

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского® 5.5
для Check Point™ FireWall-1®

РУКОВОДСТВО
АДМИНИСТРАТОРА

АНТИВИРУС КАСПЕРСКОГО® 5.5
ДЛЯ CHECK POINT™ FIREWALL-1®

Руководство администратора

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

Дата редакции: июль 2006 года

Содержание

ГЛАВА 1. ВВЕДЕНИЕ.....	6
1.1. Компьютерные вирусы и вредоносные программы	6
1.2. Назначение, основные функции и состав Антивируса Касперского	9
1.3. Что нового в версии 5.5	11
1.4. Требования к аппаратному и программному обеспечению	12
1.5. Комплект поставки.....	13
1.5.1. Лицензионное соглашение.....	14
1.5.2. Регистрационная карточка	14
1.6. Сервис для зарегистрированных пользователей.....	15
1.7. Принятые обозначения.....	16
ГЛАВА 2. СХЕМА РАБОТЫ ПРИЛОЖЕНИЯ.....	17
2.1. Схема развертывания приложения	17
2.2. Схема развертывания антивирусной защиты.....	18
2.3. Поддержка системы антивирусной защиты	19
ГЛАВА 3. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ.....	20
3.1. Установка приложения	20
3.1.1. Первая установка	21
3.1.2. Повторная установка.....	24
3.2. Удаление приложения	24
ГЛАВА 4. ИНТЕГРАЦИЯ АНТИВИРУСА КАСПЕРСКОГО С CHECK POINT™ FIREWALL-1®.....	26
4.1. Регистрация Сервера безопасности на Check Point™ FireWall-1®	26
4.2. Получение сертификата Сервера безопасности.....	33
ГЛАВА 5. НАЧАЛО РАБОТЫ	35
5.1. Запуск программы	35
5.2. Интерфейс программы	35
5.2.1. Главное окно программы.....	35
5.2.2. Контекстное меню.....	37
5.3. Создание списка управляемых серверов	38

5.4. Подключение Консоли управления к серверу.....	40
5.5. Подключение Сервера безопасности к Check Point™ FireWall-1®	41
5.6. Минимально необходимая настройка	47
5.7. Защита без дополнительной настройки.....	47
5.8. Проверка работоспособности приложения	49
5.8.1. Тестовый "вирус" EICAR и его модификации	49
5.8.2. Тестирование защиты HTTP-трафика	50
5.8.3. Тестирование защиты SMTP-трафика	50
5.8.4. Тестирование защиты FTP-трафика.....	51
ГЛАВА 6. ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ	52
6.1. Загрузка обновлений из интернета.....	55
6.2. Загрузка обновлений из сетевого каталога	56
6.3. Автоматическое обновление	58
6.4. Обновление вручную	58
ГЛАВА 7. АНТИВИРУСНАЯ ЗАЩИТА	59
7.1. Антивирусная обработка объектов	61
7.1.1. Действия над объектами, передаваемыми по HTTP-протоколу.....	62
7.1.2. Действия над объектами, передаваемыми по FTP-протоколу	63
7.1.3. Действия над объектами, передаваемыми по SMTP-протоколу	64
7.2. Уровень антивирусной защиты	64
7.3. Включение и отключение антивирусной защиты. Выбор уровня	65
7.4. Проверка HTTP-трафика	66
7.5. Проверка FTP-трафика.....	71
7.6. Проверка SMTP-трафика	73
7.7. Производительность антивирусной проверки.....	75
ГЛАВА 8. РЕЗЕРВНОЕ ХРАНИЛИЩЕ	79
8.1. Просмотр резервного хранилища	80
8.2. Фильтр резервного хранилища	81
8.3. Восстановление объекта из резервного хранилища.....	84
8.4. Удаление объекта из резервного хранилища	86
8.5. Настройка параметров резервного хранилища	87
ГЛАВА 9. ОТЧЕТЫ	89
9.1. Получение отчета.....	91
9.2. Создание шаблона отчета	93

9.3. Просмотр отчета.....	95
ГЛАВА 10. ЖУРНАЛЫ СОБЫТИЙ ПРИЛОЖЕНИЯ.....	98
10.1. Настройка уровня диагностики.....	99
10.2. Настройка параметров файлов журналов.....	101
ГЛАВА 11. ЛИЦЕНЗИОННЫЕ КЛЮЧИ.....	102
11.1. Информация о лицензии.....	104
11.2. Информация о лицензионных ключах.....	105
11.3. Лицензионные уведомления.....	107
11.4. Установка лицензионного ключа.....	108
11.5. Удаление лицензионного ключа.....	109
ГЛАВА 12. УВЕДОМЛЕНИЕ.....	110
ГЛАВА 13. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ.....	114
ПРИЛОЖЕНИЕ А. ПАРАМЕТРЫ УВЕДОМЛЕНИЙ.....	118
ПРИЛОЖЕНИЕ В. ГЛОССАРИЙ.....	123
ПРИЛОЖЕНИЕ С. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО".....	127
С.1. Другие разработки Лаборатории Касперского.....	128
С.2. Наши координаты.....	137

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.

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 и предотвращении эпидемий внутри предприятия.

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 ин-

формационные 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 пользовательские 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 конфиденциальной 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, основные функции и состав Антивируса Касперского

Антивирус Касперского® для Check Point™ FireWall-1® (далее также **Антивирус Касперского**) – это система антивирусного контроля над файлами, передаваемыми по протоколам HTTP, FTP и SMTP через межсетевой экран Check Point™ FireWall-1®, обеспечивающая высокий уровень защиты корпоративных сетей от проникновения вредоносных программ.

Управление Антивирусом Касперского осуществляется через специализированный интерфейс, встроенный в Microsoft Management Console (далее **MMC**).

Приложение обеспечивает выполнение следующих функций:

- Антивирусная проверка и обработка потоков данных, передаваемых по протоколам HTTP и FTP. В зависимости от настроек приложение пропускает или лечит вредоносный объект, блокирует доступ к объекту, уведомляет о его обнаружении.
- Передача вылеченных файлов клиенту, запросившему HTTP или FTP-поток.
- Проверка на наличие вредоносного кода входящих и исходящих электронных почтовых сообщений, передающихся по протоколу SMTP, а также всех присоединенных к ним файлов в режиме реального времени. В зависимости от настроек приложение пропускает, удаляет и сопровождает предупреждающей информацией зараженные сообщения.
- Формирование списка объектов, которые не будут подвергаться антивирусной проверке.
- Сохранение резервных копии объектов перед лечением, удалением или блокировкой в специальном хранилище, что исключает возможность потери информации. Наличие настраиваемых фильтров для резервного хранилища позволяет легко находить исходные копии конкретных объектов.
- Уведомление пользователя, запросившего объект, содержащий вредоносный код.
- Уведомление путем запуска внешних программ, в том числе написанных администратором файлов сценария, о результатах антиви-

русной проверки объектов, обновлении антивирусных баз, результатах создания отчета, приближении окончания срока действия лицензии и изменении состояния приложения. Эта возможность позволяет администратору организовать уведомление о перечисленных событиях наиболее удобным для него способом.

- Обновление антивирусных баз через интернет и из локального каталога как автоматически, так и в ручном режиме. Ресурсом обновления баз в интернете являются HTTP и FTP-сервера обновлений Лаборатории Касперского.



Поиск вирусов и лечение зараженных объектов выполняются на основании записей *антивирусных баз*, содержащих описание всех известных в настоящий момент вирусов, способов лечения пораженных ими объектов, а также 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. 52).

- Ведение журналов событий и создание регулярных отчетов о результатах антивирусной проверки. Программа позволяет формировать отчеты по встроенным шаблонам с необходимой периодичностью.
- Настройка параметров работы приложения в соответствии с объемом и характером проходящего трафика, а также характеристиками установленного оборудования (объем оперативной памяти, быстродействие, количество процессоров и пр.).
- Управление лицензионными ключами.

Антивирус Касперского 5.5 для Check Point™ FireWall-1® состоит из 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.

1.3. Что нового в версии 5.5

Отличия Антивируса Касперского 5.5 для Check Point™ FireWall-1® от предыдущей версии состоят в следующем:

- Полностью переработанный, удобный для использования графический интерфейс программы выполнен по стандартам Microsoft Management Console. Новый интерфейс позволяет администратору начать работу без каких-либо предварительных настроек, а также предоставляет 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 трафик не только от вредоносного программного обеспечения, но и от потенциально опасного программного обеспечения, такого как программы удаленного наблюдения, программы-рекламы, программы автоматического дозвола на платные сайты, программы-взломщики, программы-шутки.
- Реализована возможность выбора уровня антивирусной защиты, что позволяет администратору регулировать уровень безопасности проходящего через межсетевой экран потока и нагрузку Антивируса при проверке.
- Наличие настраиваемых фильтров для резервного хранилища позволяет легко находить исходные копии конкретных объектов, например, для их последующего восстановления.
- Появилась возможность масштабировать приложение в соответствии с числом процессоров компьютера, на котором оно установлено. Для увеличения производительности приложения (увеличения количества одновременно проверяемых объектов) возможен запуск и одновременная работа нескольких экземпляров антивирусного ядра.
- Возможность управлять размером очереди объектов на проверку позволяет более гибко регулировать нагрузку Антивируса в зависимости от объема проверяемого потока данных.
- Реализована возможность по проверке объектов в оперативной памяти без использования дисковой подсистемы, что существенно повышает производительность.
- За счет поддержки протоколов AMON и ELA достигнута более глубокая интеграция Антивируса Касперского с приложением Check Point™ FireWall-1®, что позволяет, например, передавать информацию о ра-

боте Антивируса и просматривать ее при помощи стандартных средств Check Point™ FireWall-1®.

- Значительно улучшена система ведения журналов. Она позволяет регистрировать зафиксированные события в журнале приложений операционной системы Microsoft Windows и собственных журналах приложения. Предусмотрена возможность настраивать полноту информации и уровень ее детализации. Просмотр журналов организован при помощи приложения Microsoft Windows **Просмотр событий** и таких стандартных средств работы с текстовыми файлами как **Блокнот**.
- Появилась возможность создания расширенных регулярных отчетов о результатах антивирусной проверки. 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.
- Не поддерживается работа с программой из командной строки.

1.4. Требования к аппаратному и программному обеспечению

Антивирус Касперского функционирует совместно с продуктом Check Point™ FireWall-1® версий NG, NG AI и NGX.

Для установки и работы компонентов приложения необходимо, чтобы аппаратное и программное обеспечение компьютера удовлетворяло следующим минимальным требованиям:

Сервер безопасности:

- Аппаратные требования:
 - процессор Intel Pentium II с частотой 300 МГц или выше;
 - около 512 МБ доступной (свободной) оперативной памяти;
 - около 20 МБ свободного дискового пространства для установки приложения (без учета объема резервного хранилища и других служебных каталогов);
 - не менее 1 ГБ свободного дискового пространства для временного хранения копируемых из интернета данных перед антивирусной проверкой и резервного хранилища файлов.
- Программные требования:

- Microsoft Windows 2000 Professional с установленным Service Pack 4 и выше;
- Microsoft Windows XP Professional Edition с установленным Service Pack 2 и выше;
- 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.

Консоль управления:

- Аппаратные требования:
 - процессор Intel Pentium II с частотой 300 МГц или выше;
 - объем оперативной памяти 256 МБ;
 - объем свободной (доступной) памяти на диске 10 МБ.
- Программные требования:
 - Microsoft Windows 2000 Professional с установленным Service Pack 4 и выше;
 - Microsoft Windows XP Professional Edition с установленным Service Pack 2 и выше;
 - 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.

1.5. 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.

1.5.1. 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.

1.5.2. 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.

1.6. 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 можете получать 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.

1.7. 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.
 <i>Чтобы выполнить действие,</i> Шаг 1. ...	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 5.5 для Check Point™ FireWall-1® выполняет функции фильтра: обрабатывает данные, передаваемые по протоколам HTTP, FTP и SMTP, выделяет из них контролируемые объекты, анализирует их на присутствие вредоносного кода и блокирует проникновение в локальную сеть зараженных файлов и веб-документов.

2.1. Схема развертывания приложения

В состав Антивируса Касперского 5.5 для Check Point™ FireWall-1® входят два компонента. Антивирусную функциональность приложения обеспечивает серверный компонент Сервер безопасности. Пользовательский интерфейс программы предоставляет компонент Консоль управления.

Схема развертывания Антивируса Касперского одинакова как для локальной, так и для распределенной конфигурации Check Point™ FireWall-1®.

Сервер безопасности представляет собой CVP-сервер. Он интегрируется в приложение Check Point™ FireWall-1® в соответствии со стандартами OPSEC™ и по умолчанию поддерживает защищенный протокол передачи данных.

Сервер безопасности может быть установлен как на одном компьютере с Check Point™ FireWall-1®, так и на любом из компьютеров, имеющих сетевое соединение по протоколу TCP/IP с компьютером, где установлен Check Point™ FireWall-1®.

Выбор варианта установки Сервера безопасности зависит от того, какая операционная система установлена на компьютере с Check Point™ FireWall-1®, и удовлетворяет ли он требованиям к установке серверного компонента либо от объема передаваемого Check Point™ FireWall-1® трафика.

Следует отметить, что при обработке большого потока данных Антивирус Касперского может вызвать некоторое замедление в работе компьютера, это может сказаться на пропускной способности Check Point™ FireWall-1®. Поэтому в сетях с большим объемом трафика, рекомендуется устанавливать Сервер безопасности на отдельный компьютер.

2.2. Схема развертывания антивирусной защиты



Для создания системы антивирусной защиты при помощи Антивируса Касперского 5.5 для Check Point™ FireWall-1® следует:

1. Установить компонент **Сервер безопасности** на компьютер, имеющий сетевое соединение по протоколу TCP/IP с компьютером, где установлен Check Point™ FireWall-1® (см. п. 3.1 на стр. 20). Установка производится с дистрибутива.

Если в сети установлено несколько серверов Check Point™ FireWall-1®, для каждого из них должен быть установлен свой серверный компонент Сервер безопасности.

Возможна установка нескольких Серверов безопасности, проверяющих данные, поступающие от одного Check Point™ FireWall-1®. В этом случае распределение данных между антивирусными серверами осуществляет межсетевой экран. Для каждого Сервера безопасности результаты антивирусной проверки, а следовательно:

- содержание резервного хранилища;
- информация, представленная в отчетах;
- набор событий, зарегистрированных в журналах приложения и журнале Windows;

будут приводиться только по тем объектам, которые были переданы Check Point™ FireWall-1® на этот Сервер безопасности.

Вместе с **Сервером безопасности** на компьютер будет установлена **Консоль управления**. Через **Консоль управления** вы можете управлять работой не только совместно установленного Сервера безопасности, но и тех Серверов, с компьютерами которых имеется сетевое соединение по протоколу TCP/IP.



Количество установленных в сети экземпляров Антивируса Касперского определяется числом установленных Серверов безопасности.

2. Провести интеграцию Антивируса Касперского и Check Point™ FireWall-1® (см. Глава 4 на стр. 26), для каждого из установленных Серверов безопасности.

3. Для централизованного управления работой всех установленных в сети Серверов безопасности с единого выделенного рабочего места администратора установить **Консоль управления** на компьютер, имеющий сетевое соединение по протоколу TCP/IP со всеми компьютерами, где установлены компоненты **Сервер безопасности**.
4. Сформировать список управляемых серверов (см. п. 5.3 на стр. 38).
5. Подключить Консоль управления к серверам (см. п. 5.4 на стр. 40).
6. Для каждого из серверов настроить параметры подключения к Check Point™ FireWall-1® (см. п. 5.5 на стр. 41).
7. Для каждого из серверов настроить систему антивирусной защиты:
 - Откорректировать параметры обновления антивирусных баз (см. Глава 6 на стр. 52).
 - Проверить правильность настройки параметров и корректность работы Антивируса с помощью тестового "вируса" **EI-CAR** (см. п. 5.8 на стр. 49).
 - Настроить параметры журналов событий и отчетов (см. Глава 10 на стр. 98 и Глава 9 на стр. 89).
 - Настроить параметры уведомления о результатах антивирусной проверки объектов, обновлении антивирусных баз, создании отчетов, приближении окончания срока действия лицензии, изменении состояния приложения (см. Глава 12 на стр. 110).

2.3. Поддержка системы антивирусной защиты

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

- в регулярном обновлении антивирусных баз;
- в регулярной проверке журналов работы приложения и отчетов о результатах антивирусной проверки.

ГЛАВА 3. УСТАНОВКА И УДАЛЕНИЕ ПРИЛОЖЕНИЯ

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



Для установки Антивируса Касперского 5.5 для Check Point™ FireWall-1® необходимо наличие прав локального администратора на компьютере, где осуществляется установка.



Обновление предыдущих версий Антивируса Касперского для Check Point™ FireWall® до версии 5.5 не производится.

3.1. Установка приложения

Программа установки предложит установить на компьютер, где она запущена, компоненты приложения Антивирус Касперского 5.5 для Check Point™ FireWall-1® – Сервер безопасности и Консоль управления. Вы можете выбрать как полную, так и выборочную установку приложения, а также восстановить некорректную установку Антивируса Касперского.

В результате установки Консоли управления на компьютере в меню **Пуск / Программы** появится программная группа **Антивирус Касперского для Check Point™ FireWall-1®**; и значок для ее запуска.

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

- имя – **Антивирус Касперского 5.5 для Check Point™ FireWall-1®**;
- тип запуска – **автоматический**;
- учетная запись – **Локальная система**.

Просмотр свойств Сервера безопасности и наблюдение за его работой осуществляется при помощи стандартных средств администрирования Microsoft Windows – **Управление компьютером / Службы**. Информация о работе Сервера безопасности фиксируется и сохраняется в журнале приложений Windows на компьютере, где установлен Сервер безопасности и в собственных журналах приложения Антивирус Касперского.

3.1.1. Первая установка

Чтобы установить Антивирус Касперского, запустите исполняемый файл с дистрибутивного CD-диска приложения. 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 выполняется проверка соответствия аппаратных и программных характеристик компьютера минимально-необходимым требованиям. В случае их несоблюдения установка выполнена не будет.

При несоответствии программных характеристик обновите версию операционной системы и установите требуемые Пакеты обновлений (Service Packs), после этого повторите установку Антивируса Касперского.

Шаг 2. 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 3. Выбор типа установки

На этом этапе определите тип установки: полная или выборочная.

Для установки на компьютер и Сервера безопасности, и Консоли управления выберите вариант **Полная**. Установка производится в каталог, предусмотренный по умолчанию (**Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point FireWall**).

Если вы хотите установить только один из компонентов приложения либо изменить каталог установки компонентов, предусмотренный по умолчанию, воспользуйтесь выборочным типом установки. В этом случае на следующем этапе вам будет предложено выбрать нужный компонент и указать путь к каталогу установки.

Шаг 4. Выбор компонентов приложения для установки и каталога установки

Если вы используете выборочный тип установки, укажите, какие компоненты приложения должны быть установлены на компьютер. Вы также можете изменить предусмотренный по умолчанию каталог для их установки.

Вы можете выбрать для установки либо оба компонента, либо только Консоль управления. Установка Сервера безопасности без Консоли не производится.

По умолчанию, будет предложено установить оба компонента: **Сервер безопасности** и **Консоль управления** в каталог **Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point FireWall**. Если такого каталога нет, он будет создан автоматически. Вы можете изменить каталог установки при помощи кнопки **Обзор**.



Если аппаратные или программные характеристики компьютера не соответствуют минимально-необходимым требованиям для установки Сервера безопасности, вам будет предложено установить только Консоль управления.

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

Шаг 5. Выбор каталога данных

При установке Сервера безопасности создаются необходимые для работы приложения служебные каталоги и базы данных. В их число входят:

- каталоги временных файлов и резервного хранилища;
- каталог размещения антивирусных баз, используемых приложением;
- каталог для хранения отчетов;
- каталог хранения журналов;
- база данных резервного хранилища;
- база данных отчетной статистики.



Каталог данных должен быть исключен из проверки установленными на компьютере антивирусными программами.

Укажите каталог для размещения служебных данных приложения. По умолчанию предлагается создать каталог **Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point FireWall\DataFolder**. Вы можете изменить путь к каталогу при помощи кнопки **Обзор**.

После установки приложения вы сможете изменить путь к каталогу данных через Консоль управления Антивирусом Касперского, в окне настройки параметров антивирусной защиты **Антивирусная проверка** на закладке **Общие**. Новое значение вступит в силу при перезапуске Сервера безопасности.

Обращаем ваше внимание на то, что используемые приложением базы данных создаются только один раз, при установке Сервера безопасности.



В случае смены каталога данных приложения, для корректного переноса информации в новый каталог должно быть полностью скопировано содержимое старого каталога с сохранением целостности структуры подкаталогов и их названий.

При нарушении целостности структуры каталога данных, Сервер безопасности не будет запущен, т.е. Антивирус Касперского работать не будет.

Шаг 6. Запуск установки

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

Шаг 7. Установка лицензионного ключа

При установке компонента Сервер безопасности вам будет предложено установить лицензионный ключ к приложению Антивирус Касперского 5.5 для Check Point™ FireWall-1®.

Вы можете установить лицензионный ключ позже через Консоль управления, однако без лицензионного ключа антивирусная функциональность приложения будет недоступна, возможен запуск только Консоли управления.

Лицензионный ключ является вашим личным "ключом", в котором находится служебная информация, необходимая для полнофункциональной работы приложения, а также дополнительная справочная информация:

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

В открывшемся окне установите текущий лицензионный ключ. Для этого в разделе **Текущий лицензионный ключ** нажмите на кнопку **Добавить/Заменить**. 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.



В качестве лицензионного ключа к Антивирусу Касперского 5.5 для Check Point™ FireWall-1® может быть использован лицензионный ключ к предыдущей версии приложения - Антивирусу Касперского 4.0 для FireWall, если срок действия этого ключа еще не закончился.

Вы можете также установить резервный лицензионный ключ, который будет активирован автоматически по окончании срока действия текущего лицензионного ключа. Для этого в разделе **Резервный лицензионный ключ** нажмите на кнопку **Добавить** и в открывшемся окне выбора файлов укажите файл ключа.

Закройте окно установки лицензионных ключей при помощи кнопки **Заккрыть**.

Шаг 8. Завершение установки

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

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:

запустите исполняемый файл с дистрибутивного компакт-диска и в открывшемся окне 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.

3.2. Удаление приложения

Удаление Антивируса Касперского для Check Point™ FireWall-1® вы можете провести стандартными средствами установки и удаления программ **Microsoft 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 Check Point™ FireWall-1® с использованием дистрибутива:

запустите исполняемый файл с дистрибутивного компакт-диска и в открывшемся окне выберите вариант **Удалить**.

ГЛАВА 4. ИНТЕГРАЦИЯ АНТИВИРУСА КАСПЕРСКОГО С CHECK POINT™ FIREWALL-1®

Процедура интеграции Антивируса Касперского и Check Point™ FireWall-1® является стандартной для приложений OPSEC™ и состоит из двух этапов:

1. Регистрация Сервера безопасности в качестве OPSEC™ - приложения на Check Point™ FireWall-1®.
2. Получение сертификата Сервера безопасности.

После завершения интеграции Антивируса Касперского с Check Point™ FireWall-1® следует подключить Сервер безопасности к Check Point™ FireWall-1® (см. п. 5.5 на стр. 41).



Если проходящий через межсетевой экран трафик передается на обработку нескольким Серверам безопасности, каждый из них следует интегрировать с Check Point™ FireWall-1®.

4.1. Регистрация Сервера безопасности на Check Point™ FireWall-1®

Подробное описание регистрации OPSEC™-приложений приводится в руководствах к Check Point™. Опишем настройку параметров, специфичных для Антивируса Касперского. Процедура проводится с консоли управления Check Point™ FireWall-1® (**Check Point SmartDashboard™**).



Для регистрации Сервера безопасности в качестве OPSEC™ - приложения на Check Point™ FireWall-1®:

1. Создайте новый сетевой объект (**Network Objects/ New Nodes/Host**) для компьютера, на котором установлен Сервер безопасности. В открывшемся окне (см. рис 1) укажите сетевое имя и IP-адрес этого компьютера.

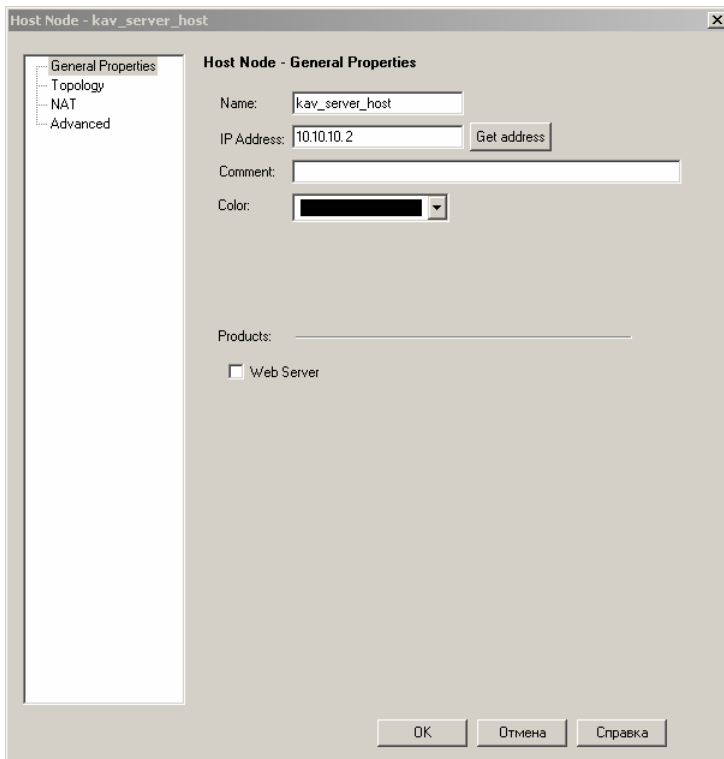


Рисунок 1. Создание сетевого объекта **Сервер безопасности**

2. При создании нового объекта - приложения OPSEC™ (**OPSEC Application/New**) в окне настройки параметров **OPSEC Application Properties** на закладке **General** (см. рис 2) выполните следующие действия:
 - в поле **Name** введите имя OPSEC™-приложения, по которому будет проводиться адресация к Серверу безопасности служб Check Point™ FireWall-1®;
 - в поле **Host** из раскрывающегося списка выберите созданный ранее для Сервера безопасности сетевой объект;
 - в разделах **Server Entities** и **Client Entities** выберите в качестве поддерживаемых приложением протоколов CVP, AMON и ELA.



Настраивать параметры работы протоколов не требуется. Антивирус Касперского использует настройки, предусмотренные в Check Point™ FireWall-1® по умолчанию.

Если конфигурация взаимодействия Check Point™ FireWall-1® с OPSEC™-приложениями отличается от стандартной, укажите нужные значения параметров.

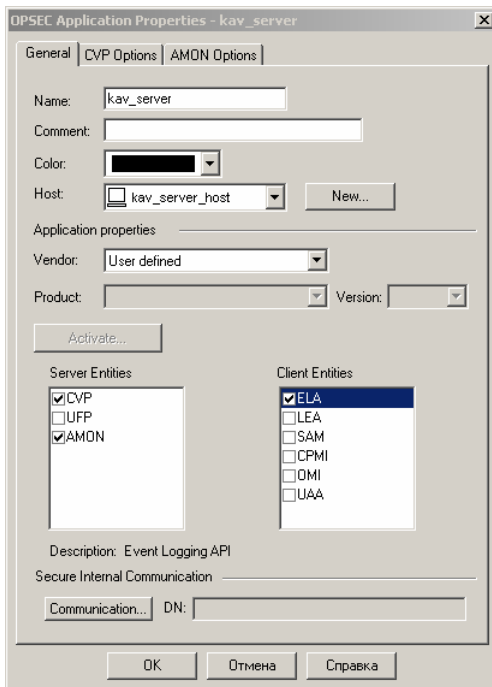


Рисунок 2. Создание OPSEC™ приложения

3. Настройте защищенное подключение Сервера безопасности к Check Point™ FireWall-1® (Secure Internal Communications). В результате будут созданы:
 - ключ для получения сертификата Сервера безопасности;
 - сертификат Сервера безопасности;
 - SIC-имя Сервера безопасности (OPSEC™ application's SIC name).



SIC-имя Сервера безопасности отображается в окне **OP-SEC Application Properties** в поле **DN** раздела **Secure Internal Communication**.

4. Опишите протоколы, которые будут передаваться на антивирусную проверку.

Антивирус Касперского обеспечивает проверку данных, проходящих через межсетевой экран по HTTP-, FTP- и SMTP-протоколам. Создайте:

- URI-ресурс для передачи на проверку HTTP-протокола;
- FTP-ресурс для передачи на проверку FTP-протокола;
- SMTP-ресурс для передачи на проверку SMTP-протокола.

При описании ресурсов для того, чтобы Check Point™ передавал Антивирусу данные на проверку, установите следующие значения параметров:

- для URI-, FTP- и SMTP-ресурсов на закладке **CVP** (см. рис. 3) установите флажок **Use CVP (Content Vectoring Protocol)** и в поле **CVP server** выберите имя **OPSEC™**-приложения, соответствующее Серверу безопасности;

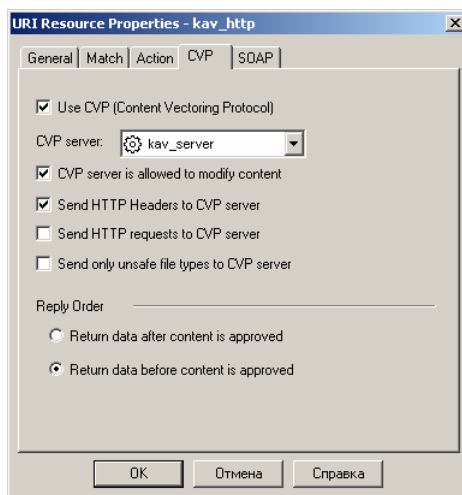


Рисунок 3. Создание URI-ресурса.
Закладка **CVP**

- для FTP-ресурса на закладке **Match** в разделе **Methods** (см. рис. 4) установите флажки **GET** и **PUT**;

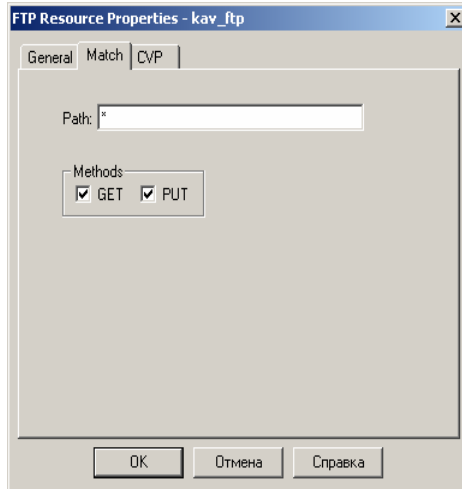


Рисунок 4. Создание FTP-ресурса.
Закладка **Match**

- для URI-ресурса на закладке **General** в разделе **Use this resource to** (см. рис. 5) выберите вариант **Enforce URI capabilities**;

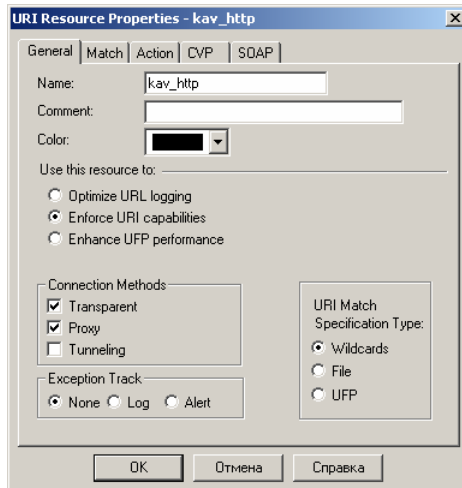


Рисунок 5. Создание URI-ресурса.
Закладка **General**

Для увеличения производительности антивирусной проверки на закладке **CVP** (см. рис. 3) укажите следующие значения параметров:

- Установите флажок **CVP server is allowed to modify content** для URI-, SMTP- и FTP-ресурсов.

Параметр определяет возможность лечения и замены обнаруженных в результате антивирусной проверки объектов (см. п. 7.1 на стр. 61).



Если флажок не установлен, лечение, а для HTTP- и SMTP-трафиков и замена вредоносных объектов, выполняться не будет. Такие объекты будут признаны зараженными и заблокированы средствами Check Point™ FireWall-1®.

- Установите флажки **Send HTTP Headers to CVP server** для URI-ресурса и **Send SMTP Headers to CVP server** для SMTP-ресурса.
- В разделе **Reply Order** выберите вариант **Return data before content is approved** для URI-, SMTP- и FTP-ресурсов.

Параметр определяет возможность досрочной передачи непроверенных данных пользователю (см. п. 7.4 на стр. 66).



Если для URI- и FTP-ресурсов этот вариант не выбран, при проверке объектов, проходящих по HTTP- и FTP-протоколам, досрочная передача данных выполняться не будет.



При создании SMTP-ресурса обратите внимание на следующие ограничения:

- размер перенаправляемых Check Point™ FireWall-1® на антивирусную проверку сообщений, на закладке **Action2** в поле **Do not send mail larger than** (см. рис. 6);
- размер проходящих через Check Point™ FireWall-1® сообщений (**Network Objects/ Check Point/ Advanced/ SMTP**) в поле **Don't accept mail larger than** (см. рис. 7).

Установленные значения должны соответствовать характеристикам вашего трафика. Сообщения, превышающие ограничения, не обрабатываются Check Point™ FireWall-1® и, как следствие, не поступают на антивирусную проверку и не доставляются пользователю.

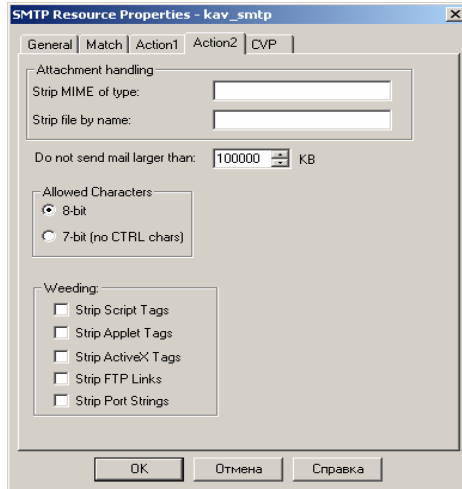


Рисунок 6. Настройка параметров SMTP-ресурса.
Закладка **Action2**

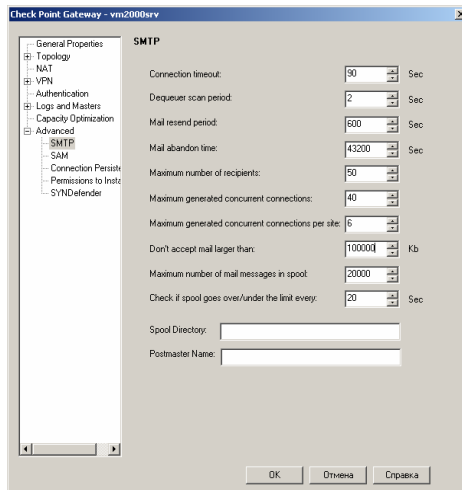


Рисунок 7. Настройка параметров Check Point™ FireWall-1®.
Ограничение объема сообщений

4.2. Получение сертификата Сервера безопасности

Получение сертификата является стандартной процедурой для интегрируемых с Check Point™ FireWall-1® приложений. Она выполняется при помощи утилиты получения сертификатов **opsec_pull_cert.exe**, входящей в состав дистрибутива Антивируса Касперского. После установки Сервера безопасности данная утилита размещается в каталоге установки компонента в подкаталоге **OpsecTools**.

В качестве параметров используются значения, заданные при регистрации Сервера безопасности на Check Point™ FireWall-1® (см. п. 4.1 на стр. 26).



Для получения сертификата Сервера безопасности:

на компьютере, где установлен Сервер безопасности, запустите из командной строки входящий в состав дистрибутива Антивируса Касперского исполняемый файл **opsec_pull_cert.exe** со следующим набором параметров:

```
opsec_pull_cert.exe -h <IP-адрес> -n <имя OPSEC-приложения> -p <ключ> -o <путь к файлу сертификата>
```

где:

<IP-адрес> - IP-адрес компьютера, на котором установлен Check Point™ FireWall-1®;

<имя OPSEC-приложения> - имя OPSEC™-приложения, заданное для Сервера безопасности при регистрации на Check Point™ FireWall-1®;

<ключ> - ключ для получения сертификата Сервера безопасности, заданный при настройке защищенного подключения к Check Point™ FireWall-1®;

<путь к файлу сертификата> - полный путь к файлу, в котором будет сохранен полученный с Check Point™ FireWall-1® сертификат Сервера безопасности. Файл должен быть сохранен в локальном каталоге компьютера, на котором установлен Сервер безопасности. По умолчанию в настройках Антивируса предполагается, что файл сертификата хранится в каталоге данных приложения в служебном каталоге **OpsecDir** под именем **opsec.p12**. Мы рекомендуем использовать данное значение для этого параметра.



Если параметр **-o <путь к файлу сертификата>** не используется, файл сертификата будет сохранен под именем **opsec.p12** в том каталоге, откуда была запущена утилита **opsec_pull_cert.exe**.

Мы рекомендуем перенести файл сертификата в каталог данных приложения в служебный каталог **OpsecDir**, что позволит избежать дополнительной настройки при подключении Сервера безопасности к Check Point™ FireWall-1® (см. п. 5.5 на стр. 41).

После успешного завершения выполнения утилиты на экран выводится полный путь (включая имя файла) к файлу сертификата и SIC-имя Сервера безопасности.

ГЛАВА 5. НАЧАЛО РАБОТЫ

5.1. Запуск программы

Запуск серверной части приложения, Сервера безопасности, осуществляется автоматически при старте операционной системы компьютера, на котором она установлена. Если настроены параметры взаимодействия Сервера безопасности и Check Point™ FireWall-1® (см. п. 5.5 на стр. 41) и включена антивирусная защита (см. п. 7.1 на стр. 61), она начинает работать сразу после запуска серверного компонента.

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 5.5 для Check Point™ FireWall-1®** стандартного меню **Пуск \ Программы**. Данная программная группа создается только на рабочих местах администраторов при установке компонента Консоль управления.

5.2. Интерфейс программы

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

5.2.1. Главное окно программы

Главное окно программы (см. рис. 8) содержит меню, панель инструментов, панель обзора и панель результатов. Меню обеспечивает функции управления окнами, а также доступ к справочной системе. Набор кнопок панели инструментов обеспечивает прямой доступ к некоторым наиболее используемым пунктам главного меню. Панель обзора отображает в виде дерева консоли пространство имен **Антивирус Касперского 5.5 для Check**

Point™ FireWall-1®, панель результата – список элементов выбранного в дереве объекта.

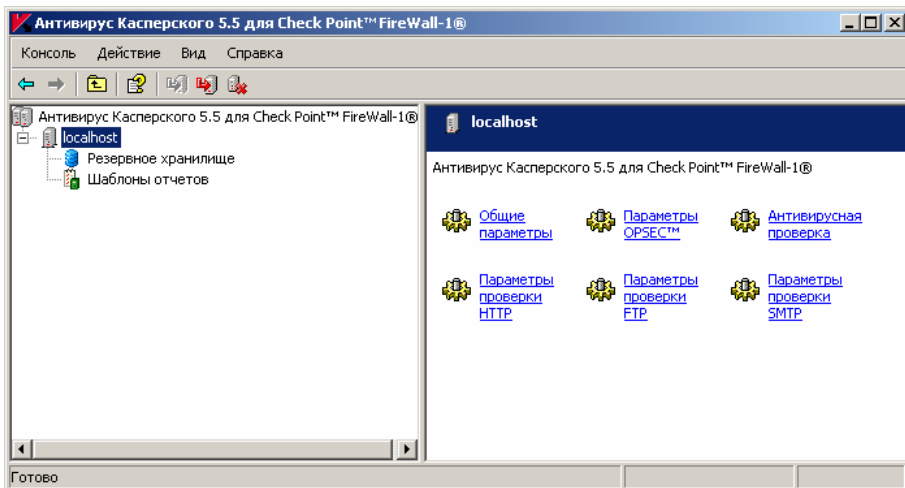


Рисунок 8. Главное окно программы

Пространство имен **Антивирус Касперского 5.5 для Check Point™ FireWall-1®** содержит в виде узлов перечень **управляемых серверов** - компьютеров, на которых управление Антивирусом Касперского осуществляется через данную консоль.

Сразу после установки Консоли управления пространство имен не содержит никаких элементов.

После добавления в дерево консоли управляемый сервер отображается в виде узла с именем **<Имя компьютера>**. Настройка параметров и управление работой Антивируса Касперского осуществляется при помощи расположенных 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 и параметров уведомления.
- [Параметры OPSEC™](#) – просмотр и настройка параметров взаимодействия с приложением Check Point™ FireWall-1®.
- [Антивирусная проверка](#) – управление антивирусной защитой; настройка параметров получения обновлений антивирусных баз, об-

новление вручную, составление расписания автоматического обновления; настройка производительности Антивируса Касперского.

- [Параметры проверки HTTP](#) – настройка параметров проверки HTTP-трафика.
- [Параметры проверки FTP](#) – настройка параметров проверки FTP-трафика.
- [Параметры проверки SMTP](#) – настройка параметров проверки SMTP-трафика.

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

- **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 об антивирусной проверке, на основании которых формируются отчеты.

5.2.2. 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 5.5 для Check Point™ FireWall-1®	Добавить сервер	Добавить в дерево консоли компьютер, на котором управление Антивирусом Касперского будет осуществляться через консоль.
<Имя компьютера>	Отключиться от сервера	Разорвать соединение Консоли управления с установленным на данном компьютере Сервером безопасности.

Объект	Команда	Назначение команды
	Подключиться к серверу	Установить соединение Консоли управления с установленным на данном компьютере Сервером безопасности.
	Удалить сервер из дерева консоли	Удалить компьютер из числа серверов, на которых управление работой Антивируса Касперского осуществляется через консоль.
Резервное хранилище	Новый фильтр	Создание и настройка параметров нового фильтра для поиска объектов, размещенных в хранилище резервных копий.
Шаблоны отчетов	Новый шаблон отчета	Создание нового шаблона отчета.

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

- при помощи команды **Сформировать отчет** по выбранному шаблону создается отчет и сохраняется в виде файла;
- при помощи команды **Просмотреть отчет** выводится на экран последний сформированный по выбранному шаблону отчет;
- команда **Получить файл** позволяет получать исходную копию объекта, сохраненную перед его обработкой Антивирусом.

5.3. Создание списка управляемых серверов

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



Чтобы добавить новый сервер в список управляемых серверов,

1. Выберите в дереве консоли узел **Антивирус Касперского 5.5 для Check Point™ FireWall-1®**, откройте контекстное меню и выберите команду **Добавить сервер** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате откроется окно **Добавление сервера** (см. рис. 9).
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 компьютера 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 было сразу же установлено соединение Консоли управления с Сервером безопасности, установите флажок **Подключится сейчас** (подробнее см. п. 5.4 на стр. 40).



Для успешного подключения на выбранном компьютере обязательно должен быть установлен компонент Сервер безопасности.

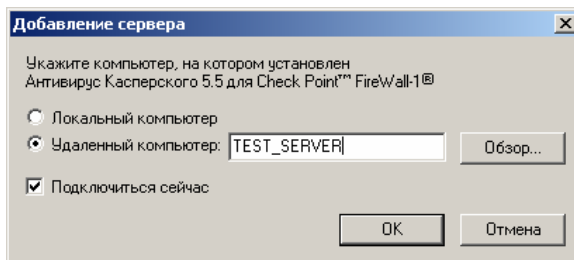




Рисунок 9. Диалоговое окно **Добавление сервера**

В результате выбранный вами компьютер появляется в дереве консоли в виде узла **<Имя компьютера>**. Локальный компьютер отображается под именем **localhost**.

Если соединение с Сервером безопасности успешно установлено, управляемый сервер будет сопровождаться значком  и в состав узла будут входить вложенные папки **Резервное хранилище** и **Шаблоны отчетов**. Если соединение не устанавливалось или не удалось установить, сервер будет отмечен значком . Подключиться к нему вы можете вручную (см. п. 5.4 на стр. 40).



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.


5.4. Подключение Консоли управления к серверу

Для настройки и управления работой Антивируса Касперского 5.5 для Check Point™ FireWall-1® через консоль следует подключиться к установленному на управляемом 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 **Резервное хранилище** и **Шаблоны отчетов**.

Если подключиться к серверу не удалось, выводится предупреждающее сообщение 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.

5.5. Подключение Сервера безопасности к Check Point™ FireWall-1®

Для того чтобы Антивирус Касперского обеспечивал проверку данных, перемещаемых через Check Point™ FireWall-1®, следует настроить параметры взаимодействия приложений.



Без настройки параметров взаимодействия Антивируса Касперского с Check Point™ FireWall-1® антивирусная проверка трафика выполняться не будет!

Взаимодействие Check Point™ FireWall-1® и интегрируемых в него приложений поддерживает подсистема Secure Internal Communications (SIC). При этом подключение приложений к Check Point™ FireWall-1® производится с использованием **защищенного протокола**. Аутентификация приложений осуществляется на основании *сертификата* и *SIC-имени* приложения (OPSEC™ application's SIC name). Эти параметры формируются при интеграции Антивируса Касперского с Check Point™ FireWall-1® (см. п. 4.1 на стр. 26).



Подключение приложений с использованием защищенного протокола рекомендовано компанией Check Point. По умолчанию Антивирус Касперского использует защищенный протокол подключения и значения параметров, предусмотренные в Check Point™ FireWall-1® по умолчанию.

Взаимодействие приложений осуществляется по трем протоколам. По протоколам CVP и AMON Сервер безопасности ожидает подключения от Check Point™ FireWall-1®, по ELA-протоколу сам инициирует подключение Check Point™ FireWall-1®.



Поддержку CVP- и AMON-протоколов осуществляет Сервер безопасности, ELA-протокол реализует Check Point™ FireWall-1®.

Настройка параметров взаимодействия производится с рабочего места администратора через Консоль управления Антивирусом Касперского.

Процедура настройки не зависит от того, установлен Сервер безопасности на выделенном компьютере или на одном компьютере с Check Point™ FireWall-1®. Шаги настройки полностью совпадают.



Для настройки параметров взаимодействия Сервера безопасности и Check Point™ FireWall-1®

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Параметры OPSEC™](#) в панели результата.
2. В открывшемся окне **Параметры OPSEC™** на закладке **Соединение** (см. рис. 10) установите значения параметров подключения по протоколам CVP, AMON и ELA.



По умолчанию используется защищенное подключение Сервера безопасности к Check Point™ FireWall-1®. Для его настройки следует указать значения параметров подключения для протоколов CVP и AMON, а также путь к файлу сертификата.

Для того чтобы Сервер безопасности передавал на Check Point™ FireWall-1® информацию о своей работе, например, зарегистрированные в работе Антивируса события, следует настроить параметры передачи данных по протоколу ELA.



Используемый по умолчанию тип защищенного подключения для каждого из протоколов соответствует параметрам по умолчанию, используемым Check Point™ FireWall-1® начиная с версии NG. Рекомендуется изменять эти настройки только при необходимости.

Для протоколов **CVP** и **AMON** укажите:

- Номер порта на Сервере безопасности, по которому будет приниматься запрос на подключение от Check Point™ FireWall-1®. По умолчанию это 18181 для CVP- и 18193 порт для AMON-протокола.
- Тип используемой при подключении аутентификации. Выберите из раскрывающегося списка необходимое значение:

none - незащищенное ("clear") подключение;

sslca – для аутентификации используется протокол, основанный на криптографических сертификатах, данные шифруются;

sslca_clear – для аутентификации используется протокол, основанный на криптографических сертификатах, данные не шифруются;

auth_opsec – для аутентификации используется внутренний протокол Check Point, данные не шифруются;

ssl_opsec – для аутентификации используется протокол на базе SSL, данные шифруются;

ssl_clear_opsec – для аутентификации используется протокол на базе SSL, данные не шифруются.

Если нужного значения в списке нет, введите его вручную.



Если для аутентификации используются протоколы, требующие наличия ключей для шифрования, файлы ключей должны размещаться в каталоге данных приложения в служебном каталоге **OPSEC**.

- **SIC-имя Сервера безопасности**, заданное при регистрации Сервера безопасности на Check Point™ FireWall-1® (см. п. 4.1 на стр. 26).



Вы можете посмотреть SIC-имя Сервера безопасности через консоль управления Check Point™ FireWall-1®. Оно отображается в окне **OPSEC Application Properties** в поле **DN** раздела **Secure Internal Communication**.



Если используется незащищенное подключение, **SIC-имя Сервера безопасности** указывать не требуется.

Для протокола **ELA** укажите:

- Номер порта, по которому приложение Check Point™ FireWall-1® будет принимать информацию от Антивируса Касперского (по умолчанию 181187 порт).
- Тип используемой при подключении аутентификации (см. выше).
- **Сервер ELA**: NetBIOS-имя, полное доменное имя (FQDN) или IP-адрес компьютера, на котором установлен Check Point™ FireWall-1®.
- **SIC-имя сервера ELA**: внутреннее SIC-имя Check Point™ FireWall-1®, к которому осуществляется подключение Сервера безопасности.



Вы можете посмотреть внутреннее SIC-имя Check Point™ FireWall-1® через консоль управления Check Point™ FireWall-1®. Оно отображается в окне настройки параметров Check Point™ FireWall-1® (**Network Objects/ Check Point/ GeneralProperties**) в поле **DN** раздела **Secure Internal Communication**.

В поле **Путь к файлу сертификата SSLCA** укажите полный путь к полученному с Check Point™ FireWall-1® файлу сертификата Сервера безопасности (см. п. 4.2 на стр. 33). По умолчанию файл сертификата сохраняется на сервере в каталоге данных приложения в служебном каталоге **OpsecDir** под именем **opsec.p12**. Поэтому, если задан относительный путь к файлу, программа будет искать его по адресу: **<Каталог данных>\OpsecDir**.

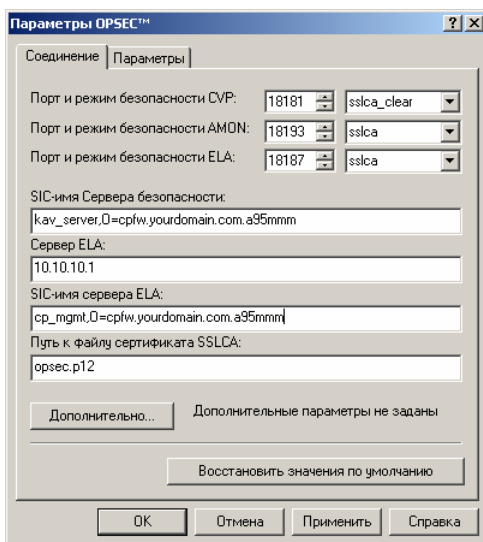


Рисунок 10. Настройка параметров OPSEC™.
Закладка **Соединение**

Чтобы указать параметры, необходимые для настройки соединения Антивируса Касперского и Check Point™ FireWall-1®, но не представленные на закладке **Соединение**, нажмите на кнопку **Дополнительно**.

В результате открывается окно **Настройка дополнительных параметров OPSEC™** (см. рис. 11). Введите описание нужных параметров и нажмите на кнопку **ОК**.

Примером таких параметров для CVP и AMON-протоколов является IP-адрес, по которому Сервер безопасности ожидает подключение Check Point™ FireWall-1®. Если параметр не задан, Сервер безопасности будет ожидать подключения по всем имеющимся на нем IP-адресам.

Пример:

```
cvp_server      ip      10.10.10.2
amon_server    ip      10.10.10.2
```



Подробнее о типах защищённых соединений и значениях по умолчанию для различных версий Check Point™ FireWall-1® можно узнать на официальном сайте этой компании по адресу: http://www.opsec.com/developer/gw_comm_mode.html

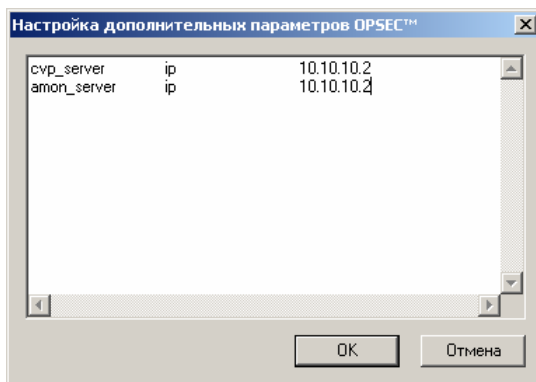


Рисунок 11. Настройка дополнительных параметров OPSEC™

3. Выберите закладку **Параметры** (см. рис. 12). На ней представлены параметры, регулирующие обмен данными между Сервером безопасности и Check Point™ FireWall-1®. Установите нужные значения.
 - Укажите время ожидания Сервером безопасности данных с Check Point™ FireWall-1® в поле **Тайм-аут соединения** раздела **Общие** в секундах. По истечении этого временного интервала, если не поступило никакой информации, соединение Сервера безопасности с Check Point™ FireWall-1® разрывается. Оно будет установлено при первой же передаче Check Point™ FireWall-1® данных на антивирусную обработку. По умолчанию интервал составляет 120 секунд.
 - Установите частоту передачи Сервером безопасности подтверждающего сигнала для поддержки соединения с Check Point™ FireWall-1® в поле **Подтверждение соединения каждые** раздела **Общие** в секундах. По умолчанию предлагается 5 секунд.
 - Для того чтобы зарегистрированные в работе Антивируса Касперского события выводились в журналы событий Check Point™ FireWall-1® и о них проводилось уведомление сред-

ствами Check Point™ FireWall-1®, установите флажок **Сообщать о событиях по протоколу ELA**. После этого:

- Выберите из раскрывающегося списка **Типы уведомлений** значение, определяющее, каким образом будет проводиться уведомление. Чтобы оповещение не производилось, выберите значение **не уведомлять**.
- Установите периодичность, с которой Сервер безопасности будет пытаться возобновить соединение с Check Point™ FireWall-1® в случае его обрыва, в поле **Попытка соединения каждые**.

Информация о событиях, произошедших за время отсутствия соединения, будет передана на Check Point™ FireWall-1® при первом же подключении.

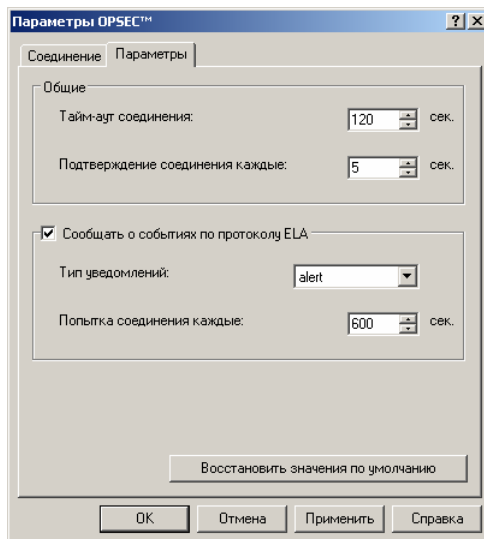


Рисунок 12. Настройка параметров OPSEC™.
Закладка **Параметры**



На Check Point™ FireWall-1® передается информация о следующих событиях:

- обновление антивирусных баз;
- приближение окончания срока действия лицензии;

- изменение состояния приложения (запуск/остановка Сервера безопасности, изменение функциональности приложения).

По умолчанию флажок **Сообщать о событиях по протоколу ELA** не установлен.

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**.

5.6. Минимально необходимая настройка

После настройки параметров взаимодействия с Check Point™ FireWall-1® 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 Сервер безопасности.



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

Настройка приложения производится с рабочего места администратора. Операция может проводиться независимо от того, запущен Check Point™ FireWall-1® или нет.

5.7. Защита без дополнительной настройки

Антивирусная защита начинает работать сразу после настройки параметров взаимодействия Антивируса Касперского и Check Point™ FireWall-1®. По умолчанию предусмотрен следующий режим работы Антивируса:

- Приложение выполняет проверку объектов на наличие всех известных в настоящее время вредоносных программ (установлен стандартный уровень антивирусной защиты).

- Антивирусной защите подлежат данные, перемещаемые по протоколам HTTP, FTP и SMTP.
- Проверяются объекты любых форматов, за исключением объектов-контейнеров выше 32-го уровня вложенности.
- Максимальное время проверки одного объекта составляет 1800 секунд.
- При проверке HTTP-трафика в случае обнаружения зараженного объекта приложение выполняет попытку лечения, вылеченный объект пропускает; если объект неизлечим, блокирует доступ и в окне браузера выводит информационное сообщение следующего формата:

Антивирус Касперского 5.5 для Check Point™ FireWall-1®
Запрошенный адрес "<путь к ресурсу>" содержит **зараженный объект <имя вируса>**. Доступ к ресурсу заблокирован.

Обнаруженные подозрительные и защищенные или поврежденные объекты пропускаются пользователю без изменений.

- При проверке FTP-трафика в случае обнаружения зараженного объекта приложение выполняет попытку лечения, вылеченный объект пропускает; если объект неизлечим, блокирует доступ к ресурсу, в результате на экран выводится сообщение FTP-клиента об ошибке подключения.

Обнаруженные подозрительные и защищенные или поврежденные объекты пропускаются пользователю без изменений.

- При проверке SMTP-трафика в случае обнаружения зараженного объекта приложение выполняет следующие действия:
 - сохраняет исходную копию письма вместе со всеми вложенными файлами в резервном хранилище;
 - удаляет все вложенные в сообщение файлы;
 - тело письма заменяет информационным сообщением следующих форматов:

Антивирус Касперского 5.5 для Check Point™
FireWall-1®

Отправленное Вам сообщение содержит **зараженный объект <имя вируса>**. Сообщение заблокировано.


Подозрительные и защищенные или поврежденные объекты пропускаются пользователю без изменений.

- Обновление антивирусных баз проводится каждый час через интернет с HTTP- и FTP-серверов обновлений Лаборатории Касперского.
- Отчет о результатах антивирусной защиты не формируется.

5.8. Проверка работоспособности приложения

После установки и настройки Антивируса Касперского мы рекомендуем вам проверить правильность настроек и корректность работы приложения с помощью тестового "вируса" и его модификаций. Проверку следует проводить для каждого протокола отдельно.

5.8.1. Тестовый "вирус" EICAR и его модификации

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

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



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

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



Перед загрузкой необходимо отключить антивирусную защиту (см. п. 7.3 на стр. 65), поскольку файл `anti_virus_test_file.htm` будет идентифицирован и обработан Антивирусом как зараженный объект, перемещаемый по HTTP-протоколу.

Не забудьте включить антивирусную защиту сразу после загрузки тестового "вируса".

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.

5.8.2. Тестирование защиты HTTP-трафика



Для проверки обнаружения вирусов в потоке данных, передаваемых по HTTP-протоколу:

загрузите тестовый "вирус" с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

При попытке загрузить тестовый "вирус" Антивирус Касперского обнаружит объект, идентифицирует как зараженный неизлечимый и выполнит действие, установленное в параметрах проверки HTTP-трафика для такого объекта. По умолчанию (см. п. 5.7 на стр. 47), при попытке загрузить тестовый "вирус" соединение с ресурсом будет разорвано, и в окне браузера будет выведено сообщение о том, что данный объект заражен вирусом *EICAR-Test-File*.

5.8.3. Тестирование защиты SMTP-трафика

Для проверки обнаружения вирусов в потоке данных, передаваемых по SMTP-протоколу, вы можете использовать почтовую систему, передача данных в которой осуществляется по этому протоколу.



Для этого:

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 или присоедините к письму файл, содержащий тестовый "вирус".
3. Отправьте письмо на адрес администратора.
4. Ознакомьтесь с содержанием письма, поступившего на указанный адрес.

Антивирус Касперского обнаружит объект, идентифицирует как зараженный и выполнит действие, установленное в параметрах проверки SMTP-трафика для такого объекта. По умолчанию (см. п. 5.7 на стр. 47):

- все вложенные объекты будут удалены;
- тело письма заменено информационным сообщением об обнаруженном вирусе *EICAR-Test-File*;
- исходная копия письма вместе со всеми вложенными файлами будет сохранена в резервном хранилище.

5.8.4. Тестирование защиты FTP-трафика



Для проверки обнаружения вирусов в потоке данных, передаваемых по FTP-протоколу:

1. Разместите тестовый "вирус" на доступном вам ресурсе, обращение к которому осуществляется по FTP-протоколу.
2. Попытайтесь скачать вирус *eicar* с данного ресурса.

В результате Антивирус Касперского обнаружит объект, идентифицирует как зараженный неизлечимый и выполнит действие, установленное в параметрах проверки FTP-трафика для такого объекта. Так, в случае действия настроек по умолчанию (см. п. 5.7 на стр. 47) при попытке загрузить тестовый "вирус" соединение с ресурсом будет разорвано, и на экран будет выведено сообщение об ошибке подключения.

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.

Антивирусные базы Лаборатории Касперского содержат описания следующих категорий объектов:

- а. Всех известных в настоящее время вредоносных программ.
- б. 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.
- в. 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.
- г. Программ, которые не являются вредоносным кодом и не несут никакого ущерба их обладателю, но могут 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.).

Какие категории объектов Антивирус обнаруживает в проходящем через межсетевой экран трафике, определяется установленным уровнем антивирусной защиты (см. п. 7.2 на стр. 64).

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

Приложение скачивает обновления антивирусных баз через интернет с серверов обновлений Лаборатории Касперского или указанного администратором сервера либо из сетевого каталога обновлений. Выбор ресурса зависит от настроек. В качестве каталога обновлений может использоваться папка общего доступа, в которую складываются получаемые из интернета обновления следующие приложения Лаборатории Касперского: Kaspersky Administration Kit 5.0, Антивирус Касперского 5.0 для Windows Workstations и Антивирус Касперского 5.0 для File Servers (см. п. 6.2 на стр. 56).

Загрузка обновлений происходит либо по расписанию, либо вручную. Для успешной загрузки антивирусных баз из интернета необходимо, чтобы ваш компьютер был подключен к нему. Используя сервера обновлений, Антивирус Касперского скачивает с них обновления, после чего устанавливает необходимые файлы на ваш компьютер. Антивирус Касперского предоставляет возможность настроить уведомление о результатах обновления антивирусных баз (см. Глава 12 на стр. 110).

Информацию об используемых приложением антивирусных базах можно посмотреть при помощи гиперссылки [Общие параметры](#) в окне **Общие параметры** на закладке **Общие** (см. рис. 40) и при помощи гиперссылки

[Антивирусная проверка](#) в окне **Антивирусная проверка** на закладке **Обновление** (см. рис. 13). Приводится следующая информация:

- количество записей в антивирусных базах;
- дата и время создания антивирусных баз.



Для обновления антивирусных баз Антивируса Касперского:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** на закладке **Обновление** (см. рис. 13) определите источник получения обновлений. Вы можете выбрать получение обновлений из сетевого каталога (подробнее см. п. 6.1 на стр. 55 и п. 6.2 на стр. 56) или из интернета и настроить параметры подключения.

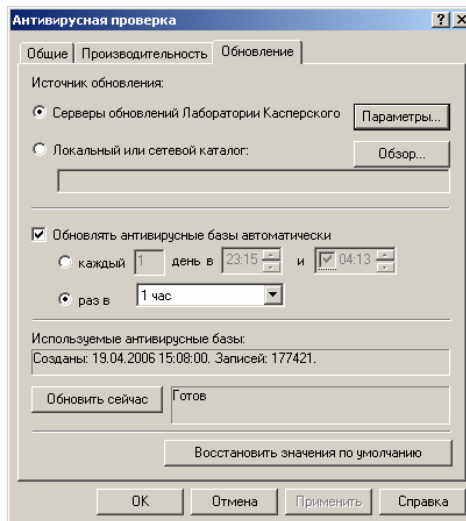


Рисунок 13. Окно настройки параметров обновления антивирусных баз.
Настройка обновления из интернета

3. Для автоматического обновления сформируйте расписание получения обновлений (подробнее см. п. 6.3 на стр. 58). Если обновления необходимы немедленно, получите их вручную при помощи кнопки **Обновить сейчас** (подробнее см. п. 6.4 на стр. 58).



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**.

6.1. Загрузка обновлений из интернета



Для того чтобы Антивирус Касперского получал обновления антивирусных баз через интернет,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** (см. рис. 13) на закладке **Обновление** в качестве источника обновлений выберите **Серверы обновлений Лаборатории Касперского** (данный вариант установлен по умолчанию).
3. После этого нажмите на кнопку **Параметры** и укажите параметры сетевых подключений в открывшемся окне **Параметры обновления через интернет** (см. рис. 14):

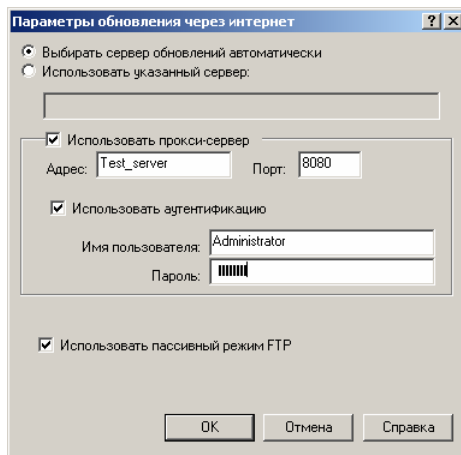


Рисунок 14. Настройка параметров сетевого подключения

- Определите, с какого сервера будут скачиваться обновления. Выберите вариант **Выбирать сервер обновлений автоматически**, для того чтобы сервер выбирался из числа рекомендуемых Лабораторией Касперского, либо вариант **Использовать указанный сервер** и введите адрес нужного HTTP- или FTP-сервера обновлений.
 - 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 пользователя** и **Пароль**.
 - 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, для того чтобы изменения были применены, в окне **Параметры обновления через интернет** нажмите на кнопку **ОК**.
 5. Нажмите на кнопку **Применить** или **ОК** на закладке **Обновление**.

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. Справочное руководство к Kaspersky Administration Kit 5.0). Вы можете использовать данную папку в качестве источника обновлений для Антивируса Касперского.

Возможность сохранять полученные через интернет обновления в папке общего доступа и предоставлять ее в качестве локального источника обновлений существует также в приложениях Антивирус Касперского 5.0 для Windows Workstations и Антивирус Касперского 5.0 для File Servers.



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. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** на закладке **Обновление** (см. рис. 15) в качестве источника обновлений выберите **Локальный или сетевой каталог** и в поле ввода укажите путь к нужному каталогу вручную либо при помощи кнопки **Обзор**.

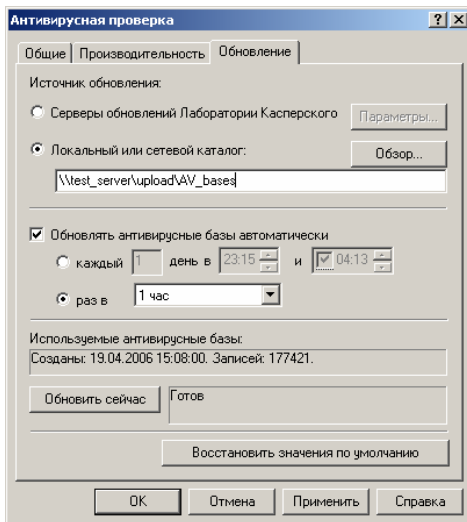


Рисунок 15. Настройка обновлений из сетевого каталога

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**.

6.3. Автоматическое обновление



Для того чтобы обновление антивирусных баз производилось автоматически,

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** на закладке **Обновление** (см. рис. 13) установите флажок **Обновлять антивирусные базы автоматически** и сформируйте расписание получения обновлений. Для этого выберите нужный вариант расписания и установите необходимую периодичность, единицу измерения интервала обновления и время 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 обновлять антивирусные базы с заданной периодичностью в соответствии с установленными параметрами.

6.4. Обновление вручную



Для обновления антивирусных баз вручную:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** на закладке **Обновление** (см. рис. 13) нажмите на кнопку **Обновить сейчас**.



Кнопка **Обновить сейчас** не доступна, если выполняется обновление антивирусных баз либо данная функциональность приложения отключена, например, из-за нарушения лицензии (см. Глава 11 на стр. 102).

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

ГЛАВА 7. АНТИВИРУСНАЯ ЗАЩИТА

Главной задачей Антивируса Касперского является проверка проходящего через Check Point™ FireWall-1® трафика и блокирование или лечение зараженных объектов с использованием информации текущей (последней) версии антивирусных баз.

В зависимости от установленного администратором уровня антивирусной защиты (см. п. 7.1 на стр. 61), приложение позволяет обнаружить:

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

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 межсетевой экран передается программное обеспечение, программы данного класса следует исключить из числа проверяемых объектов.

Если антивирусная защита включена (подробнее см. п. 7.3 на стр. 65), запуск и остановка проверки трафика происходит вместе с запуском и остановкой операционной системы компьютера, на котором установлен Сервер безопасности.

Все перемещаемые через межсетевой экран объекты проверяются в режиме реального времени. По умолчанию обрабатываются HTTP-, FTP- и SMTP-трафики. В случае необходимости (например, трафик поступает на Check Point™ FireWall-1® уже проверенный другим антивирусным приложением) проверку любого из указанных протоколов можно отключить.

В соответствии с установленными для каждого из протоколов параметрами антивирусной проверки приложение:

- выделяет проверяемые объекты;
- выполняет проверку объекта с использованием антивирусных баз;

- пропускает пользователю незараженные объекты, остальные обрабатывает в соответствии с параметрами, перед обработкой копия объекта может быть сохранена в резервном хранилище.

Антивирус Касперского предоставляет возможность настроить уведомление о результатах антивирусной проверки объектов (см. Глава 12 на стр. 110).

При проверке сообщений, перемещаемых по SMTP-протоколу, программа проверяет тело сообщения и все 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, документ Microsoft Word, содержащий макросы). Для уменьшения нагрузки на сервер из антивирусной проверки могут исключаться все объекты-контейнеры выше заданного уровня вложенности.

Для данных, перемещаемых по HTTP- и FTP-протоколам, можно определять дополнительный перечень объектов, не подлежащих антивирусной проверке. Из проверки могут исключаться: архивы, упакованные исполняемые файлы, некоторые типы файлов.

При проверке многотомных архивов и данных, скачиваемых с источника по частям, каждый том и каждая часть воспринимаются и обрабатываются Антивирусом Касперского как отдельный объект. В этом случае приложение сможет обнаружить вредоносный код, только если он целиком содержится в одном из томов или частей. Разделенный на части вредоносный объект Антивирус не сможет найти. В такой ситуации не исключена вероятность распространения вредоносного кода после восстановления целостности объекта.



Многотомные архивы и объекты, скачиваемые по частям, могут быть проверены после сохранения на диске, например, установленным на компьютере Антивирусом Касперского для Windows Workstations.

Для HTTP-протокола Антивирус Касперского предоставляет возможность запретить доступ к объектам, передаваемым по частям (см. п. 7.4 на стр. 66). Для FTP-протокола такая возможность не предусмотрена; чтобы снизить вероятность заражения описанным выше способом, рекомендуется отключить возможность скачивать информацию по частям в настройках Check Point™ FireWall-1®.

Антивирусная проверка увеличивает время доставки информации пользователю. Поэтому при обработке объектов, перемещаемых по HTTP- и FTP-протоколам, предусмотрена возможность передачи непроверенных данных, исключаяющая вероятность доставки зараженного объекта (см.

п. 7.4 на стр. 66). Она предполагает передачу непроверенных данных по частям с максимально-допустимыми интервалами и возможностью удерживать часть данных до окончания проверки объекта. Если в результате антивирусной проверки выясняется, что объект незаражен, пользователю передается оставшаяся часть данных. Во всех остальных случаях соединение с источником разрывается и выводится сообщение о том, что дальнейшая передача данных не возможна. При этом объект обрабатывается в соответствии с параметрами антивирусной проверки, информация о нем фиксируется в журнале событий и в отчете.

Кеширование результатов проверки в течение некоторого временного интервала предоставляет возможность сократить число повторных проверок объекта (см. п. 7.4 на стр. 66).

Антивирус Касперского позволяет одновременно проверять несколько объектов. Число параллельно обрабатываемых объектов зависит от количества запущенных и одновременно работающих экземпляров антивирусного ядра (см. п. 7.7 на стр. 75).

Режим проверки объектов в памяти предоставляет возможность проверять объекты, не сохраняя их в рабочем каталоге на жестком диске. За счет настройки параметров проверки до 1000 объектов объемом до 1024 КБ каждый могут обрабатываться параллельно в оперативной памяти без использования дисковой подсистемы (см. п. 7.7 на стр. 75).

Использование очереди объектов на проверку (см. п. 7.7 на стр. 75) позволяет увеличивать или уменьшать пропускную способность Антивируса Касперского, тем самым регулировать нагрузку в зависимости от объема проходящего через межсетевой экран трафика.

7.1. Антивирусная обработка объектов

По результатам антивирусной проверки каждому объекту присваивается один из следующих статусов:

- **Незараженный** – не содержит вредоносного или потенциально опасного кода.
- **Зараженный** – содержит как минимум один из известных вредоносных или потенциально опасных объектов.
- **Подозрительный** – код объекта похож на код известного или неизвестного вредоносного или потенциально опасного объекта.
- **Защищенный** – объект защищен паролем.

- **Поврежденный** – объект поврежден.

Обнаруженные в результате антивирусной проверки объекты приложение может лечить, блокировать или пропускать без изменений.

Об обнаруженных в результате антивирусной проверки зараженных, подозрительных, защищенных и поврежденных объектах может быть настроено уведомление (см. Глава 12 на стр.110). О незараженных объектах уведомление не производится.

Исходная копия поступившего на обработку объекта может быть сохранена в резервном хранилище для последующего восстановления или удаления.

Возможность лечения предусмотрена только для **зараженных** объектов, передаваемых по HTTP- и FTP-протоколам. При этом для **неизлечимых** объектов может быть задан свой порядок обработки.

7.1.1. Действия над объектами, передаваемыми по HTTP- протоколу

Для лечения **зараженных** объектов, обнаруженных при проверке данных, передаваемых по HTTP-протоколу, предлагаются варианты действий:

- *Лечить* – лечить, вылеченный объект пропускать пользователю. Если объект неизлечим, применить действие, установленное для неизлечимых объектов.
- *Лечить, сохранять копию* - лечить, вылеченный объект пропускать пользователю, сохранять исходную копию объекта в резервном хранилище. Если объект неизлечим, применить действие, установленное для неизлечимых объектов.

Для обработки **зараженных, неизлечимых, подозрительных, защищенных и поврежденных** объектов предусмотрены следующие действия:

- *Пропускать без изменений* – пропускать объект пользователю без каких-либо изменений.
- *Заменять на текст* – блокировать доступ к объекту, выводить в окне браузера информационное сообщение, составленное по шаблону замены.
- *Заменять на текст, сохранять копию* - блокировать доступ к объекту, выводить в окне браузера информационное сообщение, со-

ставленное по шаблону замены, сохранять исходную копию объекта в резервном хранилище.

Копия незараженных и пропущенных без изменения объектов также может быть сохранена в резервном хранилище.

7.1.2. Действия над объектами, передаваемыми по FTP-протоколу

Для лечения **зараженных** объектов, обнаруженных при проверке данных, передаваемых по FTP-протоколу, предлагаются варианты действий:

- *Лечить* – лечить, вылеченный объект пропускать пользователю. Если объект неизлечим, к нему применить действие, установленное для неизлечимых объектов.
- *Лечить, сохранять копию* - лечить, вылеченный объект пропускать пользователю, сохранять исходную копию объекта в резервном хранилище. Если объект неизлечим, к нему применить действие, установленное для неизлечимых объектов.

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

- *Пропускать без изменений* – пропускать объект пользователю без каких-либо изменений.
- *Блокировать* – блокировать доступ к объекту, в результате в окне браузера будет выводиться сообщение FTP-клиента об ошибке передачи данных.
- *Блокировать, сохранять копию* - блокировать доступ к объекту, сохранять исходную копию объекта в резервном хранилище. В результате в окне браузера будет выводиться сообщение FTP-клиента об ошибке передачи данных.

Копия незараженных и пропущенных без изменения объектов также может быть сохранена в резервном хранилище.

7.1.3. Действия над объектами, передаваемыми по SMTP-протоколу

Для обработки **зараженных, подозрительных, защищенных и поврежденных** объектов, обнаруженных при проверке данных, передаваемых по SMTP-протоколу, предусмотрены следующие действия:

- *Пропускать без изменений* – пропускать объект пользователю без каких-либо изменений.
- *Заменять на текст* – удалять все вложенные в сообщение файлы, тело письма заменять информационным сообщением, составленным по шаблону замены.
- *Заменять на текст, сохранять копию* - удалять все вложенные в сообщение файлы, тело письма заменять информационным сообщением, составленным по шаблону замены, сохранять исходную копию сообщения (тело письма и все вложенные файлы) в резервном хранилище.

Выбранное действие выполняется над всем письмом, не зависимо от того, где обнаружен зараженный, подозрительный, защищенный и поврежденный объект в теле письма или в каком-либо из вложенных файлов.

Копия незараженных и пропущенных без изменения объектов также может быть сохранена в резервном хранилище.

7.2. Уровень антивирусной защиты

Антивирус Касперского позволяет определять в проходящем через межсетевой экран трафике все известные на сегодняшний день вредоносные и потенциально опасные программы. Описания этих программ и способов лечения зараженных ими объектов содержат антивирусные базы Лаборатории Касперского (см. Глава 6 на стр. 52). Какие категории объектов обнаруживает Антивирус, определяется установленным уровнем антивирусной защиты.

В приложении предусмотрены следующие уровни защиты:

- **Стандартная антивирусная защита:** защита от всех известных в настоящее время вредоносных программ. Данный уровень установлен по умолчанию.

- **Расширенная антивирусная защита:** защита от всех известных в настоящее время вредоносных программ и потенциально опасных программ, перечисленных в пункте б приведенного на стр. 52 списка.
- **Избыточная антивирусная защита:** защита от всех известных в настоящее время вредоносных программ и потенциально опасных программ, перечисленных в пунктах б, в и г приведенного на стр. 52 списка.

7.3. Включение и отключение антивирусной защиты. Выбор уровня

Если антивирусная защита включена, то вместе с запуском и остановкой операционной системы компьютера, на котором установлен Сервер безопасности, происходит запуск антивирусной проверки проходящего через межсетевой экран трафика. По умолчанию выполняется проверка HTTP-, FTP- и SMTP- протоколов. Для снижения нагрузки на сервер вы можете отключить проверку трафика в настройках для каждого протокола отдельно.

Проверка объектов выполняется в соответствии с установленным уровнем антивирусной защиты.

Если антивирусная защита отключена, не проверяется трафик ни одного из протоколов.



Следует помнить, что отключение антивирусной защиты значительно повышает вероятность проникновения вредоносных программ через межсетевой экран. 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 проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** на закладке **Общие** (см. рис. 16) в группе полей **Антивирусная защита** выберите:
 - **Выключена** для того чтобы отключить антивирусную проверку данных, проходящих через межсетевой экран.

- **Стандартная антивирусная защита, Расширенная антивирусная защита** или **Избыточная антивирусная защита** для того чтобы включить антивирусную проверку 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 может быть отнесен к потенциально опасным программам.

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

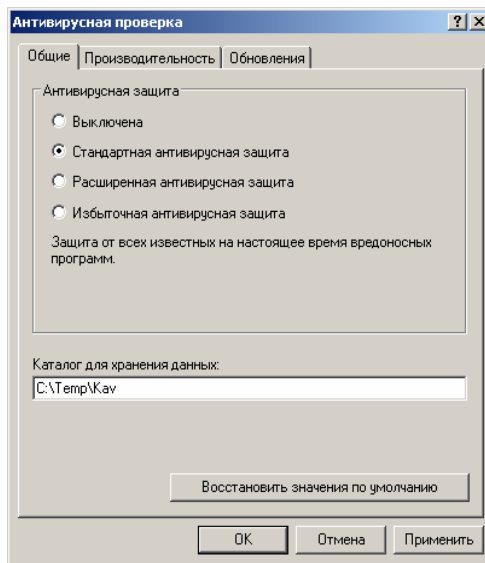


Рисунок 16. Включение антивирусной защиты

7.4. Проверка HTTP-трафика



Для настройки параметров проверки данных, передаваемых по HTTP-протоколу:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Параметры проверки HTTP](#) в панели результата.

В открывшемся окне **Параметры проверки HTTP** (см. рис. 17) определите значения параметров работы антивируса на представленных закладках.

2. На закладке **Параметры** (см. рис. 17) установите флажок **Проверять HTTP-трафик**, для того чтобы проверка выполнялась. После этого определите значения параметров, регулирующих:

- передачу непроверенных данных пользователю в случае, если проверка объекта затягивается;
- проверку объекта при повторном обращении;
- передачу пользователю данных, скачиваемым с источника по частям.

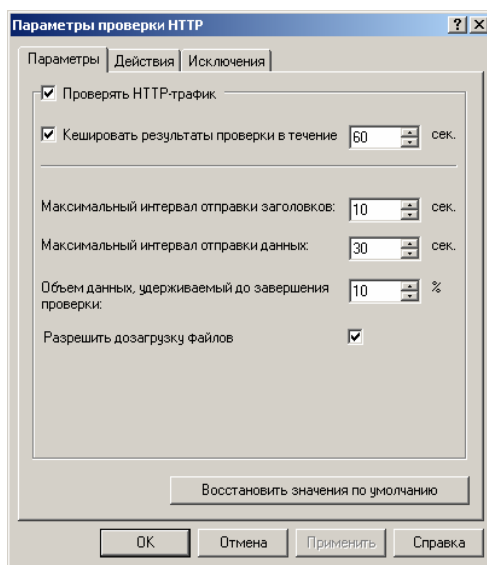


Рисунок 17. Параметры проверки HTTP-трафика.
Закладка **Параметры**

- Для сокращения количества повторных проверок объекта установите флажок **Кешировать результаты проверки в течение** и укажите время в секундах, в течение которого программа будет "помнить" результат проверки. При повторном запросе объекта в течение заданного интервала пользователь сразу же получит доступ к объекту либо уве-

домление о результате его проверки. По умолчанию флажок установлен, интервал составляет 60 секунд.

- Для того чтобы клиентская программа, запросившая поток, не разрывала соединение и не выводила сообщение о неудачной попытке подключения, в течение всей проверки Антивирус Касперского с заданной частотой передает служебную информацию (как правило, это заголовки HTTP-протокола) и небольшие пакеты данных. Укажите в секундах величину временного интервала отправки очередного пакета данных в поле **Максимальный интервал отправки заголовков**. Значение параметра устанавливается, исходя из характеристик программы-клиента, и не должно превышать время, по истечении которого клиент выводит сообщение о неудачной попытке подключения по указанному адресу. По умолчанию предлагается 10 секунд.
 - Укажите максимально-допустимый интервал ожидания пользователем очередного пакета данных в поле **Максимальный интервал отправки данных** (30 секунд по умолчанию). Параметр определяет, с какой скоростью будут предоставляться пользователю реальные данные.
 - Установите, какой процент от общего объема непроверенных данных должен удерживаться до окончания проверки объекта в поле **Объем данных, удерживаемый до завершения проверки**. Чем больше значение данного параметра, тем меньше вероятность заражения при передаче пользователю непроверенных данных. По умолчанию предлагается 10%.
 - Для того чтобы разрешить доставку пользователю файлов, скачиваемых частями, установите флажок **Разрешить загрузку файлов**. Если флажок не установлен, при обнаружении такого объекта соединение с источником разрывается и выводится сообщение о том, что дальнейшая передача данных не возможна. По умолчанию флажок установлен.
3. На закладке **Действия** (см. рис. 18) укажите, какие действия будут выполняться при обнаружении зараженных, неизлечимых, подозрительных и защищенных или поврежденных объектов. Определите порядок обработки для каждого статуса отдельно. Для этого выберите нужное действие из раскрывающегося списка в соответствующем разделе.

Если вы выбираете действие, предполагающее замену объекта, следует сформировать шаблон замещения. Для этого нажмите на кнопку **Шаблон замены** и в открывшемся окне (см.

рис. 19) введите текст сообщения. В его состав может включаться информация об обнаруженном вирусе, HTTP-адрес зараженного объекта и информация о возникшей при подключении ошибке. Для этого добавьте в шаблон соответствующие макросы подстановки, выбрав их из раскрывающегося при помощи кнопки **Макросы** списка.

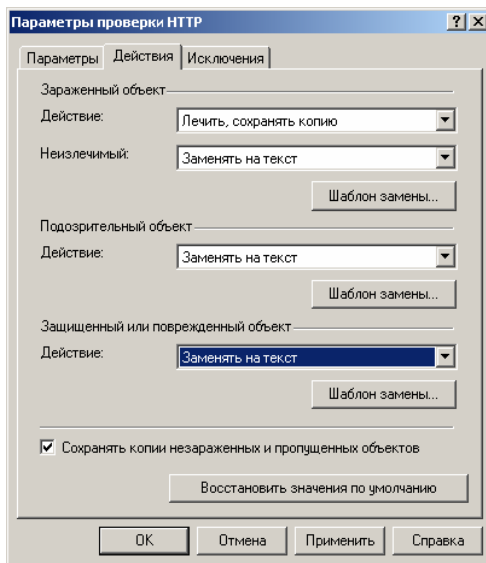


Рисунок 18. Параметры проверки HTTP-трафика.
Закладка **Действия**

Для того чтобы в резервном хранилище сохранялись копии незараженных и пропущенных без изменения объектов, установите флажок **Сохранять копии незараженных и пропущенных объектов**.



Для **зараженных** объектов при установке флажка **Сохранять копии незараженных и пропущенных объектов** действие **Лечить** будет заменено на действие **Лечить, сохранять копию**. При этом будут сохраняться исходные копии вылеченных объектов и неизлечимых объектов, если для них было выбрано действие **Пропустить без изменений**.

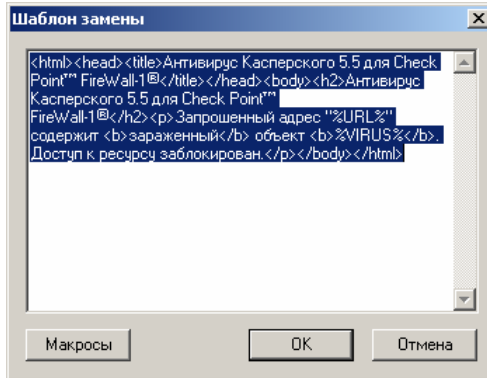
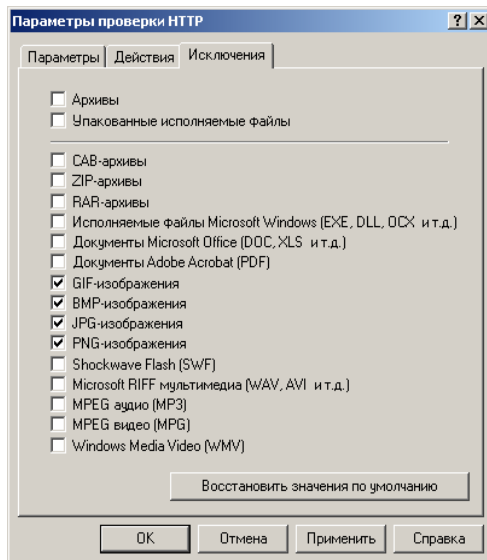


Рисунок 19. Создание шаблона замены

- На закладке **Исключения** (см. рис. 20) определите перечень объектов, которые не будут проверяться на присутствие вредоносного кода. Для этого установите флажки рядом с нужными названиями в представленном списке типов.

Рисунок 20. Параметры проверки HTTP-трафика.
Закладка **Исключения**

- Чтобы изменения вступили в силу, нажмите на кнопку **Применить** или **OK**.

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



Чтобы отключить проверку данных, передаваемых по HTTP-протоколу,

в окне **Параметры проверки HTTP** на закладке **Параметры** (см. рис. 17) снимите флажок **Проверять HTTP-трафик** и нажмите на кнопку **Применить** или **ОК**.

7.5. Проверка FTP-трафика



Для настройки параметров проверки данных, передаваемых по FTP-протоколу:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Параметры проверки FTP](#) в панели результата.

В результате открывается окно **Параметры проверки FTP** (см. рис. 21). Определите значения параметров работы антивируса при проверке FTP-трафика на представленных закладках.

Настройка параметров проводится так же, как и для HTTP-трафика (см. п.7.4 на стр. 66).

2. Для того чтобы проверка выполнялась, на закладке **Параметры** (см. рис. 21) установите флажок **Проверять FTP-трафик**. После этого определите значения параметров, регулирующих передачу непроверенных данных пользователю в случае, если проверка объекта затягивается.
3. На закладке **Действия** (см. рис. 22) укажите, какие действия будут выполняться при обнаружении зараженных, неизлечимых, подозрительных и защищенных или поврежденных объектов.

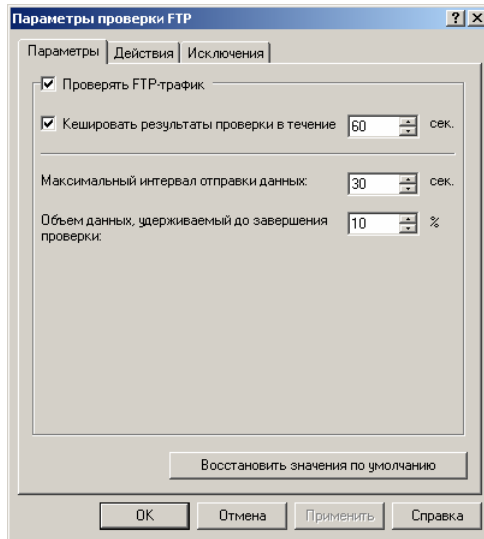


Рисунок 21. Параметры проверки FTP-трафика.
Закладка **Параметры**

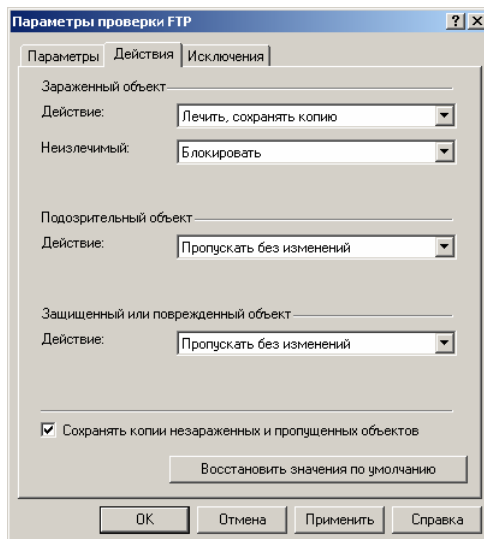


Рисунок 22. Параметры проверки FTP-трафика.
Закладка **Действия**

4. На закладке **Исключения** (см. рис. 23) определите перечень объектов, которые не будут проверяться на присутствие вредоносного кода. Для этого установите флажки рядом с названиями представленных типов файлов.

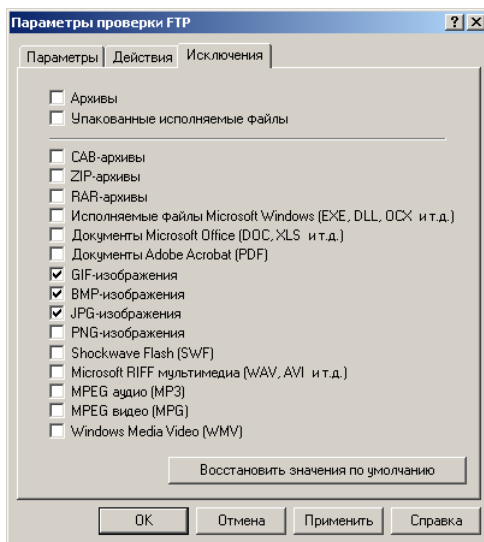


Рисунок 23. Параметры проверки FTP-трафика.
Закладка **Исключения**

6. 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**.



Чтобы отключить проверку данных, передаваемых по FTP-протоколу,

в окне **Параметры проверки FTP** на закладке **Параметры** (см. рис. 21) снимите флажок **Проверять FTP-трафик** и нажмите на кнопку **Применить** или **ОК**.

7.6. Проверка SMTP-трафика



Для настройки параметров проверки данных, передаваемых по SMTP-протоколу:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Параметры проверки SMTP](#) в панели результата.

В результате открывается окно **Параметры проверки SMTP** (см. рис. 24).

2. Для того чтобы проверка трафика выполнялась, установите флажок **Проверять SMTP-трафик** (см. рис. 24) на закладке **Параметры**.

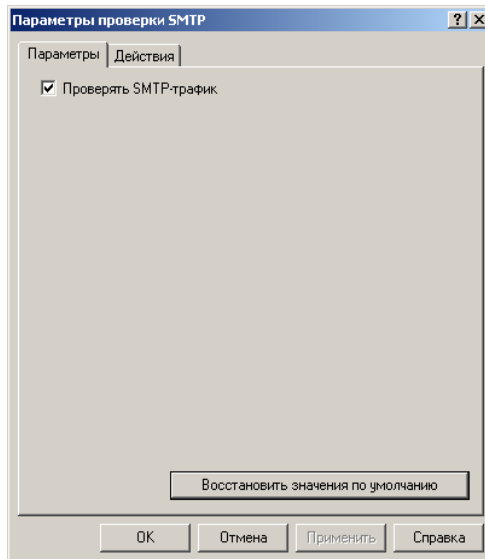


Рисунок 24. Параметры проверки SMTP-трафика.
Закладка **Параметры**

3. На закладке **Действия** (см. рис. 25) укажите, какие действия будут выполняться при обнаружении зараженных, подозрительных и защищенных или поврежденных объектов. Настройка параметров проводится так же, как и для HTTP-трафика (см. п.7.4 на стр. 66).

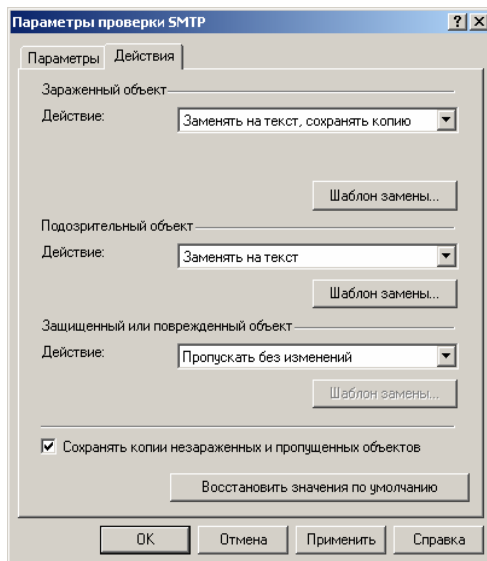


Рисунок 25. Параметры проверки SMTP-трафика.
Закладка **Действие**

4. 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**.



Чтобы отключить проверку данных, передаваемых по SMTP-протоколу,

в окне **Параметры проверки SMTP** на закладке **Параметры** (см. рис. 24) снимите флажок **Проверять SMTP-трафик** и нажмите на кнопку **Применить** или **ОК**.

7.7. Производительность антивирусной проверки



Для настройки параметров производительности антивирусной проверки:

1. Выберите в дереве консоли узел, соответствующий нужному серверу, и воспользуйтесь гиперссылкой [Антивирусная проверка](#) в панели результата.
2. В открывшемся окне **Антивирусная проверка** (см. рис. 26) выберите закладку **Производительность** и установите значения представленных на ней параметров:

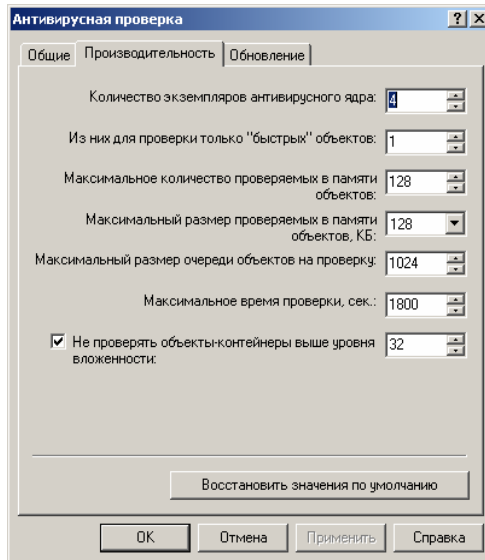


Рисунок 26. Настройка производительности Антивируса Касперского

- Количество параллельно работающих экземпляров антивирусного ядра. По умолчанию создаются и одновременно работают 4 экземпляра. Вы можете установить значение в интервале от 1 до 32. Компания Microsoft рекомендует назначать число, не превышающее количество процессоров компьютера, на котором установлен Сервер безопасности, умноженное на 4.
- Количество экземпляров антивирусного ядра, резервируемых для прохождения рабочего ("быстрого") трафика. Параметр позволяет снизить влияние проверки больших объектов на пропускную способность Антивируса Касперского. По умолчанию предлагается 1.

К "быстрым" объектам относятся только объекты HTTP-трафика, соответствующие следующим критериям:

- текстовые объекты размером менее 2 МБ;
 - *html*-файлы размером менее 2 МБ;
 - графические объекты размером менее 2 МБ;
 - все остальные объекты (за исключением приложений) размером менее 256 КБ.
- Максимальное количество объектов, проверяемых в оперативной памяти без сохранения в рабочем каталоге на диске. Вы можете установить значение в интервале от 1 до 1000. По умолчанию предлагается 128.
 - Максимальный размер для проверяемых в памяти объектов в килобайтах. Выберите нужное значение из раскрывающегося списка.



Если очередь целиком заполнена или размер объекта превышает установленное ограничение, объект будет сохранен и проверен в рабочем каталоге, расположенном в каталоге данных приложения.

Все файлы размером более 1024 КБ сохраняются для обработки в рабочем каталоге.



Значения параметров проверки объектов в памяти должны определяться, исходя из аппаратных характеристик компьютера, на котором установлен Сервер безопасности.

Суммарный объем проверяемых объектов не должен превышать размер свободной оперативной памяти.

- Размер очереди объектов на проверку - максимальное количество объектов, проверяемых и ожидающих проверки на диске в рабочем каталоге. Вы можете установить значение в интервале от 1 до 16383. По умолчанию предлагается 1024.



Если очередь целиком заполнена, новый объект не будет проверен, будет признан незараженным и отправлен запросившему его клиенту.

- Максимальное время, отведенное на проверку одного объекта (в секундах). Укажите значение в интервале от 0 до 86400 секунд включительно. Значение по умолчанию – 1800 секунд.



Если объект не удалось проверить в течение указанного времени, он будет признан незараженным и отправлен запросившему его клиенту.

Для того чтобы исключить из проверки объекты-контейнеры, установите флажок **Не проверять объекты-контейнеры выше уровня вложенности** и определите уровень проверки (32 по умолчанию). 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.

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



Параметры проверки объектов в оперативной памяти будут применены только после перезагрузки операционной системы компьютера, на котором установлен Сервер безопасности либо остановки и запуска службы Антивирус Касперского 5.5 для Check Point™ FireWall-1® вручную через **Управление компьютером / Услуги**.

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

ГЛАВА 8. РЕЗЕРВНОЕ ХРАНИЛИЩЕ

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 (см. п. 0 на стр. 84) либо удален (см. п. 8.4 на стр. 86). Возможность восстановления объекта может быть полезна, например, если при его лечении были утеряны данные, объект был удален по ошибке или необходимо провести повторное лечение объекта с использованием обновленной версии антивирусных баз, например, установленным в сети Антивирусом Касперского для Windows Workstations.



Резервная копия объекта создается, только если это предусмотрено значением параметров антивирусной проверки.

При создании резервной копии объекта, передаваемого по протоколам HTTP и FTP, в резервном хранилище размещается объект, к которому проходило обращение. Для объекта, перемещаемого по протоколу SMTP, сохраняется тело письма и все входящие в него вложения, не зависимо от того, где был обнаружен вредоносный объект.

Резервное хранилище представляет собой служебный каталог. Он создается в каталоге данных приложения при установке Сервера безопасности.

Объем информации в резервном хранилище может быть ограничен по следующим параметрам: размеру резервного хранилища и времени хранения объекта. По умолчанию максимальный размер хранилища составляет 1024 МБ, время хранения – 30 дней. Администратор может изменить значения параметров ограничения (см. п. 8.5 на стр. 87).

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

- удаляет объекты, срок хранения которых закончился;
- если для размещения объекта все-таки недостаточно памяти, освобождает необходимый объем за счет удаления наиболее старых объектов;



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

Просмотр резервного хранилища (см. п. 8.1 на стр. 80), настройка его параметров (см. п. 8.5 на стр. 87) и работа с резервными копиями объектов (см. п. 0 на стр. 84 и п. 8.4 на стр. 86) осуществляется через служебную папку **Резервное хранилище** (см. рис. 27). Данная папка входит в состав каждого узла, отображающего управляемый сервер.

Для удобства просмотра и поиска информации в резервном хранилище, а также ее структурирования предусмотрена возможность настройки пользовательских фильтров (см. п. 8.2 на стр. 81). Сформированные для резервного хранилища фильтры отображаются в папке **Резервное хранилище** в виде вложенных подпапок с именами, заданными администратором при их создании.

8.1. Просмотр резервного хранилища



Для просмотра резервного хранилища:

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

После этого в панели результатов будет представлена таблица (см. рис. 27), содержащая полный перечень всех объектов, размещенных в резервном хранилище.

Протокол	Описание	Откуда	Куда	Размер	Статус	Вирус	Время обнаружения
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	5592	Зараж...	EISA...	26.04.2006 8:17:26
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	23040	Зараж...	EISA...	26.04.2006 8:17:54
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	23040	Вылеч...	EISA...	26.04.2006 8:32:30
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	23040	Вылеч...	EISA...	26.04.2006 8:33:36
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	23040	Вылеч...	EISA...	26.04.2006 8:33:41
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	37376	Вылеч...	Virus...	26.04.2006 8:33:49
HTTP	http://10.10.10...	10.10.10.2	10.10.10.5	74784	Вылеч...	Virus...	26.04.2006 8:35:22

Рисунок 27. Просмотр резервного хранилища

Для каждого объекта в таблице отображается следующая информация:

- **Протокол.** Тип протокола, при проверке которого был обнаружен объект.

- **Описание.** HTTP-, FTP-адрес источника либо тема письма для объектов, перемещаемых по протоколу SMTP.
- **Откуда.** IP-адрес источника, где размещен объект либо электронный адрес отправителя для объектов, перемещаемых по протоколу SMTP.
- **Куда.** IP-адрес компьютера, с которого запросили объект либо электронный адрес получателя для объектов, перемещаемых по протоколу SMTP.
- **Размер.** Размер объекта в байтах.
- **Статус.** Статус, присвоенный объекту в результате антивирусной проверки: **зараженный, вылеченный, подозрительный, защищенный/поврежденный** (см. п. 7.1 на стр. 61).



В резервном хранилище размещается **копия** объекта **до того**, как он был обработан Антивирусом. Поле **Статус** показывает состояние объекта **после** обработки.

- **Вирус.** Имя обнаруженного вируса либо подозрительного программного обеспечения (заполняется только для объектов со статусом **зараженный, вылеченный** и **подозрительный**).
- **Время обнаружения.** Точная дата и время, когда объект был обнаружен Антивирусом Касперского.

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

8.2. 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 **Новый фильтр** контекстного меню или аналогичным пунктом в меню **Действие**. В результате открывается окно настройки фильтра (см. рис. 28).

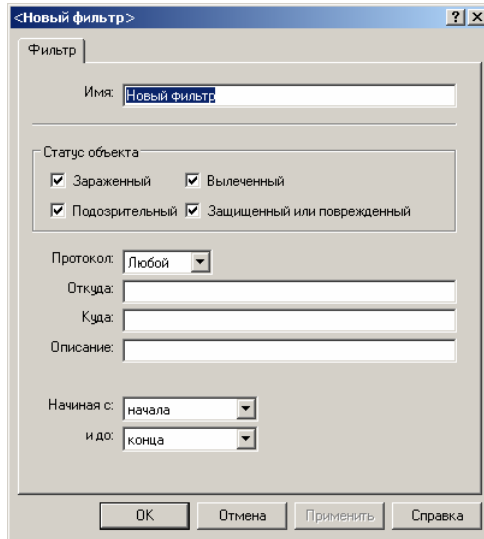


Рисунок 28. Создание фильтра

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. Вы можете указать значение любого числа параметров. Обязательным для ввода является только имя фильтра.

Для настройки параметров может использоваться следующая информация об объекте:

- статус объекта (можно выбрать несколько значений);
- протокол, при проверке которого был обнаружен объект. Для отображения информации по всем протоколам, следует выбрать из раскрывающегося списка значение **Любой**;
- IP-адрес источника, где размещен объект либо электронный адрес отправителя для объектов, перемещаемых по протоколу SMTP;

- IP-адрес компьютера, с которого запросили объект либо электронный адрес получателя для объектов, перемещаемых по протоколу SMTP.
 - HTTP-, FTP-адрес источника либо тема письма для объектов, перемещаемых по протоколу SMTP;
 - временной интервал, в течение которого был обнаружен объект.
4. По окончании настройки параметров фильтра 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 его критериям.

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. 29).
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**.

Рисунок 29. Настройка фильтра

8.3. 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. 27), выберите объект для восстановления. Для поиска объекта вы можете использовать фильтр (см. п. 8.2 на стр. 81).
3. Откройте контекстное меню и воспользуйтесь командой **Получить файл** или аналогичным пунктом в меню **Действие**.
4. В результате выводится предупреждающее сообщение (см. рис. 30) с запросом на продолжение операции. Для восстановления объекта нажмите на кнопку **Да**.

5. В открывшемся окне (см. рис. 31) укажите каталог, в котором будет сохранен восстановленный объект и, если это необходимо, введите или измените имя объекта.

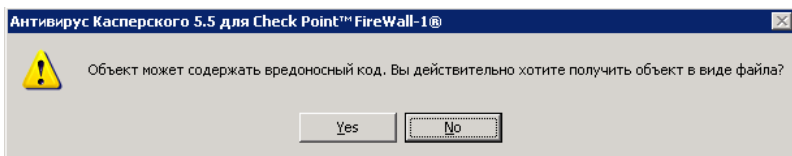


Рисунок 30. Подтверждение восстановления объекта

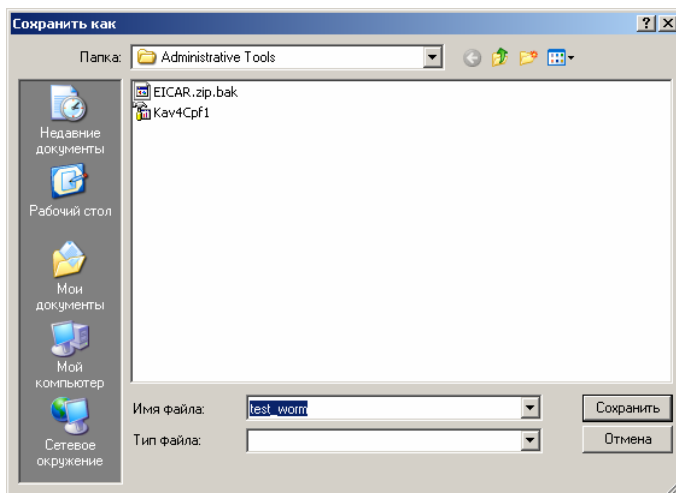


Рисунок 31. Восстановление объекта из резервного хранилища

В результате объект перемещается из резервного хранилища в указанный каталог 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**. При повторной проверке, например, Антивирусом Касперского для Windows Workstations с использованием обновленной версии антивирусных баз объект может быть вылечен или в нем обнаружен ранее неизвестный вирус.

Восстановление других объектов может привести к заражению вашего компьютера.

8.4. Удаление объекта из резервного хранилища

Из резервного хранилища автоматически удаляются следующие объекты:

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

Предусмотрена также возможность удаления объекта из резервного хранилища вручную. Она может быть полезна для удаления успешно восстановленных 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. 27), выберите объект для удаления. Для поиска объекта вы можете использовать фильтр (см. п. 8.2 на стр. 81).
3. Откройте контекстное меню и воспользуйтесь командой **Удалить** или аналогичным пунктом в меню **Действие**.

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

8.5. 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. 32) установите необходимые значения параметров.

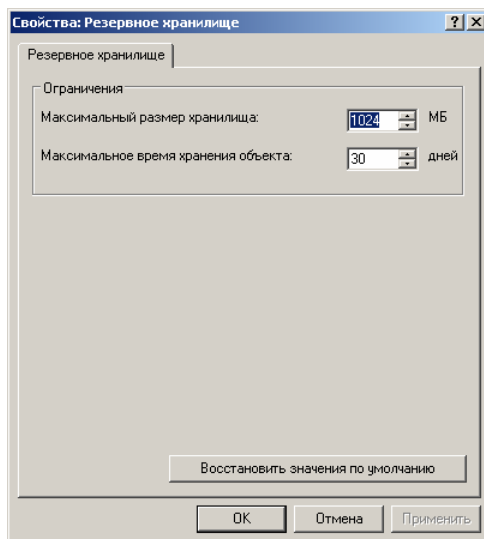


Рисунок 32. Настройка параметров резервного хранилища

В поле **Максимальный размер хранилища** укажите максимальный суммарный объем объектов, которые могут храниться в резервном хранилище. По умолчанию он составляет 1024 МБ.

В поле **Максимальное время хранения объекта** установите максимальный срок хранения объектов в резервном хранилище в днях. 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**.

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

ГЛАВА 9. ОТЧЕТЫ

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

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

- общие результаты проверки:
 - общее количество проверенных объектов;
 - суммарный размер проверенных объектов (в байтах);
- об обнаруженных вредоносных объектах;
- об источниках зараженных объектов;
- о производительности антивирусной проверки:
 - средняя скорость проверки (объектов в секунду);
 - средняя скорость проверки (байт в секунду);
 - максимальная достигнутая скорость проверки.

Отчет формируется автоматически, в соответствии с расписанием или по запросу и сохраняется в виде *html-страницы* в каталоге хранения отчетов. Имя файла отображает дату и время создания отчета и имеет формат **<ДД.ММ.ГГГГ ЧЧ-ММ-СС>**. Антивирус Касперского предоставляет возможность настроить уведомление о результатах формирования отчетов (см. Глава 12 на стр. 110).

Хранилищем отчетов на сервере по умолчанию является каталог **Reports**. Он создается в каталоге данных приложения. В качестве хранилища отчета может быть задан любой другой каталог по выбору администратора (см. п. 9.2 на стр. 93). Срок хранения отчетов на сервере и размер хранилища отчетов не ограничены. Удаление отчетов осуществляется вручную через файловую систему.

Для просмотра отчетов используется браузер, установленный в системе по умолчанию (см. п. 9.3 на стр. 95).

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

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

Перечень сформированных шаблонов отчетов отображается в панели результатов в виде таблицы (см. рис. 33).

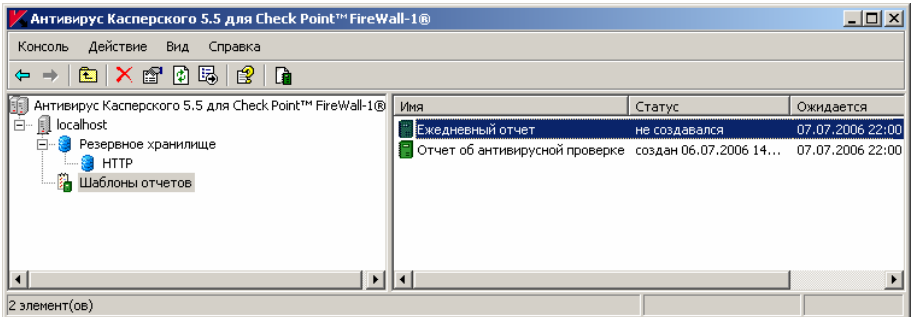


Рисунок 33. Папка **Шаблоны отчетов**

Для каждого шаблона таблица помимо имени содержит следующую информацию:

- **Статус:** статус отчета, формируемого по шаблону.
- **Ожидается:** дата и время создания очередного отчета по расписанию либо **по требованию**, если автоматическое формирование отчета отключено.

В зависимости от того, на каком этапе находится создание отчета, статус отчета может иметь одно из следующих значений:

- создается с <дата и время создания отчета по расписанию>;
- создан <дата и время создания отчета>;
- не создавался;
- ошибка;
- ошибка создания в <дата и время возникновения ошибки>.

Подробно с параметрами шаблона отчета можно ознакомиться, вызвав окно его настройки при помощи команды контекстного меню **Свойства** (см. п. 9.2 на стр. 93).

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

9.1. Получение отчета



Для получения отчета о результатах антивирусной проверки:

1. Создайте шаблон отчета (см. п. 9.2 на стр. 93) или выберите существующий.
2. Установите флажок **Формировать отчет** на закладке **Общие** окна настройки шаблона отчета (см. рис. 35).

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

Чтобы ознакомиться с результатами антивирусной проверки, следует посмотреть отчет за соответствующий отчетный период (см. п. 9.3 на стр. 95).

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



Для получения отчета о результатах антивирусной проверки по запросу:

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. В таблице, отображающей перечень сформированных шаблонов (см. рис. 33), 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. 35).

Отчет формируется на основании сохраняемой приложением информации о результатах антивирусной проверки. Для уменьшения объема информации может быть ограничен срок ее хранения. По умолчанию он составляет один год.

Объем выводимой в отчетах информации об источниках зараженных объектов и об обнаруженных вредоносных объектах ограничен и не может превышать 10 строк. Предоставляется информация о десяти наиболее

зараженных источниках и первые десять по количеству обнаружений типов вредоносных объектов.



Чтобы ограничить срок хранения информации о результатах антивирусной проверки,

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. 34):
 - установите флажок **Хранить отчетную статистику**.
 - укажите период хранения информации и выберите единицу измерения времени.

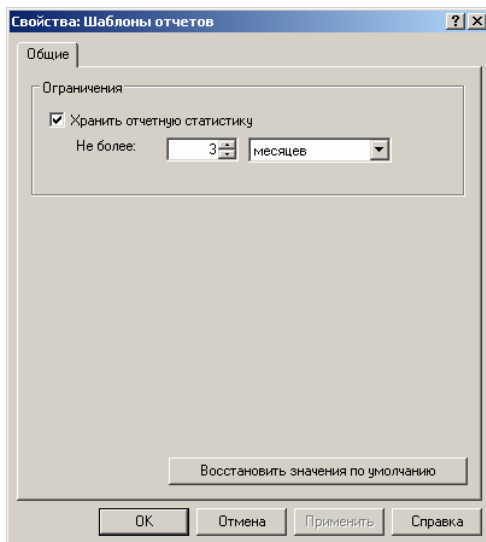


Рисунок 34. Настройка параметров отчета

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**.

9.2. 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 отчета** или аналогичным пунктом в меню **Действие**.
3. В результате открывается окно настройки шаблона отчета **<Новый шаблон отчета>** (см. рис. 35), состоящее из закладок **Общие** и **Параметры**. Установите нужные значения для параметров, представленных на закладках.

На закладке **Общие** (см. рис. 35) выполните следующие действия:

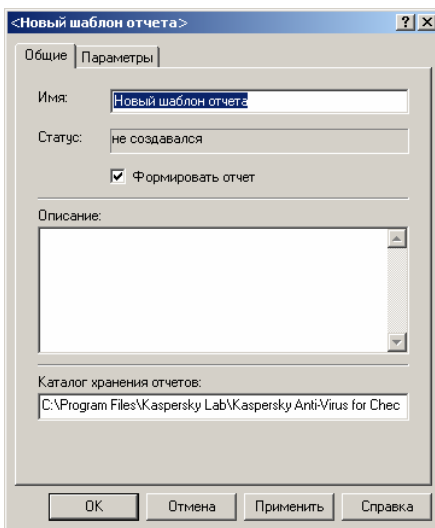


Рисунок 35. Шаблон отчета. Закладка **Общие**

- Введите имя шаблона в поле **Имя**.
- Укажите, будут автоматически формироваться отчеты на основании данного шаблона или нет. Для этого установите или снимите флажок **Формировать отчет**.

- Если необходимо, введите более подробное описание отчета, который будет создаваться по шаблону, в поле **Описание**.
- Укажите путь к каталогу, в котором сформированные отчеты будут сохраняться. По умолчанию это каталог **Reports**, расположенный на сервере в каталоге данных приложения. Вы можете указать другой каталог вручную. Если каталога с таким именем не существует, он будет создан приложением.

На закладке **Параметры** (см. рис. 36) укажите отчетный период и установите параметры расписания создания отчета.

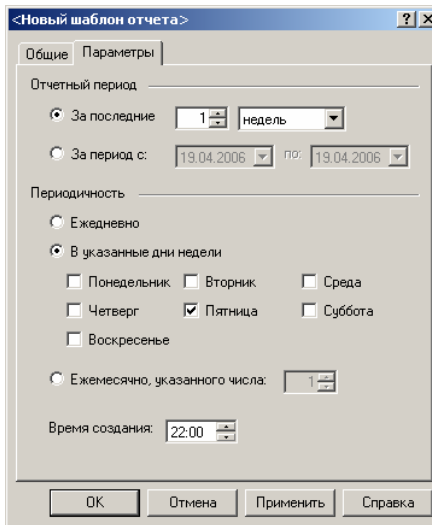


Рисунок 36. Шаблон отчета. Закладка **Параметры**

- 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** вы-

берите вариант **За период** и установите необходимые даты в полях **С** и **по**.

- Для создания расписания в разделе **Периодичность**:
 - 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 создания**.

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.

9.3. Просмотр отчета



Для просмотра отчета через файловую систему:

1. Зайдите в каталог размещения отчетов. По умолчанию это каталог **Reports**, расположенный на сервере в каталоге данных приложения.
2. Выберите и запустите *htm*-файл с именем, соответствующим дате и времени создания отчета в формате **<ДД.ММ.ГГГГ ЧЧ-ММ-СС>**.

В результате загружается браузер, установленный в системе по умолчанию. В главном окне браузера представлен отчет о результатах антивирусной проверки (см. рис. 37). Сразу после загрузки отчет отображает общие результаты проверки. Отчетный период указан в заголовке.

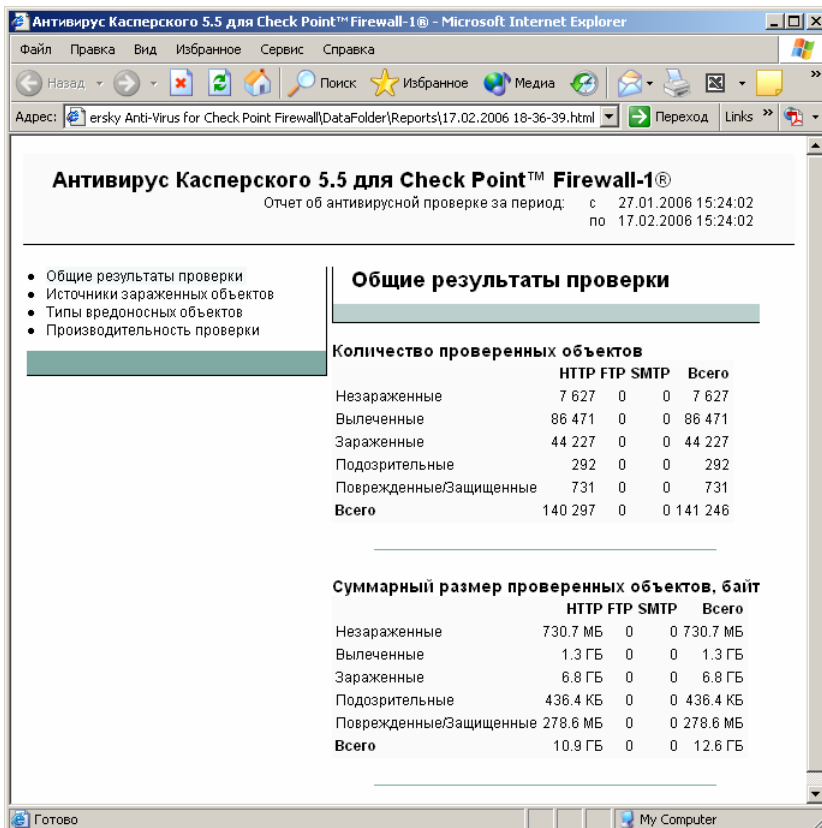


Рисунок 37. Просмотр отчета. Общие результаты проверки

В левой части отчета отображается перечень разделов – 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.



Для просмотра отчета через Консоль управления:

1. Выберите в дереве консоли папку **Шаблоны отчетов**.
2. В таблице, отображающей перечень сформированных шаблонов (см. рис. 33), выберите необходимый шаблон отчета.

3. Откройте контекстное меню и воспользуйтесь командой **Просмотреть отчет** или аналогичным пунктом в меню **Действие**.
4. В результате на экран будет выведен последний из сформированных по выбранному шаблону отчетов. Просмотр реализован с помощью браузера, установленного в системе по умолчанию.

Если по шаблону не было сформировано ни одного отчета, выводится информационное сообщение (см. рис. 38). В этом случае сформируйте отчет и повторно вызовите его на просмотр через консоль.

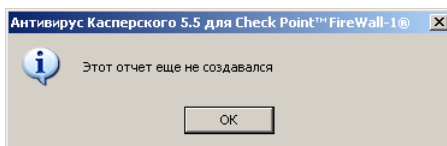


Рисунок 38. Сообщение о том, что по шаблону отчет не создавался

ГЛАВА 10. ЖУРНАЛЫ СОБЫТИЙ ПРИЛОЖЕНИЯ

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

Полнота информации, выводимой в журналы, зависит от установленных в параметрах приложения уровней диагностики (см. п. 10.1 на стр. 99).

Просмотр событий, зарегистрированных в журнале приложений Windows, осуществляется при помощи стандартного приложения Microsoft Windows **Просмотр событий**. В графе **Источник** для Антивируса Касперского прописывается строка **Kav4Cpf1**.



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

В приложении предусмотрено два типа журналов: журнал работы приложения и журнал результатов антивирусной проверки. В зависимости от типа файлы журналов имеют следующую структуру имен:

Kav4Cpf1_ДАТА.log – журнал Антивируса Касперского, содержащий информацию о работе приложения в заданном вами объеме на определенную дату. В качестве *ДАТА* в названии файла приводится дата его создания в формате **ГГГГММДД**. Например: *Kav4Cpf1_20050410.log*.

В случае если в момент дополнения журнала он будет, например, открыт администратором на редактирование, Антивирус Касперского сформирует новый файл с дополнительным постфиксом к его имени. Например: *Kav4Cpf1_20050410_1.log*.

virusДАТА.log – журнал Антивируса Касперского, включающий информацию о результатах антивирусной проверки.

Новый файл журнала по умолчанию создается раз в неделю. Срок хранения файлов не ограничен, однако, ограничено количество файлов журналов одного типа, по умолчанию не более трех. При создании нового файла журнала, если установленное ограничение превышено, удаляется наиболее старый файл журнала такого же типа. Периодичность создания файлов

журналов и ограничение на их количество могут быть изменены (см. п. 10.2 на стр. 101).

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 **Logs**. Он создается на сервере в каталоге данных приложения при установке компонента Сервер безопасности. В качестве хранилища журналов может быть задан любой другой каталог по выбору администратора (см. п. 10.2 на стр. 101).

Настройка параметров журналов Антивируса Касперского осуществляется на закладке **Диагностика** окна настройки параметров приложения **Общие параметры** (см. рис. 39). Чтобы открыть окно, следует воспользоваться гиперссылкой [Общие параметры](#).

10.1. Настройка уровня диагностики

Для каждого компонента программы предусмотрен набор диагностических сообщений, выводимых в журналы. Объем и полнота информации определяется установленным для группы сообщений уровнем диагностики.

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 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. 39).

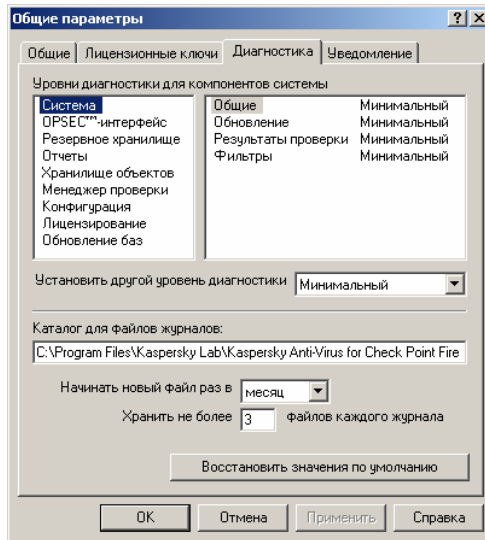


Рисунок 39. Закладка **Диагностика**

3. На закладке в разделе **Уровни диагностики для компонентов системы** представлена таблица. В левой части таблицы приведены все компоненты, входящие в состав программы. В правой части таблицы отображаются группы диагностических сообщений, предусмотренные для выбранного компонента, и уровень диагностики для каждой из них.



В журнал результатов антивирусной проверки записываются только диагностические сообщения группы **Результаты проверки** для компонента **Фильтры**.

В журнале работы приложения сообщения этой группы не регистрируются.

Выберите в левой части таблицы компонент, после этого в правой части - нужную группу диагностических сообщений. Установите необходимый уровень диагностики при помощи раскрывающегося списка.

Определите нужные уровни диагностики для каждого компонента программы. Вы можете установить уровень диагностики одновременно для всех или нескольких компонентов, выбрав их при помощи клавиш *<Shift>* и *<Ctrl+ Shift>* или мышью.

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**.

10.2. Настройка параметров файлов журналов



Для настройки параметров файлов журналов:

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. 39).
3. В поле **Каталог для файлов журналов** введите путь к новому каталогу.
4. Установите периодичность создания файлов журналов в поле **Начинать новый файл раз в**, выбрав нужное значение из раскрывающегося списка.
5. Укажите, какое количество файлов журналов одного типа 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 11. 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 почтового трафика, поступающего и запрашиваемого с того количества рабочих станций, которое указано в лицензии.

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.

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



Без лицензионного ключа из всей функциональности Антивируса Касперского доступны только сервисы управления.

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;
- приложению Check Point™ FireWall-1® передается информация о нарушении лицензионного соглашения. Если в данном приложении настроены параметры оповещения, производится соответствующее уведомление средствами Check Point™ FireWall-1®.

По окончании действия коммерческой лицензии функциональность Антивируса Касперского сохраняется за исключением возможности обновления антивирусных баз. Приложение по-прежнему осуществляет антивирусную проверку трафика, 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 окончания срока действия лицензии средствами Check Point™ FireWall-1® производится предупреждающее уведомление. В нем содержится информация о дате окончания установленного лицензионного ключа. Срок уведомления может быть изменен (см. п. 11.3 на стр. 107).

Возможность настроить уведомление о приближении окончания срока действия лицензии и об ограничении функциональности приложения также предусмотрена в параметрах Антивируса Касперского (см. Глава 12 на стр. 110).

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 Check Point™ FireWall-1®.

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. 11.4 на стр. 108).



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 ранее 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.

11.1. 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. 40).

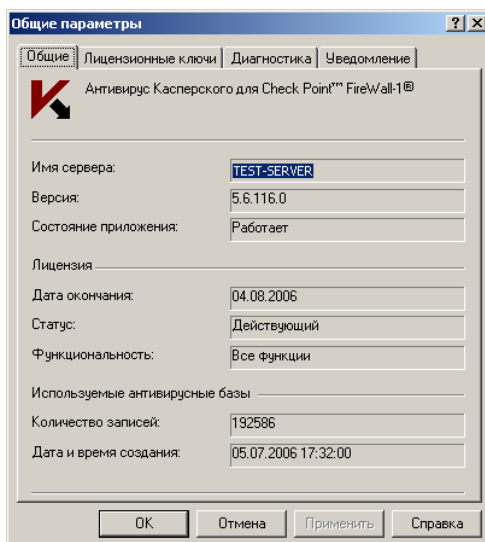


Рисунок 40. Просмотр информации о лицензии

На закладке представлена следующая информация:

- имя компьютера, на котором установлен компонент Антивируса Касперского Сервер безопасности;
- номер установленной версии приложения;
- текущее состояние компонента Сервер безопасности (**Работает, Ограничена функциональность, Возникла ошибка**);
- дата окончания лицензии;
- статус текущего лицензионного ключа;
- объем доступной функциональности приложения, соответствующий текущему лицензионному ключу:
 - **Все функции.** 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. Возможно, превышено лицензионное ограничение по количеству защищаемых рабочих станций 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.
- информация об используемых приложением антивирусных базах.

11.2. 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. 41).

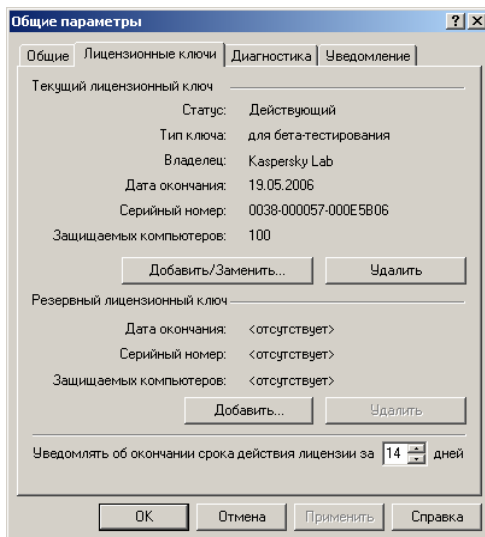


Рисунок 41. Просмотр информации о лицензионных ключах.
Настройка лицензионных уведомлений

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 рабочих станций.

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

- Дата окончания срока действия.
- Серийный номер.
- Максимальное количество защищаемых рабочих станций.

11.3. 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";

заносятся запись в журналы приложения и передается информация приложению Check Point FireWall-1®.

Если в Check Point™ FireWall-1® настроены параметры оповещения, производится соответствующее уведомление средствами Check Point™ FireWall-1®. Предусмотрена также возможность настроить уведомление о приближении окончания срока действия лицензии в параметрах Антивируса (см. Глава 12 на стр. 110).

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



Для настройки периода уведомления об окончании срока действия 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 **Лицензионные ключи** (см. рис. 41).

Укажите, за сколько дней до окончания срока действия лицензии выполнять лицензионные уведомления в поле **Уведомлять об окончании срока действия лицензии за**.

3. Нажмите на кнопку **Применить** или **ОК**.

11.4. Установка лицензионного ключа

Для приложения 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. 41).
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**.

11.5. Удаление лицензионного ключа



При удалении текущего лицензионного ключа автоматически удаляется установленный резервный 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. 41).
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**.

ГЛАВА 12. УВЕДОМЛЕНИЕ

Уведомления о событиях, регистрируемых в работе приложения Антивирус Касперского, может быть организовано с помощью встроенного механизма оповещения Check Point™ FireWall-1®. Для этого должны быть настроены:

- Параметры взаимодействия Сервера безопасности и Check Point™ FireWall-1® по протоколу ELA (см. п. 5.5 на стр. 41). Эти параметры представлены в окне **Параметры OPSEC™** на закладке **Дополнительно** (см. рис. 12).
- Оповещение о событиях Антивируса Касперского на Check Point™ FireWall-1®.

Средствами Check Point™ FireWall-1® может выполняться уведомление о следующих событиях Антивируса Касперского:

- **Обновление антивирусных баз** (успешное или завершившееся с ошибкой).
- **Приближение окончания срока действия лицензии** (при достижении периода уведомления об окончании срока действия лицензии (см. п. 11.3 на стр. 107)).
- **Изменение состояния приложения** (запуск и остановка Сервера безопасности, ограничение функциональности приложения в связи с окончанием срока действия лицензии, восстановление функциональности после продления лицензии).

Помимо этого Антивирус Касперского предоставляет возможность при регистрации в работе приложения некоторых типов событий автоматически запускать на Сервере безопасности заданные администратором программы.

Вы можете закрепить запуск внешней программы или файла сценария за следующими типами событий:

- **Антивирусная проверка объекта:** при обнаружении зараженного, подозрительного, защищенного или поврежденного объекта (об обнаружении незараженных объектов уведомление не производится).
- **Обновление антивирусных баз:** после обновления антивирусных баз, независимо от его результата (успешное или завершившееся с ошибкой).
- **Создание отчета:** после создания отчета по шаблону (как успешного, так и завершившегося с ошибкой).

- **Приближение окончания срока действия лицензии:** при достижении периода уведомления об окончании срока действия лицензии. По умолчанию этот период составляет 14 дней до окончания срока действия лицензии и может быть изменен (см. п. 11.3 на стр. 107). Посмотреть установленное значение параметра вы можете в окне **Общие параметры** на закладке **Лицензионные ключи** (см. рис. 41).
- **Изменение состояния приложения:** при следующих изменениях состояния приложения: запуск и остановка Сервера безопасности, ограничение функциональности приложения в связи с окончанием срока действия лицензии, восстановление функциональности после продления лицензии.



Для настройки уведомлений через Антивирус Касперского:

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 **Уведомление** (см. рис. 42).

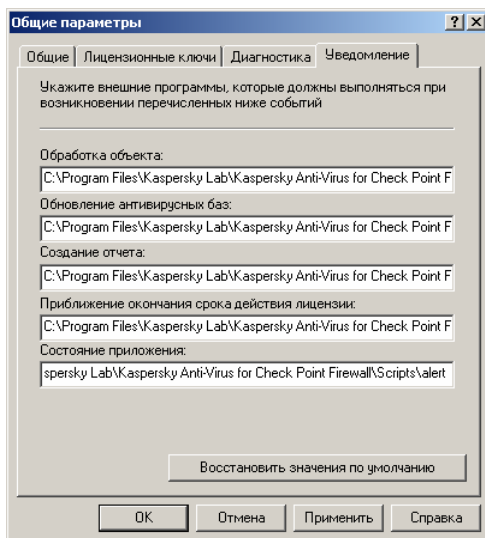


Рисунок 42. Настройка уведомления через Антивирус Касперского

3. В представленных на закладке полях в поле, соответствующем нужному событию, укажите полный путь к модулю, который будет запущен на Сервере безопасности при возникновении

этого события. Если это необходимо, введите также требуемые параметры командной строки.



Если путь к файлу содержит символы пробелов, весь путь должен быть заключен в кавычки. Параметры командной строки следует указывать после закрывающих кавычек.

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

В качестве примера программы для запуска может быть использован входящий в состав дистрибутива приложения файл сценария **alert.js**. После установки Сервера безопасности файл **alert.js** сохраняется в каталоге установки компонента в служебном каталоге **Scripts**. Вы можете использовать данный файл в его исходном виде (выполнив предварительно настройку параметров рассылки), можете вносить в него изменения либо написать и использовать собственные файлы сценария или другие исполняемые модули для уведомления о событиях.

В результате выполнения файла **alert.js** на заданный администратором адрес по электронной почте отправляется сообщение, содержащее следующую информацию о событии:

- в теле сообщения представлено описание события;
- к заголовку письма добавлено описание типа события;
- для события **Создание отчета** сообщение будет содержать вложенный файл отчета в случае его успешного создания.

Адрес отправителя и получателя, адрес и номер порта SMTP-сервера, а также тема письма задаются в переменных файла сценария. Данные параметры должны быть настроены для корректного выполнения файла **alert.js** перед его использованием.



Для того чтобы присвоить необходимые значения переменным файла сценария **alert.js**:

1. Откройте файл **alert.js** для редактирования.
2. Укажите значения следующих переменных, расположенных в начале файла:

- `g_smtpServer = "<адрес SMTP-сервера>";`

В качестве адреса можно использовать IP-адрес или другой сетевой адрес компьютера.

- `g_smtpPort = 25;`

Номер коммуникационного порта SMTP-сервера. По умолчанию используется 25 порт.

- `g_mailFrom = "<электрон-
ный_адрес_отправителя_уведомления>";`
- `g_mailTo = "<электрон-
ный_адрес_получателя_уведомления>";`

Допускается ввод нескольких адресов, разделенных запятой.

- `g_mailSubject = "<тема_письма>";`

Тема письма задается в произвольной форме.

3. Сохраните изменения в файле.

Информацию о событии вызываемой программе Антивирус Касперского передает с помощью переменных среды Microsoft Windows. Для каждого типа событий набор передаваемых переменных свой, их полный список содержит Приложение А на стр. 118.

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 Pro, SP4, Антивирус Касперского 5.5 для Check Point™ FireWall-1®, 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 Check Point™ FireWall-1® 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 бессильным 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. ПАРАМЕТРЫ УВЕДОМЛЕНИЙ

В данном разделе описываются параметры, которые передаются приложению, вызываемому для уведомления о событиях Антивируса Касперского (см. Глава 12 на стр. 110).

Параметры передаются с помощью переменных среды Microsoft Windows. Ниже приводится список событий, на которые может вызываться приложение и соответствующий каждому событию список передаваемых переменных.

Описание события	Передаваемые параметры
Антивирусная проверка объекта	
Завершена антивирусная проверка объекта.	kav4cpfl_event = «object» kav4cpfl_scan = «cured» «infected» «suspicious» «other» «cured» - вылеченный «infected» - зараженный «suspicious» - подозрительный «other» - защищенный/поврежденный kav4cpfl_id = <внутренний_идентификатор_объекта> (число) kav4cpfl_time = <дата_и_время_завершения_проверки> kav4cpfl_object = <URL_объекта> или <идентификатор_письма> kav4cpfl_size = <размер_объекта_в_байтах> kav4cpfl_protocol = «HTTP» «FTP» «SMTP» kav4cpfl_source = <IP-адрес_сервера-источника_объекта> kav4cpfl_destination = <IP-адрес_сервера-получателя_объекта> kav4cpfl_subject = <тема_письма> (только для SMTP) kav4cpfl_from = <отправитель_письма> (только

Описание события	Передаваемые параметры
	для SMTP) kav4cpfl_to = <получатель_письма> (только для SMTP) kav4cpfl_virus = <имя_вируса> или <пусто> kav4cpfl_error = <описание_ошибки> или <пусто>
Переполнение очереди уведомлений об антивирусной проверке объектов.	kav4cpfl_event = «overflow» kav4cpfl_number = <количество_пропущенных_уведомлений> kav4cpfl_time = <время_возникновения_события>
Обновление антивирусных баз	
Обновление антивирусных баз успешно завершено.	kav4cpfl_event = «update» kav4cpfl_bases = <дата_и_время_создания_используемых_приложением_антивирусных_баз> kav4cpfl_error = <пусто> kav4cpfl_time = <время_возникновения_события>
Обновление антивирусных баз завершено с ошибкой. Выполнен откат антивирусных баз до предыдущей версии.	kav4cpfl_event = «update» kav4cpfl_bases = <дата_и_время_создания_используемых_приложением_антивирусных_баз> kav4cpfl_error = <описание_ошибки> kav4cpfl_time = <время_возникновения_события>
Обновление антивирусных баз завершено с ошибкой. Рабочей версии антивирусных баз нет.	kav4cpfl_event = «update» kav4cpfl_bases = <пусто> kav4cpfl_error = <описание_ошибки> kav4cpfl_time = <время_возникновения_события>

Описание события	Передаваемые параметры
Создание отчета	
Отчет создан успешно.	kav4cpf1_event = «report» kav4cpf1_title = <имя_отчета> (заданное в параметрах отчета) kav4cpf1_path = <путь_к_файлу_отчета> kav4cpf1_error = <пусто> kav4cpf1_time = <время_возникновения_события>
Ошибка создания отчета. Отчет не создан.	kav4cpf1_event = «report» kav4cpf1_title = <имя_отчета> (заданное в параметрах отчета) kav4cpf1_path = <пусто> kav4cpf1_error = <описание_ошибки> kav4cpf1_time = <время_возникновения_события>
Приближение окончания срока действия лицензии	
Достигнут установленный в параметрах Антивируса Касперского период уведомления об окончании срока действия лицензии.	kav4cpf1_event = «license» kav4cpf1_time = <время_возникновения_события> kav4cpf1_days = = <количество_дней,_оставшихся_до_окончания_срока_действия_лицензии>
Изменение состояния приложения	
Антивирус Касперского работает в полном объеме, предусмотрено лицензионным	kav4cpf1_event = «status» kav4cpf1_error = <пусто> kav4cpf1_time = <время_возникновения_события>

Описание события	Передаваемые параметры
<p>соглашением.</p> <p>Событие возникает при запуске Сервера безопасности, если функциональность приложения не ограничена, а также при восстановлении функциональности приложения в результате продления лицензии.</p>	
<p>Из всей функциональности приложения доступно только управление.</p> <p>Событие возникает при нарушении лицензионного соглашения, окончании срока действия пробного лицензионного ключа (trial) либо нарушении целостности антивирусных баз.</p>	<pre>kav4cpf1_event = «status» kav4cpf1_error = «disabled» kav4cpf1_time = <время_возникновения_события></pre>
<p>Компонент Сервер безопасности не</p>	<pre>kav4cpf1_event = «status» kav4cpf1_error = «failed» kav4cpf1_time = <время_возникновения_события></pre>

Описание события	Передаваемые параметры
запущен или не инициализирован.	мя_возникновения_события>
Компонент Сервер безопасности остановлен (например, в связи с выключением компьютера).	kav4cpf1_event = «status» kav4cpf1_error = «shutdown» kav4cpf1_time = <вре- мя_возникновения_события>

ПРИЛОЖЕНИЕ В. ГЛОССАРИЙ

В документации встречаются термины и понятия, специфичные для области антивирусной защиты. Глоссарий представляет собой словарь определенных 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 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

Каталог данных приложения – каталог размещения необходимых для работы приложения служебных каталогов и баз данных. В случае смены каталога данных, вся входящая в его состав информация должна быть сохранена по новому адресу.

Консоль управления – компонент Антивируса Касперского. Представляет 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).

Контролируемый объект - любой файл, перемещаемый по протоколам HTTP, FTP и SMTP через межсетевой экран.

Л

Лечение объектов – способ обработки *зараженных объектов*, в результате которого происходит полное или частичное восстановле-

ние данных либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей *анти-вирусных 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.

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.

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.

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 объектов.

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.

К

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, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

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

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

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

Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты Лаборатории Касперского обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наша антивирусная база обновляется каждый час. 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 Microsoft 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, ARJ, LHA и ICE.

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

Обновления антивирусных баз осуществляется каждый час, 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 Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP, а также с бизнес-приложениями из состава Microsoft Office. Антивирус Касперского® Personal Pro включает программу загрузки ежедневных обновлений антивирусных баз 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** автоматически осуществляет проверку и лечение всей входящей и исходящей почтовой корреспонденции для любой почтовой программы, работающей по протоколам POP3 и SMTP, и эффективно обнаруживает вирусы в почтовых базах;
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов приложений Microsoft Office;
- **антивирусную проверку** более 900 версий форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP, CAB, RAR, ARJ, LHA и ICE.

Kaspersky® Anti-Hacker

Программа Kaspersky® Anti-Hacker представляет собой персональный сетевой экран, обеспечивающий полномасштабную защиту компьютера, работающего под управлением операционной системы Microsoft 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 сетевой экран под конкретного пользователя и конкретный компьютер.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite – программный комплекс, предназначенный для организации всесторонней защиты персонального компьютера под управлением операционной системы Microsoft Windows. Комплекс предотвращает проникновение вредоносных и потенциально-опасных программ через всевозможные источники, обеспечивает защиту от попыток несанкционированного доступа к данным компьютера, а также защищает от получения спама.

Kaspersky® Personal Security Suite обладает следующими функциональными возможностями:

- антивирусная защита данных, хранящихся на компьютере;
- защита пользователей почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express от нежелательных сообщений электронной почты (спама);

- защита компьютера от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети или интернета.

Новостной Агент Лаборатории Касперского

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

Новостной Агент также позволяет:

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

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

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в веб-браузере, используя технологию Microsoft ActiveX®. Таким образом, пользователи могут максимально оперативно получать ответ на опасения, связанные с заражением вредоносными программами. В рамках проверки пользователь может:

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

Kaspersky® OnLine Scanner Pro

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

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

Антивирус Касперского® 6.0

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

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

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

Возможности проактивной защиты включают в себя:

- **Контроль изменений в файловой системе.** Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.
- **Наблюдение за процессами в оперативной памяти.** Антивирус Касперского 6.0 своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а

также в случае несанкционированного изменения нормальных процессов.

- **Мониторинг изменений в реестре операционной системы** благодаря контролю состояния системного реестра.
- **Блокирование опасных макросов** Visual Basic for Applications в документах Microsoft Office.
- **Восстановление системы** после вредоносного воздействия программ-шпионов: за счет фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 6.0

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

Функции антивирусной защиты включают в себя:

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

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения

опасных сценариев на веб-страницах, всплывающих окон и рекламных баннеров). Функция **блокирования платных телефонных звонков** помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и заблокировать их работу.

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

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

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

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на карманных персональных компьютерах (КПК) различных типов, а также смартфонах. В состав программы входит оптимальный набор средств антивирусной защиты:

- **антивирусный сканер**, обеспечивающий проверку информации (хранимой как в памяти PDA и смартфонов, 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 защиту¹:

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

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:

¹ В зависимости от типа поставки

- *рабочих станций* под управлением Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstations и Linux.
- *файловых серверов* под управлением Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux и Samba Servers.
- *почтовых систем* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *интернет-шлюзов*: CheckPoint FireWall –1; Microsoft ISA Server 2004 Enterprise Edition.
- *карманных компьютеров*, работающих под управлением Microsoft Windows CE и Palm OS, а также смартфонов, работающих под управлением Microsoft Windows Mobile 2003 for Smartphone и Microsoft Smartphone 2002.

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 списки DNS Black List 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 баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway для Linux/Unix представляет собой решение, предназначенное для антивирусной обработки почтовых сообщений, проходящих по SMTP-протоколу. Приложение содержит ряд дополнительных инструментов фильтрации почтового трафика – по именам и MIME-типам вложенных файлов, а также ряд средств, позволяющих снизить нагрузку на почтовую систему и предотвратить хакерские атаки. В их числе – ограничение размера письма, количества адресатов и т.п. Поддержка технологии DNS Black List обеспечивает защиту от приема писем с серверов, занесенных в данные списки как источники распространения нежелательной почтовой корреспонденции (спама).

Kaspersky Security® для Microsoft Exchange 2003

Kaspersky Security® для Microsoft Exchange обеспечивает антивирусную проверку входящих, исходящих и хранящихся на сервере почтовых сообщений, в том числе сообщений в общих папках, а также осуществляет фильтрацию нежелательной корреспонденции, используя интеллектуальные технологии распознавания спама в сочетании с технологиями компании Microsoft. Приложение проверяет все сообщения, поступающие на Exchange-сервер по SMTP-протоколу, на наличие вирусов, используя антивирусные технологии, применяемые Лабораторией Касперского, и признаков спама, используя фильтрацию по формальным признакам (почтовому адресу, IP-адресу, размеру письма, заголовку), а также анализируя содержимое письма и его вложений с помощью интеллектуальных технологий, включая уникальные графические сигнатуры для распознавания спама в виде изображений. Проверке подвергается как тело сообщения, так и прикрепленные файлы.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway – универсальное решение для комплексной защиты пользователей почтовой системы. Установленное между корпоративной сетью и сетью Интернет, приложение осуществляет проверку всех элементов электронного письма на присутствие вирусов и других вредоносных программ (Spyware, Adware, и т.д.), а также производит централизованную фильтрацию потока почтовых сообщений на предмет спама. Решение также содержит ряд дополнительных возможностей по фильтрации почтового трафика.

С.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО "Лаборатория Касперского".

Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-8700
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