА

KASPERSKY® CORPORATE SUITE

Описание продукта

Тел./факс: +7 (495) 797-87-00
http://www.kaspersky.ru/

Дата редакции: март 2006 года

Содержание

ГЛАВА 1. KASPERSKY® CORPORATE SUITE

Программный продукт **Kaspersky® Corporate Suite** – интегрированная система, предназначенная для обеспечения безопасности всех составляющих корпоративной сети вне зависимости от ее масштаба и сложности. Главное преимущество данного продукта – создание независимой от платформенного обеспечения, централизованно-управляемой структуры защиты от вирусов и хакерских атак для корпоративных сетей любой топологической сложности с возможным подключением удаленных участков сети.

Антивирусные продукты, входящие в поставку Kaspersky® Corporate Suite, обеспечивают надежный контроль над всеми потенциальными источниками проникновения компьютерных вирусов. Они используются на:

- рабочих станциях под управлением Microsoft Windows 98/Me/ 2000/NT/XP Workstations и Linux;
- файловых серверах под управлением Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, Linux и Samba Server;
- почтовых системах Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Linux;
- *интернет-шлюзах* Check Point FireWall-1, Microsoft ISA Server 2004 Enterprise Edition;
- карманных компьютерах, работающих под управлением Microsoft-Windows CE и Palm OS, а также смартфонах, работающих под управлением Microsoft Windows Mobile 2003 for Smartphone и Microsoft Smartphone 2002.

Компоненты, входящие в состав Kaspersky® Corporate Suite, интегрированы в единый инструмент централизованного администрирования, существенно упрощающий управление системой антивирусной защиты корпоративной сети.

В своей работе Лаборатория Касперского ориентируется на полное удовлетворение потребностей и учет даже самых незначительных требований клиентов. Kaspersky® Corporate Suite позволяет создать надежную систему компьютерной безопасности, максимально соответствующую конфигурации сети.

1.1. Основные свойства программного продукта Kaspersky® Corporate Suite

НАДЕЖНОСТЬ ЗАЩИТЫ

Основная задача при создании корпоративной системы информационной безопасности – обеспечение бесперебойной и взаимосвязанной работы всех компонентов решения. Надежность и эффективность Kaspersky® Corporate Suite подтверждена многолетним опытом использования программных модулей, входящих в его состав, сотнями компаний по всему миру. Качество и эффективность продуктов Лаборатории Касперского подтверждены различными сертификатами, в числе которых сертификат и лицензия ГосТехКомиссии при Президенте РФ, сертификат независимой тестовой лаборатории West Coast Labs по трем уровням соответствия (Level 1, Level 2, Trojan), сертификат Международной ассоциации компьютерной безопасности, сертификат Microsoft на совместимость с операционной системой Microsoft Windows.

МУЛЬТИПЛАТФОРМЕННОЕ РЕШЕНИЕ

Инфраструктура современной корпорации представляет собой сложный многокомпонентный механизм, в котором одновременно используются различные операционные системы и программные приложения. Поддерживая наиболее распространенные операционные системы, Kaspersky® Corporate Suite представляет собой идеальное решение для обеспечения защиты всех ключевых элементов корпоративной сети – рабочих станций, файловых серверов, почтовых шлюзов и каналов выхода в интернет.

ИНТЕГРИРУЕМОСТЬ

Лаборатория Касперского ориентируется на полное удовлетворение запросов и принимает во внимание даже самые незначительные пожелания своих клиентов. Программный продукт Kaspersky® Corporate Suite разработан с учетом особенностей функционирования программных комплексов на уровне корпорации. За счет применения самых современных методов разработки Kaspersky® Corporate Suite может быть органично интегрирован в уже существующие системы или настроен под выполнение специфических задач. Результатом является предоставление заказчику решения, максимально соответствующего его специфике.

КОМПЛЕКСНАЯ ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ

Защита корпоративной сети может быть успешной только в том случае, когда она распространяется на все сетевые узлы, каналы передачи данных

и места их хранения. Kaspersky® Corporate Suite представляет собой комплексную систему обеспечения безопасности сети предприятия, предоставляя защиту для рабочих станций, файловых и почтовых серверов, а также контроль над потоками данных, проходящими через интернет-шлюзы и сетевые экраны. Kaspersky® Corporate Suite также включает в себя уникальную систему управления антивирусной защитой – Kaspersky® Administration Kit – обеспечивающую централизованную установку и управление программным комплексом.

СОВРЕМЕННЫЕ СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

В Kaspersky® Corporate Suite используются современные средства антивирусной защиты: проверка всех хранимых на компьютере файлов по запросу пользователя; проверка всех используемых файлов в режиме реального времени; уникальный модуль фонового перехвата скрипт-вирусов; поведенческий блокиратор, обеспечивающий 100% защиту от макро-вирусов. Комбинированное использование этих технологий сводит вероятность проникновения вирусов практически к нулю. Использование в Kaspersky® Corporate Suite метода эвристического анализа позволяет обнаруживать и предотвращать заражение неизвестными вирусами.

СВОЕВРЕМЕННОЕ ОБНАРУЖЕНИЕ НОВЫХ ВИРУСОВ

Лаборатория Касперского реализует автоматические обновления антивирусных баз с серверов компании каждый час. Специалисты компании круглосуточно отслеживают вирусную ситуацию и, в случае появления новой вредоносной программы, разрабатывают соответствующий антивирусный модуль, который затем в экстренном порядке распространяется среди пользователей.

КОМПЛЕКС ДОПОЛНИТЕЛЬНЫХ УСЛУГ

Лаборатория Касперского предоставляет поддержку в разработке и внедрении корпоративных систем антивирусной защиты. Мы предлагаем услуги по исследованию существующих систем обеспечения безопасности данных, разработке персональных решений на базе собственных продуктов или программных средств третьих сторон. Компания предлагает профессиональные консультационные услуги в области установки, настройки и управления программными продуктами Лаборатории Касперского, проводит обучение конечных пользователей и предоставляет расширенную техническую поддержку. В результате пользователь получает полномасштабное решение по обеспечению информационной безопасности, полностью соответствующее системным требованиям и специфическим задачам вашей компании.

Пользователи программных продуктов Лаборатории Касперского получают доступ к круглосуточной Службе технической поддержки по телефону и электронной почте на русском, английском и французском языках, а также на немецком языке в течение рабочего дня.

1.2. Состав продукта

В состав Kaspersky® Corporate Suite входят следующие приложения:

- *Защита рабочих станций*:
    - Антивирус Касперского® для Windows 98/Me/2000/NT/XP Workstations;
    - Антивирус Касперского® для Linux Workstation.
- *Защита файловых серверов*:
    - Антивирус Касперского® для Windows File Servers (Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server);
    - Антивирус Касперского® для Novell Netware;
    - Антивирус Касперского® для Linux File Server;
    - Антивирус Касперского® для Samba Server.
- *Защита почтовых систем*:
    - Антивирус Касперского® для Microsoft Exchange 2000/2003;
    - Kaspersky® Security для Microsoft Exchange Sever 2003;
    - Антивирус Касперского® для Lotus Notes/Domino;
    - Антивирус Касперского® для Linux Mail Server.
- *Защита каналов выхода в интернет:*
    - Антивирус Касперского® для Microsoft ISA Server Enterprise Edition;
    - Антивирус Касперского® для CheckPoint Firewall.
- *Защита карманных компьютеров* – Kaspersky® Security 5.5 для PDA.
- *Система централизованного удаленного управления приложениями Лаборатории Касперского* – Kaspersky® Administration Kit.

ГЛАВА 2. АНТИВИРУСНАЯ ЗАЩИТА РАБОЧИХ СТАНЦИЙ

2.1. Антивирус Касперского® для Windows Workstations

Лаборатория Касперского предоставляет антивирусную защиту для рабочих станций, функционирующих под управлением операционных систем Windows 98/ Me/ NT Workstation 4.0/ 2000 Professional/ XP Home Edition/Professional.

ЗАЩИТА В МАСШТАБЕ РЕАЛЬНОГО ВРЕМЕНИ

В режиме постоянной защиты Антивирус Касперского находится в оперативной памяти компьютера, перехватывает и анализирует все обращения к файловой системе компьютера и сетевым каталогам; лечит, удаляет зараженные и изолирует подозрительные объекты в специальное хранилище для дальнейшего анализа.

АНТИВИРУСНАЯ ФИЛЬТРАЦИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

Антивирус Касперского осуществляет проверку электронной почты в режиме мониторинга: анализирует запросы на получение и отправку сообщений электронной почты. Антивирус предотвращает попадание сообщений, содержащих вредоносный код, в почтовый ящик пользователя, а также отправку подозрительных или зараженных объектов получателям. Проверяется вся почта, отправляемая и принимаемая почтовой программой Microsoft Office Outlook, а также вся почта, отправляемая и принимаемая любой почтовой программой по протоколам SMTP и POP3.

ПЕРЕХВАТ ПОТЕНЦИАЛЬНО ОПАСНЫХ МАКРОСОВ

В режиме постоянной защиты Антивирус осуществляет защиту офисных приложений, использующих VBA-макросы: анализирует макрокоманды перед их выполнением и предотвращает выполнение потенциально опасных макрокоманд.

ПЕРЕХВАТ СКРИПТ-ВИРУСОВ

Антивирус Касперского выполняет постоянную проверку опасных скриптов VBScript и JavaScript: проверка производится перед выполнением скрипта

модулем обработки скриптов операционной системы; при обнаружении потенциально опасного скрипта Антивирус блокирует его выполнение.

ЗАЩИТА МЕСТ ХРАНЕНИЯ ДАННЫХ

По требованию пользователя или администратора Антивирус находит и обезвреживает вредоносный код в заданных областях проверки; лечит, удаляет зараженные и изолирует подозрительные объекты в специальное хранилище для дальнейшего анализа. Администратор Антивируса может создавать и настраивать задачи проверки, составлять расписание автоматического запуска.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского предоставляет возможность автоматизированного обновления антивирусных баз, которые содержат описание вирусов и методов их лечения, а также модулей приложения с серверов обновлений Лаборатории Касперского. При подключении к серверам обновлений Лаборатории Касперского через прокси-сервер на базе Microsoft ISA Server 2000 или Microsoft ISA Server 2004 поддерживается NTLM-аутентификация. При обновлении создается резервная копия всех обновляемых файлов на случай необходимости отката последнего обновления. В целях экономии интернет-трафика может быть использован сервис автоматического копирования полученных обновлений в локальный каталог, который будет служить источником обновлений для других компьютеров сети.

УДОБСТВО НАСТРОЙКИ ЗАЩИТЫ

Приложение позволяет настроить антивирусную защиту путем выбора одного из трех предопределенных уровней защиты: *максимальная защита*, *рекомендуемый* и *максимальная скорость*.

ИМПОРТ И ЭКСПОРТ НАСТРОЕК

Антивирус Касперского позволяет экспортировать собственные настройки в файл, который в дальнейшем может быть использован в качестве шаблона для других экземпляров приложения (импорт настроек).

ПРОВЕРКА ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ

Антивирус Касперского позволяет проверять и обрабатывать потенциально опасное программное обеспечение в режимах постоянной защиты и проверки по требованию. Запуск проверки может быть выполнен как при помощи интерфейса приложения, так и из командной строки.

ИЗОЛЯЦИЯ ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ

Антивирус Касперского поддерживает функцию изоляции подозрительных объектов в карантинном каталоге; их отправку по требованию в Лабораторию Касперского для дальнейшего исследования; восстановление объектов из хранилища по требованию пользователя или администратора.

Объекты хранятся на карантине в зашифрованном виде и не могут нанести вред вашему компьютеру. Для своевременной обработки данных объектов возможно настроить проверку карантинного хранилища после каждого обновления антивирусных баз.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ И ЗАРАЖЕННЫХ ОБЪЕКТОВ

В приложении реализовано сохранение резервной копии всех подозрительных или зараженных объектов перед их лечением или удалением. Это позволяет восстановить данные в случае возникновения сбоев или ошибок при их лечении или удалении, а также отследить картину заражения.

ВЫСОКИЙ УРОВЕНЬ ПРОИЗВОДИТЕЛЬНОСТИ

Использование в Антивирусе Касперского нового антивирусного ядра и новых технологий iChecker™ и iStreams™ позволяет значительно сократить объем занимаемой оперативной памяти и увеличить производительность антивирусной защиты.

РАЗДЕЛЕНИЕ ПРАВ ДОСТУПА АДМИНИСТРАТОРА И ПОЛЬЗОВАТЕЛЯ

Разделение прав администратора и пользователя приложения реализовано в двух интерфейсах: оптимизированном интерфейсе с минимально необходимым набором функций для продуктивной работы офисного пользователя и расширенном интерфейсе администратора с возможностью гибкого управления настройками приложения. Доступ к режиму администратора защищается паролем.

ЦЕНТРАЛИЗОВАННОЕ УДАЛЕННОЕ УПРАВЛЕНИЕ

Антивирус Касперского интегрирован в уникальную систему управления антивирусной защитой. Kaspersky® Administration Kit позволяет централизовано устанавливать и управлять Антивирусом Касперского с любого, даже удаленного, компьютера; составлять расписание и порядок работы задач программы; автоматически загружать и подключать новые обновления антивирусных баз через интернет; рассылать предупреждения об обнаруженных вирусных атаках; просматривать журналы отчетов рабочих станций; регулировать права доступа к изменению настроек программы другими пользователями, устанавливать парольную защиту на удаление приложения.

2.2. Антивирус Касперского® для Linux Workstation

Антивирус Касперского® для Linux Workstation обеспечивает антивирусную защиту рабочих станций, работающих под управлением операционной системы Linux, от всех типов вредоносных программ.

СОВМЕСТИМОСТЬ С РАСПРОСТРАНЕННЫМИ ДИСТРИБУТИВАМИ И ВЕРСИЯМИ LINUX-ПЛАТФОРМ

Антивирус Касперского для Linux Workstation может использоваться на наиболее популярных дистрибутивах Linux. В их число входят: RedHat Linux (версии 9.0, FedoreCore 2, Advanced Server 3), SuSE Linux (версии Enterprise Server 9.0, Professional 9.2), Debian GNU/Linux (версия 3.0 updated (r4)), Mandrakelinux (версия 10.1). Также поддерживается установка приложения под операционной системой FreeBSD (версии 4.10 и 5.3).

УНИКАЛЬНОЕ СОЧЕТАНИЕ САМЫХ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ДЛЯ LINUX

В состав Антивируса Касперского входит следующий набор средств антивирусной защиты Linux-систем:

- **Антивирусный сканер** – компонент приложения, который проводит антивирусную проверку объектов по требованию пользователя или автоматически с помощью утилиты cron.
- **Антивирусный монитор** – компонент постоянной защиты, обеспечивающий антивирусную защиту файлов в режиме реального времени.
- **Антивирусный демон** – разновидность антивирусного сканера с оптимизированной процедурой загрузки в память. Осуществляет антивирусную проверку данных в режиме реального времени. Состоит из серверной и клиентской программ, что позволяет создавать собственные решения интеграции.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского реализует обновление антивирусных баз с серверов обновлений Лаборатории Касперского или из локального каталога. Эта функция может быть осуществлена по запросу системного администратора или автоматически с помощью cron. Для повышения надежности работы выполняется проверка на целостность скачанных обновлений, прежде чем они будут загружены приложением.

РАЗЛИЧНЫЕ НАБОРЫ АНТИВИРУСНЫХ БАЗ

Приложение позволяет использовать стандартный или расширенный набор антивирусных баз. Расширенный набор используется для обнаружения не только вредоносных программ, но и потенциально опасных программ, таких как рекламные программы, программы удаленного администрирования и утилиты, которые могут использоваться злоумышленниками в своих целях. У администратора есть возможность определить используемый набор антивирусных баз для каждого из компонентов приложения.

РЕЗЕРВНОЕ ХРАНИЛИЩЕ

Приложение позволяет создать резервное хранилище, в котором будут сохраняться резервные копии подозрительных или зараженных объектов перед выполнением попытки их лечения или удаления. Резервные копии могут быть использованы для восстановления объектов в случае возникновения сбоев или ошибок при их лечении или удалении, а также могут быть отправлены для изучения специалистам Лаборатории Касперского.

ОПТИМИЗАЦИЯ ЗАГРУЗКИ СЕРВЕРА

Благодаря применению технологии iChecker™ и двухуровневого кеширования проверенных файлов значительно сокращается нагрузка на сервер при антивирусной проверке. Использование ограничений на количество одновременно проверяемых в фоновом режиме объектов также позволяет уменьшить загрузку сервера.

СИСТЕМА ВЕДЕНИЯ ОТЧЕТОВ

В Антивирусе Касперского предусмотрена возможность вывода информации о функционировании программы в виде файла отчета с определением уровня детализации данных.

ИНТЕРАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ

Антивирус Касперского для Linux Workstation содержит плагин к распространенной программе Webmin, позволяющий осуществлять удаленное управление приложением через веб-интерфейс. Дополнительно при помощи программы Webmin у администратора есть возможность просматривать в графическом виде статистику вирусной активности за определенный срок, а также данные о типах обнаруженных вирусов.

ГЛАВА 3. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВЫХ СЕРВЕРОВ

3.1. Антивирус Касперского® для Windows File Servers

Антивирус Касперского для Windows File Servers предназначен для защиты файловых серверов, работающих под управлением Windows NT 4.0/2000/2003 Server, от вирусов и вредоносных программ.

АНТИВИРУСНАЯ ЗАЩИТА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

В режиме постоянной защиты Антивирус Касперского находится в оперативной памяти компьютера, перехватывает и анализирует все обращения к файловой системе компьютера и сетевых каталогах; лечит, удаляет зараженные и изолирует подозрительные объекты в специальное хранилище для дальнейшего анализа.

ПЕРЕХВАТ СКРИПТ-ВИРУСОВ

Антивирус Касперского выполняет постоянную проверку опасных скриптов VBScript и JavaScript: проверка производится перед выполнением скрипта модулем обработки скриптов операционной системы; при обнаружении потенциально опасного скрипта Антивирус блокирует его выполнение.

ЗАЩИТА МЕСТ ХРАНЕНИЯ ДАННЫХ

По требованию администратора Антивирус находит и обезвреживает вредоносный код в заданных областях проверки; лечит, удаляет зараженные и изолирует подозрительные объекты для дальнейшего анализа. Администратор Антивируса может создавать и настраивать задачи проверки, составлять расписание автоматичесого запуска.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского предоставляет возможность автоматизированного обновления антивирусных баз, которые содержат описание вирусов и методов их лечения, а также модулей приложения с серверов обновления Лаборатории Касперского. При подключении к серверам обновлений Лаборатории Касперского через прокси-сервер на базе Microsoft ISA Server 2000 или Microsoft ISA Server 2004 поддерживается NTLM-аутентификация.

При обновлении создается резервная копия всех обновляемых файлов на случай необходимости отката последнего обновления. В целях экономии интернет-трафика может быть использован сервис автоматического копирования полученных обновлений в локальный каталог, который будет служить источником обновлений для других компьютеров сети.

ИЗОЛЯЦИЯ ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ

Антивирус Касперского поддерживает функцию изоляции подозрительных объектов в карантинном каталоге; восстановление объектов из хранилища по требованию пользователя или администратора.

Объекты хранятся на карантине в зашифрованном виде и не могут нанести вред вашему компьютеру. Для своевременной обработки данных объектов возможно настроить проверку карантинного хранилища после каждого обновления антивирусных баз.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ И ЗАРАЖЕННЫХ ОБЪЕКТОВ

В приложении реализовано сохранение резервной копии всех подозрительных или зараженных объектов перед их лечением или удалением. Это позволяет восстановить данные в случае возникновения сбоев или ошибок при их лечении или удалении, а также отследить картину заражения.

ВЫСОКИЙ УРОВЕНЬ ПРОИЗВОДИТЕЛЬНОСТИ

Использование в Антивирусе Касперского нового антивирусного ядра и новых технологий iChecker™ и iStreams™ позволяет значительно сократить объем занимаемой оперативной памяти и увеличить производительность антивирусной защиты.

РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ О ВИРУСНЫХ АТАКАХ

При управлении приложением через систему централизованного управления Kaspersky Administration Kit 5.0 в случае обнаружения попытки проникновения на сервер вирусов приложение, в соответствии с установками, отправляет администратору и/или группе пользователей оповещение о произошедшем событии. Для отправки сообщений можно использовать электронную почту или средства Net Send.

УДОБСТВО УПРАВЛЕНИЯ

Управление Антивирусом Касперского возможно локально из командной строки или с помощью Консоли администрирования, выполненной в стандарте Microsoft Management Console, а также удаленно через систему централизованного управления Kaspersky Administration Kit 5.0.

УДОБСТВО НАСТРОЙКИ ЗАЩИТЫ

Приложение позволяет настроить антивирусную защиту путем выбора одного из трех предопределенных уровней защиты: *максимальная защита*, *рекомендуемый* и *максимальная скорость*.

ИМПОРТ И ЭКСПОРТ НАСТРОЕК

Антивирус Касперского позволяет экспортировать собственные настройки в файл, который в дальнейшем может быть использован в качестве шаблона для других экземпляров приложения (импорт настроек).

ЦЕНТРАЛИЗОВАННОЕ УДАЛЕННОЕ УПРАВЛЕНИЕ

Антивирус Касперского интегрирован в уникальную систему управления антивирусной защитой. Kaspersky® Administration Kit позволяет централизовано устанавливать и управлять Антивирусом Касперского® с любого, даже удаленного, компьютера; составлять расписание и порядок работы задач программы; автоматически загружать и подключать новые обновления антивирусных баз через интернет; рассылать предупреждения об обнаруженных вирусных атаках; просматривать журналы отчетов; регулировать права доступа к изменению настроек программы другими пользователями.

3.2. Антивирус Касперского® для Novell NetWare

Антивирус Касперского® для Novell NetWare представляет собой антивирусное решение для защиты файловых серверов, работающих под управлением операционной системы Novell NetWare. Антивирус Касперского обеспечивает надежный контроль над всеми файловыми операциями, происходящими на сервере. В случае обнаружения вирусной атаки приложение сможет быстро и эффективно нейтрализовать ее и удалить нежелательные последствия.

ПОЛНОМАСШТАБНАЯ АНТИВИРУСНАЯ ЗАЩИТА

В состав Антивируса Касперского® для Novell NetWare входят все необходимые способы нейтрализации вирусов: антивирусная проверка мест хранения данных, которая может запускаться как по требованию пользователя, так и по заданному расписанию; постоянная защита всех серверов в режиме реального времени посредством мониторинга файлов, к которым происходит обращение на создание, открытие, копирование, редактирование, закрытие. Комбинированное использование этих методов обеспечивает надежный контроль над всеми вирусоопасными источниками в масштабах сети.

ГИБКОЕ УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ

Антивирус Касперского для Novell NetWare предоставляет администратору возможность осуществлять полное управление программой непосредственно через утилиту сетевого администрирования Novell ConsoleOne, а также через веб-интерфейс.

ЦЕНТРАЛИЗОВАННАЯ УСТАНОВКА И УПРАВЛЕНИЕ

Приложение может быть установлено на сервера NetWare как с дистрибутива, так и с любого компьютера, входящего в состав сети и работающего под управлением Microsoft Windows 9x/NT/2000/ME/XP.

Через ConsoleOne или дополнительный веб-интерфейс системный администратор имеет возможность удаленно управлять Антивирусом Касперского для Novell NetWare: создавать и настраивать задачи антивирусной защиты сервера и обновления антивирусных баз, проводить групповую настройку задач, настраивать параметры работы приложения и системы оповещений, формировать порядок обработки зараженных файлов.

ДИНАМИЧЕСКОЕ ИЗМЕНЕНИЕ КОНФИГУРАЦИИ

Все изменения параметров программы не требуют дополнительной перезагрузки сервера и вступают в силу непосредственно после их подтверждения.

АВТОМАТИЧЕСКАЯ ЗАГРУЗКА ОБНОВЛЕНИЙ ЧЕРЕЗ ИНТЕРНЕТ ИЛИ ИЗ ЛОКАЛЬНОЙ СЕТИ

Антивирус Касперского для Novell NetWare имеет возможность автоматической загрузки обновлений антивирусных баз. Приложение может получать последние обновления через интернет или из локальной сети, и сразу рассылать их на заданные сервера. При этом перед обновлением антивирусных баз сервера могут создаваться резервные копии всех обновляемых файлов, что предоставляет возможность, в случае необходимости, отменить последнее обновление. Перед загрузкой обновленных антивирусных баз приложением выполняется их проверка на целостность, что повышает надежность работы.

ИЗОЛЯЦИЯ ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ

Антивирус Касперского поддерживает функцию изоляции (карантина) подозрительных объектов с их последующим перемещением в специально организуемое системным администратором карантинное хранилище.

РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ О ВИРУСНЫХ АТАКАХ

В случае обнаружения попытки проникновения на сервер вирусов приложение, в соответствии с установками, отправляет администратору

и/или другим пользователям сети оповещение о произошедшем событии по сети Novell NetWare и/или по электронной почте.

ОПОВЕЩЕНИЕ О ВЫПОЛНЕННЫХ ЗАДАЧАХ

Приложение позволяет настроить оповещение администратора и пользователей сети о выполненных задачах обновления и антивирусной проверки средствами электронной почты.

ПРОСМОТР РЕЗУЛЬТАТОВ АНТИВИРУСНОЙ ПРОВЕРКИ СЕРВЕРА И ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

Система ведения журналов обеспечивает быстрый, удобный и унифицированный способ доступа администратора к результатам антивирусной проверки сервера и обновления антивирусных баз, позволяет проводить фильтрацию, сортировку и объединение данных. Система ежедневной ротации информации в журнале событий позволяет создавать отдельный файл отчета каждые 24 часа. Журналы ведутся в форматах txt и xml (htm), это позволяет использовать для их просмотра стандартные средства типа Microsoft Internet Explorer.

АВТОМАТИЧЕСКОЕ ОТКЛЮЧЕНИЕ ЗАРАЖЕННЫХ РАБОЧИХ СТАНЦИЙ

При попытке рабочей станции разместить на сервере зараженный файл Антивирус Касперского может блокировать ее доступ к серверу для предотвращения дальнейшего распространения вирусов по сети.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ И ЗАРАЖЕННЫХ ОБЪЕКТОВ

В приложении реализовано сохранение резервной копии всех подозрительных или зараженных объектов перед их лечением или удалением. Это позволяет восстановить данные в случае возникновения сбоев или ошибок при их лечении или удалении, а также отследить картину заражения.

РЕГУЛИРОВАНИЕ ЗАГРУЗКИ СЕРВЕРА

Антивирус Касперского для Novell NetWare предоставляет системному администратору возможность регулировать уровень использования ресурсов сервера при антивирусной защите.

ОТКАЗОУСТОЙЧИВОСТЬ

Запуск антивирусного ядра, осуществляющего проверку файлов на присутствие вирусов, производится в защищенном адресном пространстве. Такое решение позволяет повысить надежность работы приложения, так как в случае внештатной ситуации, возникшей при проверке файла, работоспособность приложения и файлового сервера в целом, на котором оно работает, не нарушается.

МНОГОПОТОЧНОСТЬ ПРОВЕРКИ ОБЪЕКТОВ

Для увеличения производительности приложения (увеличения количества одновременно проверяемых соединений) возможен запуск и одновременная работа нескольких экземпляров антивирусного ядра на нескольких процессорах. Эта функция приложения позволяет в масштабе реального времени производить параллельную антивирусную проверку нескольких файлов. Максимальное число параллельно запущенных экземпляров антивирусного ядра зависит от аппаратных возможностей сервера.

3.3. Антивирус Касперского® для Linux File Server

Антивирус Касперского для Linux/FreeBSD/OpenBSD File Server обеспечивает антивирусную защиту файловых серверов, работающих под управлением операционных систем Linux/Unix, от всех типов вредоносных программ.

СОВМЕСТИМОСТЬ С РАСПРОСТРАНЕННЫМИ ДИСТРИБУТИВАМИ ВЕРСИЯМИ LINUX-ПЛАТФОРМ

Антивирус Касперского для Linux File Server может использоваться на наиболее популярных дистрибутивах Linux. В их число входят: RedHat Linux (версии 9.0, FedoreCore 2, Advanced Server 3), SuSE Linux (версии Enterprise Server 9.0, Professional 9.2), Debian GNU/Linux (версия 3.0 updated (r4)), Mandrakelinux (версия 10.1). Также поддерживается установка приложения под операционной системой FreeBSD (версии 4.10 и 5.3).

УНИКАЛЬНОЕ СОЧЕТАНИЕ САМЫХ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ДЛЯ LINUX

В состав Антивируса Касперского входит следующий набор средств антивирусной защиты Linux -систем:

- **Антивирусный сканер** – компонент приложения, который проводит антивирусную проверку объектов по требованию пользователя или автоматически с помощью утилиты cron.
- **Антивирусный монитор** – компонент постоянной защиты, обеспечивающий антивирусную защиту файлов в режиме реального времени.
- **Антивирусный демон** – разновидность антивирусного сканера с оптимизированной процедурой загрузки в память. Осуществляет антивирусную проверку данных в режиме реального времени. Состоит из

серверной и клиентской программ, что позволяет создавать собственные решения интеграции.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского реализует обновление антивирусных баз с серверов обновлений Лаборатории Касперского или из локального каталога. Эта функция может быть осуществлена по запросу системного администратора или автоматически с помощью cron. Для повышения надежности работы выполняется проверка на целостность скачанных обновлений прежде чем они будут загружены приложением.

РАЗЛИЧНЫЕ НАБОРЫ АНТИВИРУСНЫХ БАЗ

Приложение позволяет использовать стандартный или расширенный набор антивирусных баз. Расширенный набор используется для обнаружения не только вредоносных программ, но и потенциально опасных программ, таких как рекламные программы, программы удаленного администрирования и утилиты, которые могут использоваться злоумышленниками в своих целях. У администратора есть возможность определить используемый набор антивирусных баз для каждого из компонентов приложения.

РЕЗЕРВНОЕ ХРАНИЛИЩЕ

Приложение позволяет создать резервное хранилище, в котором будут сохраняться резервные копии подозрительных или зараженных объектов перед выполнением попытки их лечения или удаления. Резервные копии в последствии могут быть использованы для восстановления объектов или отправлены для изучения специалистам Лаборатории Касперского.

СИСТЕМА ВЕДЕНИЯ ОТЧЕТОВ

В Антивирусе Касперского предусмотрена возможность вывода информации о функционировании программы в виде файла отчета с определением уровня детализации данных.

ОПТИМИЗАЦИЯ ЗАГРУЗКИ СЕРВЕРА

Благодаря применению технологии iChecker™ и двухуровневого кеширования проверенных файлов значительно сокращается нагрузка на сервер при антивирусной проверке. Использование ограничений на количество одновременно проверяемых в фоновом режиме объектов также позволяет уменьшить загрузку сервера.

ИНТЕРАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ

Антивирус Касперского содержит плагин к распространенной программе Webmin, позволяющий осуществлять удаленное управление приложением через веб-интерфейс. Дополнительно при помощи программы Webmin у администратора есть возможность просматривать статистику вирусной активности за определенный срок и данные о типах обнаруженных вирусов.

3.4. Антивирус Касперского® для Samba Server

Антивирус Касперского для Samba Server обеспечивает антивирусную проверку объектов на Samba-серверах, работающих под управлением операционной системы Linux и FreeBSD.

Приложение выполняет двухуровневую проверку файловой системы сервера: как в режиме реального времени, так и по требованию. В случае нахождения вредоносных программ Антивирус Касперского® позволяет эффективно лечить или блокировать зараженные объекты во избежание дальнейшего распространения эпидемии и оперативно уведомлять системного администратора о произошедшем инциденте.

ПОЛНОМАСШТАБНАЯ АНТИВИРУСНАЯ ЗАЩИТА

Функции полномасштабной защиты обеспечивает уникальный набор компонентов, входящий в состав Антивируса Касперского для Samba Servers:

- **Антивирусный монитор** – компонент приложения, осуществляющий антивирусную проверку обращений через Samba-сервер к файловой системе сервера в режиме реального времени.
- **Антивирусный сканер** – компонент, осуществляющий антивирусную защиты файловых систем. Проверка файловых систем сервера или файлов отдельных каталогов производится по требованию администратора или по расписанию (в зависимости от выбранных настроек).
- **Модуль обновления** – компонент приложения, осуществляющий обновление антивирусных баз, используемых при поиске и лечении вирусов.

ПРОВЕРКА ШИРОКОГО СПЕКТРА ФАЙЛОВЫХ ФОРМАТОВ

Благодаря уникальной технологии проверки Антивирус Касперского обнаруживает вирусы в более чем 700 наиболее распространенных форматах архивированных и сжатых файлов, а также производит лечение файлов в архивах форматов tar и zip посредством дополнительного скрипт-файла, поставляемого вместе с Антивирусом Касперского для Samba Servers.

ЗАЩИТА ПАПОК ОБЩЕГО ДОСТУПА

Антивирус Касперского для Samba Server предоставляет возможность индивидуальной настройки антивирусной защиты папок общего доступа. При этом для каждой папки можно задать любую комбинацию режимов "проверки при открытии" и "проверки при сохранении".

РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ О ВИРУСНЫХ АТАКАХ

Приложение позволяет оповещать администратора об обнаружении в файловых системах сервера зараженных или подозрительных объектов, а также о попытке обращения к зараженному или подозрительному файлу через Samba-сервер. Оповещение производится путем рассылки уведомлений по электронной почте или через стандартную утилиту **smbclient**, возможен также запуск заданных администратором скриптов.

ИЗОЛЯЦИЯ ПОДОЗРИТЕЛЬНЫХ ОБЪЕКТОВ

Антивирус Касперского для Samba Server предоставляет возможность переноса подозрительных объектов в карантинное хранилище. Объекты, хранящиеся на карантине, не могут нанести вред вашему компьютеру.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ И ЗАРАЖЕННЫХ ОБЪЕКТОВ

Антивирус Касперского для Samba Server обеспечивает возможность сохранение оригинала подозрительного или зараженного объекта перед его лечением или удалением (Backup). Это позволяет при необходимости восстановить первоначальный файл.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского для Samba Server позволяет загружать через интернет и автоматически подключать последние обновления антивирусных баз и программных модулей приложения. Эта функция может осуществляться по запросу администратора или автоматически с помощью cron.

ИНТЕРАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ

Антивирус Касперского содержит плагин к распространенной программе Webmin, позволяющий осуществлять удаленное управление приложением через веб-интерфейс.

РЕГУЛИРОВАНИЕ НАГРУЗКИ НА СЕРВЕР

Антивирус Касперского для Samba Server позволяет регулировать нагрузку сервера при работе программы: администратор может ограничивать максимальное число одновременно проверяемых в режиме реального времени файлов. Если нагрузка на сервер превышает заданный уровень, запрошенные на проверку в режиме реального времени файлы будут помещаться в очередь, антивирусная проверка файлов в фоновом режиме автоматически приостанавливается до достижения допустимого уровня нагрузки сервера.

СОКРАЩЕНИЕ ВРЕМЕНИ ПРОВЕРКИ ФАЙЛОВ

Данные об уже проверенных файлах сохраняются в оперативном кеше, что позволяет значительно уменьшить время проверки файла при

последующих его запросах (данные в кеше сохраняются до перезагрузки приложения).

ГЛАВА 4. АНТИВИРУСНАЯ ЗАЩИТА ПОЧТОВЫХ СИСТЕМ

4.1. Антивирус Касперского® для Microsoft Exchange Server

Антивирус Касперского для Microsoft Exchange Server является системой централизованной антивирусной защиты почтовых серверов, работающих под управлением Microsoft Exchange Server 2000/2003. Приложение осуществляет фильтрацию всей внутренней и внешней почтовой корреспонденции как в масштабе реального времени, так и по требованию администратора.

АНТИВИРУСНАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

Антивирус Касперского для Microsoft Exchange Server интегрируется в почтовый сервер как дополнительный модуль и производит постоянную антивирусную проверку всей почтовой корреспонденции защищенных ящиков и папок. Приложение позволяет избавиться от вирусов в старых сообщениях, полученных еще до ее установки или активирования защиты, а также обрабатывать уже проверенные сообщения с использованием обновленных антивирусных баз и обнаруживать вирусы, информация о которых отсутствовала в антивирусных базах на момент предыдущих проверок.

ЗАЩИТА РАБОЧИХ СТАНЦИЙ

Антивирус Касперского для Microsoft Exchange Server имеет функции запрета доставки на рабочие станции зараженных сообщений. Приложение может быть настроено на их удаление, блокировку или лечение.

Благодаря блокированию зараженных сообщений с одновременным информированием системного администратора, вирус, проникший на рабочую станцию, не сможет распространиться на другие компьютеры сети предприятия, используя Microsoft Exchange Server в качестве канала распространения, а администратор получает возможность оперативно реагировать на факт обнаружения зараженного письма.

КОМПЛЕКСНАЯ ПРОВЕРКА ПОЧТОВЫХ СООБЩЕНИЙ

Антивирус Касперского для Microsoft Exchange Server обеспечивает полный контроль над всеми элементами электронного письма: прикрепленными файлами (в т.ч. архивированными и упакованными) и другими сообщениями любого уровня вложенности, внедренными OLE-объектами и самим телом письма.

РЕГУЛИРОВАНИЕ ЧИСЛА ЗАЩИЩАЕМЫХ ПОЧТОВЫХ ЯЩИКОВ

Приложение предоставляет возможность отключать защиту выбранных почтовых хранилищ, что позволяет гибко соблюдать условия лицензионного соглашения. Если количество защищаемых почтовых ящиков превышает значение, указанное в Лицензионном соглашении, то приложение прекращает проверку почтового трафика до тех пор, пока не будет установлена лицензия, допускающая использование большего количества почтовых ящиков, либо пока администратор не уменьшит количество защищаемых почтовых ящиков.

ВЫБОР УРОВНЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Благодаря возможности выбора уровня антивирусной защиты в Антивирусе Касперского для Exchange Server администратор может регулировать уровень безопасности почтового потока и нагрузку на сервер при проверке.

НАДЕЖНАЯ ИЗОЛЯЦИЯ ОПАСНЫХ ОБЪЕКТОВ

Антивирус Касперского для Microsoft Exchange Server позволяет переименовывать обнаруженные зараженные и подозрительные объекты и помещать их исходные копии в карантинный каталог.

РАСПОЗНАВАНИЕ ВИРУСНЫХ ЭПИДЕМИЙ

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

РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ О ВИРУСНЫХ АТАКАХ

Приложение может отправлять уведомления о вирусах администратору, получателю, отправителю зараженных сообщений, а также помещать соответствующие записи в журнал событий приложений и файл отчета программы. Такое всестороннее наблюдение за работой Антивируса помогает вовремя предупредить заражение вирусами сервера и других компьютеров организации.

ДИНАМИЧЕСКОЕ ОБНОВЛЕНИЕ КОНФИГУРАЦИИ

В случае любого изменения конфигурации (например, обновления антивирусных баз или изменения списка защищаемых ящиков) Антивирус Касперского для Microsoft Exchange Server не требует дополнительной

перезагрузки. Все изменения вступают в силу сразу же после их подтверждения администратором.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ЧЕРЕЗ MICROSOFT MANAGEMENT CONSOLE

Входящий в состав Антивируса Касперского для Microsoft Exchange Server компонент *MMC Snap-In,* предоставляет стандартный для Microsoft Management Console интерфейс и позволяет управлять антивирусной защитой серверов удаленно с рабочего места администратора. Благодаря удобному графическому интерфейсу можно приступать к работе с программой без предварительных настроек, а большие возможности по настройке индивидуальной среды управления приложением помогают максимально адаптировать программу к сети конкретного предприятия.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского для Microsoft Exchange Server, наряду с ручным запуском обновления антивирусных баз, обеспечивает возможность автоматического обновления через интернет или из локального каталога. Перед обновлением антивирусных баз выполняется создание резервной копии всех обновляемых файлов, что предоставляет возможность, в случае необходимости, отменить последнее обновление.

ГИБКАЯ СИСТЕМА АУДИТА

В Антивирусе Касперского для Microsoft Exchange Server включена специальная функция ведения статистики обнаруженных вредоносных программ, на основе которой приложение создает отчеты в формате HTML. Уведомления об особо важных событиях в работе приложения, требующих внимания администратора, могут быть просмотрены при помощи MMC-оснастки Event Viewer (Просмотр событий).

МАКСИМАЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ СИСТЕМЫ

Для повышения производительности системы приложение проверяет почту в нескольких потоках. Это достигается путем одновременного запуска нескольких сканирующих процессов. Управляя количеством процессов, администратор может добиться максимальной производительности. Антивирус Касперского поддерживает кластерную технологию Microsoft Exchange Server 2000/2003, обеспечивая антивирусную защиту крупных корпоративных почтовых систем.

Антивирус Касперского для Microsoft Exchange Server поддерживает масштабируемость в зависимости от количества процессоров защищаемого сервера. Для увеличения производительности приложения (увеличения количества одновременно проверяемых объектов) возможен запуск и одновременная работа нескольких экземпляров антивирусного ядра.

Высокая производительность также достигается за счет использования расширенных возможностей по проверке объектов в оперативной памяти

без использования дисковой подсистемы (до 8 объектов, каждый объемом до 1 МБ).

4.2. Kaspersky® Security для Microsoft Exchange Server 2003

Kaspersky Security для Microsoft Exchange Server 2003 предназначен для защиты почтовых ящиков и общих папок на Microsoft Exchange Server 2003 от вредоносных программ и нежелательной почты (спама).

АНТИВИРУСНАЯ ЗАЩИТА

Kaspersky Security для Microsoft Exchange Server 2003 позволяет проверять входящие и исходящие сообщения на присутствие вредоносных объектов. При этом проверке подвергается как тело письма, так и вложенные файлы. Приложение позволяет избавиться от вирусов в старых сообщениях, полученных еще до его установки или активирования защиты, а также обрабатывать уже проверенные сообщения с использованием обновленных антивирусных баз.

ЗАЩИТА ОТ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ

Модуль проверки на спам осуществляет фильтрацию входящей электронной почты в процессе ее приема по SMTP-протоколу, то есть до того, как письма попадут в почтовые ящики пользователей. При этом анализируются все атрибуты и вложения письма. В зависимости от настроек приложение доставляет сообщение пользователю в папку **Входящие**, перемещает сообщение в папку **Нежелательная почта**, блокирует прием сообщения или удаляет его.

РЕЗЕРВНОЕ ХРАНИЛИЩЕ

Приложение использует резервное хранилище, в котором сохраняются резервные копии подозрительных или зараженных объектов перед выполнением попытки их лечения или удаления, а также копии спам-сообщений перед блокировкой или удалением. Резервные копии могут быть использованы для последующего восстановления информации. Наличие настраиваемых фильтров позволяет легко находить исходные копии конкретных объектов.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Kaspersky Security для Microsoft Exchange Server 2003, наряду с ручным запуском обновления антивирусных баз и баз контентной фильтрации, обеспечивает возможность автоматического обновления через интернет

или из локального каталога. При этом у администратора есть возможность настроить различные режимы обновления.

ДЕТАЛЬНАЯ ОТЧЕТНОСТЬ

Для получения информации о результатах выполнения антивирусной проверки и фильтрации спама приложение использует отчеты, формирующиеся автоматически, в соответствии с расписанием, или по запросу.

Также Kaspersky Security для Microsoft Exchange Server 2003 позволяет проводить полную диагностику своей работы и регистрировать зафиксированные события в журнале приложений операционной системы Microsoft Windows и собственных журналах приложения.

РАСПОЗНАВАНИЕ ВИРУСНЫХ ЭПИДЕМИЙ

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

ГИБКАЯ СИСТЕМА НАСТРОЙКИ

Kaspersky Security для Microsoft Exchange Server 2003 предоставляет возможность настраивать свою производительность в зависимости от объема и характера проходящего через Exchange-сервер почтового трафика и системных характеристик компьютера: объема оперативной памяти, быстродействия, количества процессоров.

ЦЕНТРАЛИЗОВАННОЕ УДАЛЕННОЕ УПРАВЛЕНИЕ

Kaspersky Security для Microsoft Exchange Server 2003 поддерживает интеграцию с системой управления антивирусной защитой Kaspersky Administration Kit, которая позволяет централизованно устанавливать и управлять приложением с любого, даже удаленного, компьютера; составлять расписание и порядок работы задач программы; автоматически загружать и подключать новые обновления антивирусных баз и баз контентной фильтрации; рассылать предупреждения об обнаруженных вирусных атаках; просматривать журналы отчетов рабочих станций; регулировать права доступа к изменению настроек программы другими пользователями, устанавливать парольную защиту на удаление приложения.

4.3. Антивирус Касперского® для Lotus Notes/Domino

Антивирус Касперского® для Lotus Notes/Domino является системой централизованной антивирусной защиты для почтовых систем Lotus Notes/Domino R5, R6, работающих под управлением операционных систем Microsoft Windows 2000/2003 Server.

ПРОВЕРКА ПО ТРЕБОВАНИЮ БАЗ ДАННЫХ СЕРВЕРА

Антивирус Касперского® для Lotus Notes/Domino позволяет выполнять по требованию пользователя антивирусную проверку и обработку документов баз данных сервера Lotus Domino.

ПОСТОЯННАЯ ЗАЩИТА ПОЧТОВОГО ТРАФИКА

Антивирус Касперского® для Lotus Notes/Domino интегрируется в почтовый сервер как дополнительный модуль и производит постоянную антивирусную проверку всей почтовой корреспонденции.

КОМПЛЕКСНАЯ ПРОВЕРКА ЭЛЕКТРОННЫХ ПИСЕМ

Антивирус Касперского® для Lotus Notes/Domino проводит полную проверку всех элементов электронного письма: прикрепленных файлов (в т.ч. архивированных и упакованных) и других сообщений любого уровня вложенности, а также самого тела письма. Возможна также проверка всей общедоступной корреспонденции.

РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ О ВИРУСНЫХ АТАКАХ

Приложение имеет встроенные функции блокировки отправления зараженных сообщений с одновременной рассылкой предупреждений отправителю и получателю зараженного письма.

НЕЙТРАЛИЗАЦИЯ ВИРУСОВ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Гибкая система настроек программы позволяет эффективно удалять, блокировать, изолировать (помещать на карантин) или лечить зараженные и подозрительные объекты так, что конечный пользователь будет получать только чистые письма. Более того, даже если вирус проник на рабочую станцию иными путями, нежели электронная почта, он не сможет с нее распространяться, поскольку Антивирус Касперского заблокирует отправку зараженных сообщений, уведомив администратора.

УДОБСТВО АДМИНИСТРИРОВАНИЯ

Управление антивирусной защитой осуществляется при помощи стандартных средств Lotus Notes. Это возможно благодаря тому, что Антивирус Касперского интегрирован с почтовой системой Lotus

Notes/Domino. Администратор может удаленно управлять программой, настраивать параметры антивирусной проверки, осуществлять мониторинг состояния активированной защиты, просматривать отчетность и т.п.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Модуль *Kaspersky AV Updater* позволяет проводить автоматическое обновление антивирусных баз, содержащих описания вирусов и способов их лечения, а также обновлять компоненты приложения.

4.4. Антивирус Касперского® для Linux Mail Servers

Антивирус Касперского для Linux Mail Servers представляет собой систему антивирусной защиты для почтовых систем Sendmail, Qmail, Postfix и Exim. Приложение интегрируется в почтовый сервер в качестве дополнительного модуля и осуществляет постоянную антивирусную проверку всей проходящей почтовой корреспонденции в режиме реального времени.

ПОЛНОМАСШТАБНАЯ АНТИВИРУСНАЯ ЗАЩИТА

Антивирус Касперского для Linux Mail Servers обеспечивает полный контроль над всеми элементами электронного письма. Приложение проверяет не только прикрепленные файлы (в т.ч. архивированные и упакованные), но и тело письма, внедренные OLE-объекты. Проверке подвергаются сообщения любого уровня вложенности.

РАЗЛИЧНЫЕ НАБОРЫ АНТИВИРУСНЫХ БАЗ

Приложение позволяет использовать стандартный или расширенный набор антивирусных баз. Расширенный набор используется для обнаружения не только вредоносных программ, но и потенциально опасных программ, таких как рекламные программы, программы удаленного администрирования и утилиты, которые могут использоваться злоумышленниками в своих целях. У администратора есть возможность определить используемый набор антивирусных баз для каждого из компонентов приложения.

УНИКАЛЬНОЕ СОЧЕТАНИЕ САМЫХ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ДЛЯ LINUX

В состав Антивируса Касперского входит следующий набор средств антивирусной защиты почтовых систем, работающих под управлением Linux:

- **Антивирусный сканер** – компонент приложения, осуществляющий антивирусную проверку объектов по требованию пользователя или автоматически с помощью утилиты cron.

- **Антивирусный SMTP-сканер** – компонент, осуществляющий перехват, проверку и обработку входящего и исходящего почтового трафика, а также позволяет производить дополнительную фильтрацию по именам и типам вложенных файлов.

Комбинированное использование этих модулей дает возможность создать антивирусную защиту, наиболее точно отвечающую вашим системным требованиям.

ОПТИМИЗАЦИЯ ЗАГРУЗКИ СЕРВЕРА

Благодаря применению технологии iChecker™ и двухуровневого кеширования проверенных файлов значительно сокращается нагрузка на сервер при антивирусной проверке. Кроме того, можно ограничить количество одновременно проверяемых в фоновом режиме объектов, что также уменьшает загрузку сервера.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского® реализует обновление антивирусных баз с серверов обновлений Лаборатории Касперского или из локального каталога. Эта функция может быть осуществлена по запросу системного администратора или автоматически с помощью cron. Перед загрузкой обновленных антивирусных баз приложением выполняется их проверка на целостность, что повышает надежность работы.

РЕЗЕРВНОЕ ХРАНИЛИЩЕ

Приложение позволяет создать резервное хранилище, в котором будут сохраняться резервные копии подозрительных или зараженных объектов перед выполнением попытки их лечения, переименования или удаления. Резервные копии могут быть использованы для восстановления объектов в случае возникновения сбоев или ошибок при их лечении или удалении, а также могут быть отправлены для изучения специалистами Лаборатории Касперского.

СИСТЕМА ВЕДЕНИЯ ОТЧЕТОВ И АВТОМАТИЧЕСКОГО УВЕДОМЛЕНИЯ

В Антивирусе Касперского предусмотрена возможность вывода информации о функционировании приложения в виде файла отчета с определением уровня детализации данных. При обнаружении подозрительного или зараженного файла системному администратору, отправителю и получателю письма может быть отправлено специальное сообщение с описанием вредоносного кода (адреса отправителя, получателя, название вируса и т.д.).

ИНТЕРАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ

Антивирус Касперского содержит плагин к распространенной программе Webmin, позволяющий осуществлять удаленное управление приложением через веб-интерфейс. Также с помощью Webmin можно просмотреть

статистику антивирусной активности за определенное время и данные о типах вирусов, которые были выявлены при антивирусной проверке.

4.5. Антивирус Касперского® для Sendmail с Milter API

Антивирус Касперского® для Sendmail с Milter API предназначен для антивирусной защиты почтового трафика Linux-сервера, использующего в качестве почтовой системы Sendmail с Milter API.

ПОЛНОМАСШТАБНАЯ АНТИВИРУСНАЯ ЗАЩИТА

Антивирус Касперского® для Sendmail с Milter API осуществляет перехват и антивирусную проверку входящих и исходящих сообщений сервера. Приложение обеспечивает полный контроль над всеми элементами электронного письма: заголовком, телом, вложением. При обнаружении зараженного элемента сообщения производится антивирусная обработка.

АНТИВИРУСНАЯ ФИЛЬТРАЦИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

Дополнительно к антивирусной проверке и обработке почтовых сообщений вы можете использовать их антивирусную фильтрацию. Данная процедура выполняется на уровне объектов почтового сообщения и может осуществляться по MIME-типу вложений, по их имени и по размеру.

ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ И МОДУЛЕЙ ПРИЛОЖЕНИЯ

Антивирус Касперского реализует обновление антивирусных баз и модулей приложения с серверов обновлений Лаборатории Касперского или локального каталога. Эта функция может быть осуществлена по запросу системного администратора или автоматически по расписанию с помощью cron.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОДОЗРИТЕЛЬНЫХ И ЗАРАЖЕННЫХ ОБЪЕКТОВ

В приложении реализована возможность сохранения резервной копии всех подозрительных или зараженных объектов перед любой операцией, меняющей что-либо в сообщении, или перед его блокировкой и отклонением. Такая возможность позволяет в любой момент времени восстановить исходное письмо.

СИСТЕМА ВЕДЕНИЯ ОТЧЕТОВ И АВТОМАТИЧЕСКОГО УВЕДОМЛЕНИЯ

В Антивирусе Касперского предусмотрена возможность вывода информации о функционировании приложения в виде файла отчета с определением уровня детализации данных.

При обнаружении подозрительного или зараженного сообщения администратору, отправителю и получателю письма может быть отправлено специальное сообщение с описанием вредоносного кода (адреса отправителя, получателя, название вируса и т.д.). Дополнительно реализовано создание собственных шаблонов уведомлений отправителей, получателей и администраторов с использованием специального языка.

ИНТЕРАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ

Антивирус Касперского для Sendmail с Milter API содержит плагин к распространенной программе Webmin, позволяющий осуществлять удаленное управление приложением через веб-интерфейс.

ГЛАВА 5. АНТИВИРУСНАЯ ЗАЩИТА КАРМАННЫХ КОМПЬЮТЕРОВ

Kaspersky® Security для PDA предназначен для защиты карманных персональных компьютеров (КПК) на базе операционных систем Pocket PC/ Windows Mobile 2003, Palm OS, а также смартфонов на базе операционных систем Microsoft Smartphone 2002, Windows Mobile 2003 for Smartphone от вирусов и несанкционированного доступа к данным.

Kaspersky® Security для PDA позволяет:

- защищать карманное устройство от вирусов, проникающих:
    - в момент синхронизации с компьютером;
    - при беспроводном обмене данными с другими устройствами;
    - через почтовые сообщения;
- проверять на присутствие вирусов объекты, находящиеся во внутренней памяти устройства или на картах расширения памяти;
- получать обновления антивирусных баз;
- шифровать данные КПК и ограничивать доступ к ним с помощью пароля.

Kaspersky® Security для PDA включает в себя следующие компоненты:

- **Антивирус Касперского® для Pocket PC** – программа предназначена для защиты КПК на базе операционной системы Pocket PC от вирусов и выполняет следующие функции:
    - постоянная защита файловой системы КПК и баз данных от вирусов в режиме мониторинга;
    - проверка объектов файловой системы и баз данных, находящихся на КПК или подключенных картах расширения памяти, по требованию пользователя;
    - обновление антивирусных баз;
    - формирование файла отчета о работе программы.

- **Kaspersky® DataSafe для Pocket PC** – программа для криптографической защиты данных КПК на базе операционной системы Pocket PC. Программа позволяет создавать в памяти КПК секретные папки для хранения конфиденциальной информации. Все данные сохраняются в секретной папке в зашифрованном виде и не могут быть прочтены без знания пароля.
- **Антивирус Касперского® для Microsoft Smartphone** – программа предназначена для антивирусной защиты смартфонов на базе операционных систем Microsoft Smartphone 2002, Windows Mobile 2003 for Smartphone.
- **Антивирус Касперского® для Palm OS** – программа предназначена для антивирусной защиты КПК на базе операционной системы Palm OS и выполняет следующие функции:
    - постоянная защита данных КПК от вирусов в режиме реального времени;
    - проверка объектов, находящихся на КПК или подключенных картах расширения памяти, по требованию пользователя;
    - обновление антивирусных баз.
- **Kaspersky® DataSafe для Palm OS** – программа для криптографической защиты данных КПК на базе операционной системы Palm OS. Программа позволяет блокировать доступ к КПК вручную, при наступлении определенной временной метки или при выключении. Для разблокирования КПК требуется ввод пароля. Одновременно с блокировкой происходит шифрование хранящихся на КПК данных. Ключ для расшифровки генерируется в момент разблокирования КПК на основании вводимого пароля. Поэтому, даже если злоумышленник получит содержимое памяти заблокированного КПК, он не сможет извлечь информацию без пароля.

ГЛАВА 6. АНТИВИРУСНАЯ ЗАЩИТА КАНАЛОВ ДОСТУПА В ИНТЕРНЕТ

6.1. Антивирус Касперского® для CheckPoint Firewall

Антивирус Касперского для CheckPoint Firewall является специальным подключаемым модулем, осуществляющим антивирусную фильтрацию данных, которые проходят через сетевые экраны, поддерживающие протокол обмена данных CVP (Content Vectoring Protocol).

АНТИВИРУСНОЕ РЕШЕНИЕ ДЛЯ ИНТЕРНЕТА

Главный принцип антивирусной защиты корпоративной сети – жесткий контроль над всеми потоками внешних данных. В первую очередь это касается файлов, получаемых пользователями из интернета и других сетей. Антивирус Касперского для CheckPoint Firewall в режиме реального времени обнаруживает и удаляет все типы вредоносных кодов из трафика, проходящего через сетевой экран по протоколам HTTP, FTP и SMTP.

СОВМЕСТИМОСТЬ С РАСПРОСТРАНЕННЫМИ СЕТЕВЫМИ ЭКРАНАМИ

Антивирус Касперского для CheckPoint Firewall может использоваться на любых сетевых экранах, поддерживающих протокол обмена данными CVP (Content Vectoring Protocol). Например, Check Point FireWall-1 и др.

ПЕРЕДОВЫЕ АНТИВИРУСНЫЕ ТЕХНОЛОГИИ

Антивирус Касперского для CheckPoint Firewall создан на основе всемирно известного антивирусного ядра, использующегося в других продуктах компании. Приложение проверяет на присутствие вирусов архивированные и упакованные файлы, электронную почту. Мощный эвристический анализатор кода и функция избыточного сканирования не допустят проникновения в сеть даже неизвестных вирусов.

ПРОЗРАЧНОСТЬ ПЕРЕДАЧИ ДАННЫХ

Антивирус Касперского для CheckPoint Firewall предоставляет конфигурируемую систему пакетного обмена данными между Антивирусом, сетевым экраном и клиентской машиной. Такая система обеспечивает прозрачность процесса передачи данных при сохранении высочайшего

уровня безопасности. Благодаря этому исключаются случаи обрыва загрузки больших файлов через сетевой экран.

НАДЕЖНАЯ ИЗОЛЯЦИЯ ОПАСНЫХ ОБЪЕКТОВ И РАССЫЛКА ПРЕДУПРЕЖДЕНИЙ

Приложение позволяет создать специальный карантинный каталог, в который будут помещаться подозрительные объекты, обнаруженные в потоке данных из интернета. Также у администратора есть возможность настроить уведомление обо всех попытках проникновения вирусов через сетевой экран.

УДОБСТВО И ПРОСТОТА ИСПОЛЬЗОВАНИЯ

Антивирус Касперского для CheckPoint Firewall ведет подробный отчет обо всех своих действиях, а также статистику обнаруженных вирусных атак. Любые настройки приложения могут быть изменены без ее дополнительной перезагрузки. Все изменения вступают в силу сразу же после их подтверждения.

Приложение может быть установлено на любом компьютере в рамках корпоративной сети и затем интегрировано с сетевым экраном. Для этого необходимо добавить Антивирус Касперского для CheckPoint Firewall в список сервисов сетевого экрана.

6.2. Антивирус Касперского® для Microsoft Server Enterprise Edition

Антивирус Касперского для Microsoft ISA Server – это система антивирусного контроля над файлами, перемещаемыми по протоколам HTTP и FTP через брандмауэр Microsoft Internet Security and Acceleration Server, обеспечивающая высокий уровень защиты корпоративных сетей от проникновения и распространения вредоносных программ через каналы доступа в интернет.

ЗАЩИТА СЕТЕВОГО ТРАФИКА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Антивирус Касперского для Microsoft ISA Server выполняет функции сетевого фильтра: перехватывает данные, передаваемые по протоколам HTTP и FTP, выделяет из них контролируемые объекты, анализирует их на присутствие вирусов и блокирует проникновение в локальную сеть зараженных файлов и веб-документов.

Для протокола HTTP приложение осуществляет лечение обнаруженных подозрительных и зараженных объектов. В случае успешного лечения

объект замещается на вылеченный и передается пользователю, если лечение не возможно, доступ к объекту блокируется.

ПОДДЕРЖКА РАБОТЫ С МАССИВОМ СЕРВЕРОВ

Использование Антивируса Касперского является оптимальным для обеспечения надежной защиты Microsoft ISA-серверов, работающих в режиме массива (Array Member). Программа обеспечивает централизованное управление настройками всех серверов, входящих в массив, а также централизованное обновление антивирусных баз.

УПРАВЛЕНИЕ ЧЕРЕЗ ISA MICROSOFT MANAGEMENT CONSOLE

Входящий в состав Антивируса Касперского для Microsoft ISA Server модуль управления предоставляет стандартный интерфейс на базе MMC и позволяет управлять приложением удаленно с рабочего места администратора.

ОПТИМИЗАЦИЯ НАГРУЗКИ НА СЕРВЕР

Антивирус Касперского для Microsoft ISA Server предоставляет возможность регулировать уровень антивирусной защиты входящего трафика путем назначения различным группам пользователей различных правил проверки пересылаемых данных. При этом из проверки могут исключаться потоки данных, запрашиваемых с доверительных серверов, а также объекты, которые заведомо не могут содержать вирусов. Это позволяет ускорить процесс антивирусной проверки и снизить загрузку сервера.

МНОГОПОТОЧНОСТЬ ПРОВЕРКИ ОБЪЕКТОВ

Для увеличения пропускной способности при обработке больших потоков данных возможен запуск и одновременная работа нескольких экземпляров антивирусного ядра. Эта функция Антивируса Касперского позволяет производить одновременную антивирусную проверку нескольких объектов. Максимальное число параллельно запущенных экземпляров антивирусного ядра зависит от аппаратных возможностей сервера, но не может превышать тридцать два.

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ

Антивирус Касперского для Microsoft ISA Server наряду с ручным запуском обновления антивирусных баз обеспечивает возможность автоматического обновления через интернет. Обновление баз происходит без остановки проверки и в случае получения с сервера поврежденных или неработоспособных баз происходит автоматический возврат к предыдущей копии баз.

БЛОКИРОВКА СОЕДИНЕНИЯ С ИСТОЧНИКОМ ЗАРАЖЕНИЯ

При обнаружении в потоке данных зараженных или подозрительных объектов (для HTTP-протокола в случае невозможности их лечения)

Антивирус Касперского для Microsoft ISA Server разрывает соединение с источником заражения. При этом пользователю, пославшему запрос, в окно браузера выводится сообщение о блокировании объекта с указанием причин.

СЧЕТЧИКИ ПРОИЗВОДИТЕЛЬНОСТИ

Антивирус Касперского для Microsoft ISA Server предоставляет возможность сбора и просмотра в режиме реального времени обобщенных показателей работы приложения через стандартную службу Microsoft Windows Администрирование / Производительность.

ГЛАВА 7. KASPERSKY® ADMINISTRATION KIT

Программный комплекс Kaspersky Administration Kit предназначен для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерной сети предприятия, построенной на основе приложений, входящих в состав Kaspersky Corporate Suite. Kaspersky Administration Kit поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

Приложение адресовано администраторам корпоративных компьютерных сетей, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях.

УПРАВЛЕНИЕ ПАРАМЕТРАМИ АНТИВИРУСНОЙ ЗАЩИТЫ

Программный пакет позволяет создавать многоуровневую систему антивирусной защиты и управлять работой всех приложений с единого рабочего места администратора. Последнее особенно важно для крупных организаций (до нескольких десятков тысяч машин), в которых корпоративная сеть может охватывать несколько территориально разделенных зданий или помещений. Приложение предоставляет администратору следующие возможности:

- Удаленная централизованная установка и удаление приложений, входящих в состав продуктов Лаборатории Касперского, на компьютеры, работающие под управлением операционных систем семейства Microsoft Windows. Эта возможность позволяет администратору один раз скопировать на выделенный компьютер необходимый набор приложений Лаборатории Касперского, и после этого проводить удаленную установку на любое количество компьютеров сети.

- Управление лицензиями. Данная возможность позволяет централизованно устанавливать лицензионные ключи ко всем установленным приложениям компании, отслеживать выполнение лицензионного соглашения (соответствие числа лицензий количеству работающих приложений в сети) и срок его окончания.

- Автоматическое обновление антивирусных баз и модулей антивирусных приложений на компьютерах. Эта возможность позволяет проводить централизованное обновление антивирусных баз для всех установленных приложений компании без непосредственного обращения каждого компьютера к серверам обновлений Лаборатории Касперского.

Обновление может происходить автоматически, по заданному администратором графику. Администратор может отслеживать распространение обновлений на клиентские компьютеры.

- Удаленное централизованное управление всеми приложениями, входящими в состав продуктов Лаборатории Касперского, работающими на компьютерах под управлением операционной системы Microsoft Windows:
    - объединение компьютеров в *группы администрирования* в соответствии с выполняемыми функциями и набором установленных на них приложений;
    - централизованная настройка параметров работы антивирусных приложений путем создания и применения *групповых политик*; для упрощения администрирования групповые политики могут быть экспортированы и импортированы из одной группы в другую;
    - индивидуальная настройка параметров работы антивирусных приложений для отдельных компьютеров при помощи *настроек приложения*;
    - централизованное управление работой антивирусных приложений путем создания, запуска и контроля выполнения *групповых и глобальных задач*;
    - построение индивидуальных схем работы приложений путем создания и запуска задач для набора компьютеров из различных групп администрирования;
    - ведение централизованного списка объектов, помещаемых в карантинные каталоги на клиентских компьютерах.
- Система получения отчетности. Данная возможность позволяет осуществлять централизованный сбор статистики о работе всех установленных приложений компании, отслеживать корректность работы этих приложений и создавать отчеты на основании полученной информации. Администратор может создавать единый сетевой отчет о работе приложения, отчеты о работе приложений на каждом компьютере.
- Механизм оповещения о событиях в работе приложений. Механизм рассылки почтовых уведомлений. Эта возможность позволяет администратору формировать список событий в работе приложений, при возникновении которых к нему будут поступать уведомления. Например, в числе таких событий может быть обнаружение вируса или некорректное завершение процедуры обновления антивирусных баз на компьютере, обнаружение нового компьютера в сети.

- Резервное копирование и восстановление. Резервное копирование позволяет переносить Сервер администрирования с одного компьютера на другой без каких-либо потерь информации, а также восстанавливать данные при переходе на более новую версию приложения Kaspersky Administration Kit. Задача резервного копирования данных может быть настроена на автоматическое выполнение.

Приложение Kaspersky Administration Kit состоит из трех основных компонентов:

- **Сервер администрирования** осуществляет функции централизованного хранения информации об установленных в сети предприятия приложениях Лаборатории Касперского и управления ими. Приложение позволяет администратору создавать иерархию серверов администрирования любого уровня вложенности.

- **Агент администрирования** осуществляет взаимодействие между Сервером администрирования и приложениями Лаборатории Касперского, установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех приложений из состава продуктов компании Антивирус Касперского Business Optimal и Kaspersky Corporate Suite.

- **Консоль администрирования** предоставляет пользовательский интерфейс к административным сервисам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC).

ГЛАВА 8. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

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

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

Лаборатория Касперского сегодня – это более двухсот пятидесяти 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 систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада). Клиенты Лаборатории Касперского обеспечиваются широким спектром дополнительных услуг,

гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

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

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700
Экстренная круглосуточная помощь:	+7 (495) 797-8707
Поддержка пользователей персональных продуктов и Business Optimal:	+7 (495) 797-8707 (с 10 до 19 часов) http://www.kaspersky.ru/helpdesk.html
Поддержка пользователей Corporate Suite:	Телефоны и электронный адрес предоставляются при покупке Corporate Suite в зависимости от пакета технической поддержки.
База знаний Лаборатории Касперского:	http://www.kaspersky.ru/faq
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)

Департамент продаж:	+7 (495) 797-8700 sales@kaspersky.com
Общая информация:	+7 (495) 797-8700 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru