# Kaspersky 2009

## полный контроль безопасности виртуального пространства


Продукты версии 2009 объединили в себе преимущества нового антивирусного ядра «Лаборатории Касперского», обеспечивающего радикальное увеличение скорости сканирования объектов, и передовой технологии контроля за активностью приложений HIPS, которая позволяет блокировать новые разновидности вредоносных программ до изучения их аналитиками и внесения в антивирусные базы. Концепцию продуктов версии 2009 отражает слоган:

**«Лучше предотвратить заражение, чем потом устранять его последствия».**

О том, какие технологии легли в основу этой концепции, читайте ниже.

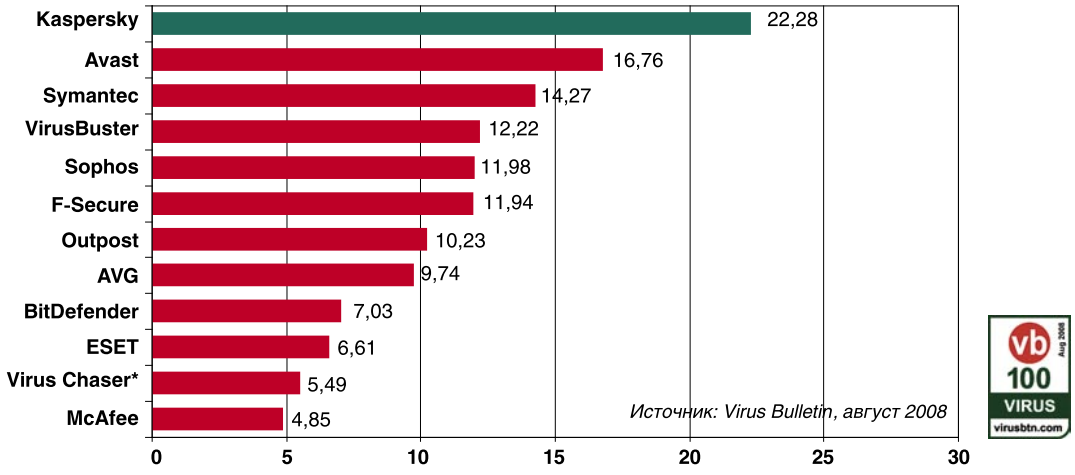
KASPERSKY lab

## Скорость работы и производительность

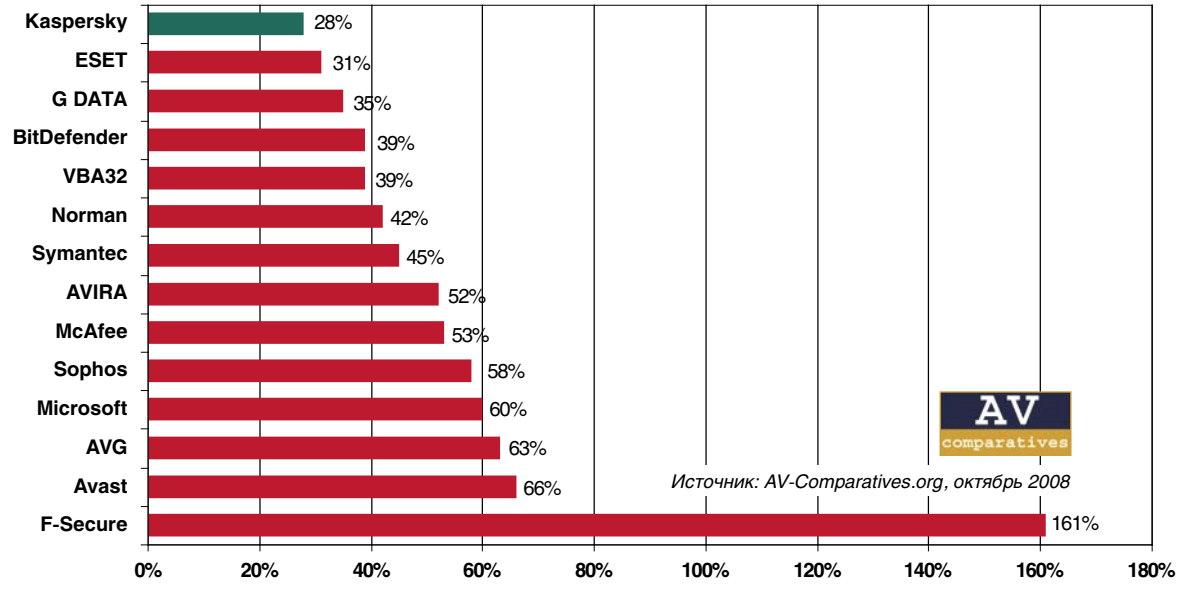
Общая логика работы компонентов защиты продуктов версии 2009, а также единая точка перехвата и проверки трафика обеспечивают бесконфликтную работу всех модулей. При этом повышаются производительность и компактность продукта: уменьшается размер дистрибутива программы и объем используемой оперативной памяти, экономится место на жестком диске.

В новом антивирусном ядре, использованном в продуктах версии 2009, существенно оптимизированы алгоритмы поиска, формат антивирусных баз, работа с упакованными объектами. Все это позволило увеличить производительность различных модулей продуктов в 3-7 раз, что незамедлительно отразилось на результатах независимых тестов: так, в ходе теста Virus Bulletin продукты версии 2009 продемонстрировали высокую скорость проверки программ и системных файлов.

**Скорость проверки программ и системных файлов (Мб/сек)**




**Замедление при копировании файлов**



Оптимизация формата антивирусных баз и механизмов лечения также позволила значительно сократить объем используемой оперативной памяти.



**Поддержка многоядерных процессоров** позволяет использовать такие преимущества современных многоядерных процессоров, как повышенная производительность однопоточных и многопоточных приложений и энергосбережение. Сертификаты, свидетельствующие о поддержке Intel® Core™ 2 Quad и Intel® Core™ 2 Duo, подтверждают эффективность технологий, реализованных в продуктах версии 2009.

**Интеллектуальные технологии iChecker и iSwift** ускоряют работу антивирусного приложения как при работе в режиме постоянной защиты, так и в режиме проверки по требованию. Данные технологии позволяют исключить из проверки некоторые ранее проверенные объекты в соответствии с определенным алгоритмом, поэтому максимальная эффективность iChecker и iSwift достигается спустя некоторое время после установки продуктов версии 2009.

**Возможность уступать ресурсы другим приложениям** позволяет автоматически приостанавливать проверку компьютера по требованию или по расписанию, если ресурсы компьютера заняты другими приложениями.


**В рамках поддержки пользователей ноутбуков** предусмотрена возможность автоматически не запускать проверку по расписанию при работе ноутбука от аккумулятора, что позволяет экономить заряд батареи. Продукты версии 2009 получили сертификат, свидетельствующий о поддержке ими технологии Intel® Centrino® Duo для мобильных ПК.

## Самозащита

Продукты версии 2009 защищены от изменения или удаления их файлов на диске, процессов в памяти, записей в системном реестре, а также от любых попыток удаленного управления сервисами продуктов. Эта функция необходима, поскольку приложения, обеспечивающие безопасность компьютера от вредоносных программ, зачастую сами становятся объектами атак со стороны вредоносного программного обеспечения, пытающегося заблокировать работу таких приложений или даже удалить их с компьютера.

## Kaspersky Security Network и Urgent Detection System

Каждый день в мире появляются новые информационные угрозы. Для ускорения сбора данных о типах новых угроз и их источниках, а так же для более оперативной разработки способа их нейтрализации в продуктах версии 2009 реализована система Kaspersky Security Network (KSN). KSN автоматически направляет в «Лабораторию Касперского» сведения о заражениях и других проблемах, возникающих на компьютерах пользователей, а также подробную информацию о загружаемых из интернета и запускаемых программах.

Подписка на участие в Kaspersky Security Network является добровольной. Сбор, обработка и хранение персональных данных пользователей в ходе работы KSN не производится. Функцию сбора информации можно в любой момент выключить и снова включить в разделе «Обратная связь» окна настройки соответствующего продукта «Лаборатории Касперского».

Система KSN позволяет «Лаборатории Касперского» более оперативно реагировать на возникающие угрозы, тем самым повышая качество работы своих продуктов.

- Вся собранная через KSN информация о загружаемых и запускаемых на компьютерах пользователей программах заносится в базу «Лаборатории Касперского» для дальнейшего анализа.
- Все программы проходят тщательную проверку, при которой учитываются данные о разработчике программы, наличие у нее цифровой подписи, степень ее распространенности и т.д. Успешно прошедшие проверку программы вносятся в онлайн-базу «белых» приложений (whitelisting).
- Подозрительные объекты подвергаются всестороннему анализу. В случае признания их вредоносными, информация о таких программах – еще до создания полноценной сигнатуры и выпуска обновления баз сигнатур – добавляется в онлайн-базу быстрого реагирования (Urgent Detection System, UDS).
- Когда пользователь запускает программу, продукт версии 2009 проверяет ее по онлайн-базам «белых» приложений и быстрого реагирования (UDS). В случае если объект присутствует в базе UDS, его запуск немедленно блокируется (до выпуска для него сигнатуры и обновления стандартных антивирусных баз). Если же программа присутствует в базе «белых» приложений, то модуль Фильтрации активности не накладывает на ее действия в системе никаких ограничений.
- Проверка программы происходит в течение нескольких секунд, объем передаваемой информации минимален.

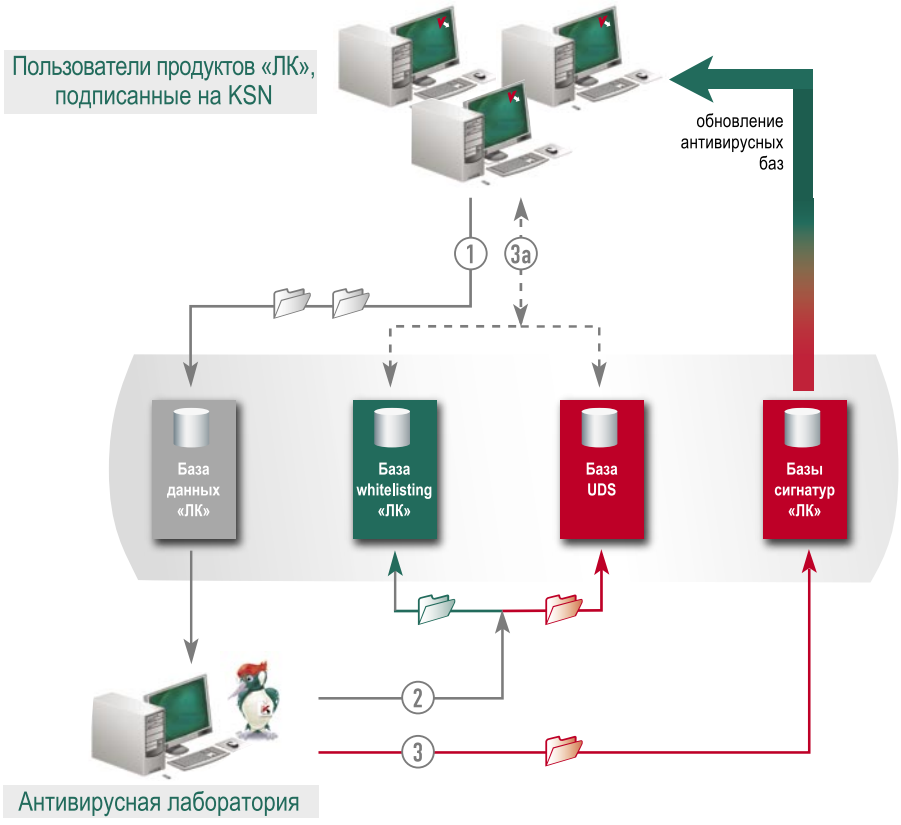
**Работа системы Kaspersky Security Network (KSN)**

① **этап:** Информация о новых запускаемых и скачиваемых приложениях собирается с компьютеров всех пользователей Kaspersky Internet Security 2009 и Антивируса Касперского 2009, подписанных на Kaspersky Security Network.

② **этап:** Специалисты проверяют подозрительные файлы и добавляют их в базу данных быстрого реагирования (Urgent Detection System, UDS). Легитимные файлы добавляются в базу «белых» приложений (whitelisting).

③ **этап:** Специалисты завершают анализ подозрительных файлов, определяют степень их опасности и добавляют запись в базу данных сигнатур.

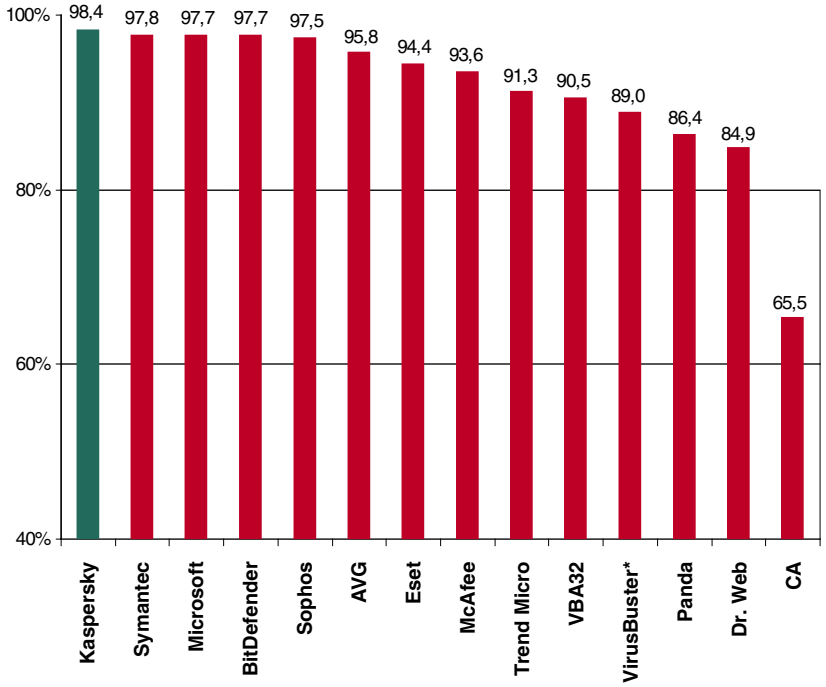
③а **этап (происходит одновременно с 3 этапом):** Другие пользователи (не только подписчики KSN) загружают и запускают те же программы. Продукты «Лаборатории Касперского» проверяют их по базе UDS и базе «белых» приложений.



## Антивирус

**Новое антивирусное ядро**, использованное в продуктах версии 2009, существенно расширяет возможности обнаружения и лечения вредоносных и шпионских программ. По итогам теста исследовательской лаборатории *AV-Test.org* продукты новой версии получили высший статус A (++) в категориях «обнаружение вредоносных программ» и «обнаружение программ-шпионов».

**Уровень обнаружения вредоносных программ (%)**




*Источник: AV-Test.org, сентябрь 2008*

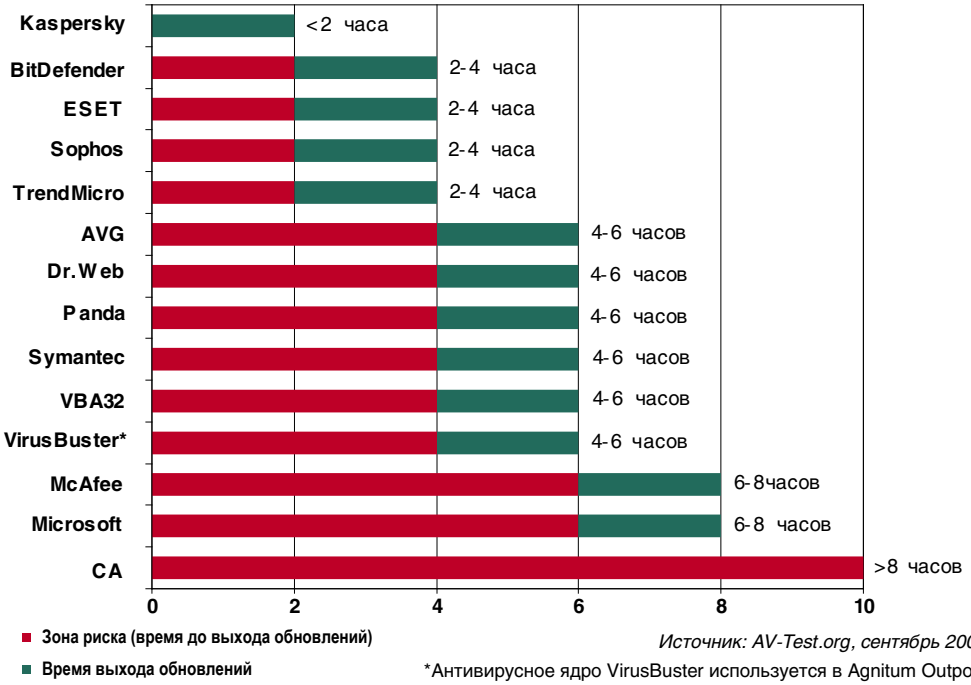
*Антивирусное ядро VirusBuster используется в Agnitum Outpost

AV-TEST

Высокую эффективность решений версии 2009 также подтверждают сертификаты, полученные после многоуровневых испытаний в исследовательском центре West Coast Labs и в тестовой лаборатории ICSA.

**Высочайшая скорость реакции на новые угрозы** позволяет минимизировать риск заражения новыми вредоносными программами. По результатам тестов лаборатории *AV-Test.org* скорость реакции «Лаборатории Касперского» на новые угрозы составляет в среднем 0-2 часа, и это лучший показатель в индустрии. Такой высокий результат, в частности, достигается за счет использования технологии Kaspersky Security Network, которая собирает информацию о заражении компьютеров пользователей и передает ее на серверы «Лаборатории Касперского» для дальнейшего анализа.

## Среднее время реакции на новые угрозы (часы)

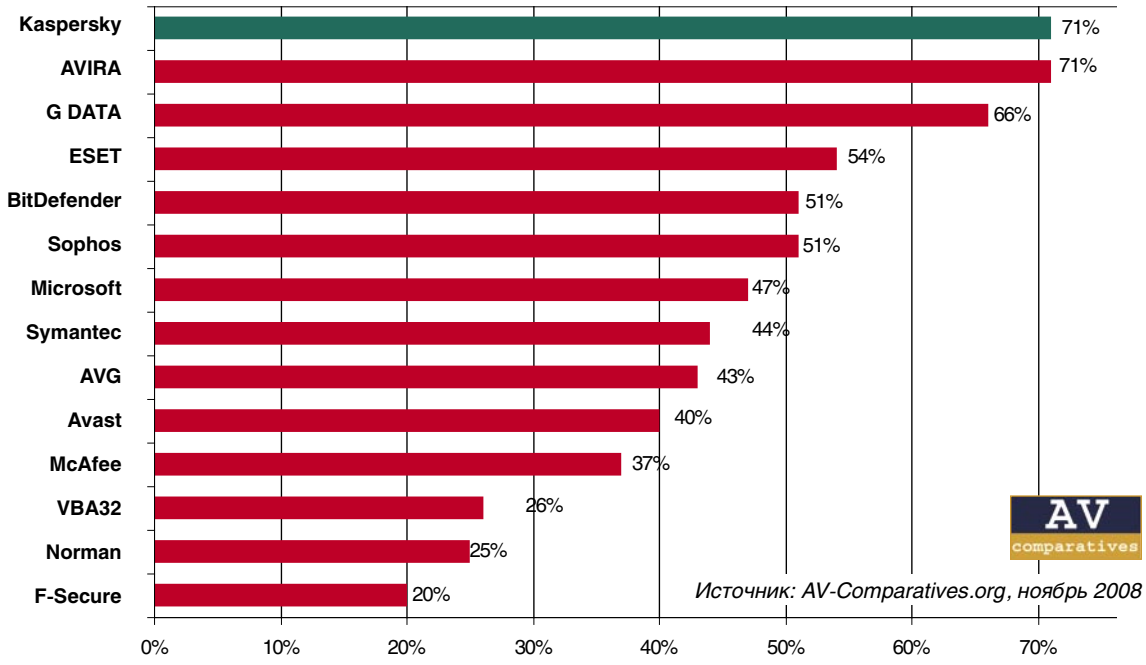



*Источник: AV-Test.org, сентябрь 2008*

*Антивирусное ядро VirusBuster используется в Agnitum Outpost

AV-TEST

## Эвристическое обнаружение неизвестных вредоносных программ (недельная коллекция вирусов)




AV comparatives

*Источник: AV-Comparatives.org, ноябрь 2008*

KASPERSKY lab

**Эвристический анализ** позволяет определить, является ли программа вредоносной, даже в том случае, если она еще не известна вирусным аналитикам. Это достигается за счет анализа кода программы путем эмуляции ее запуска в защищенной среде. По результатам тестов *AV-Comparatives.org*, эвристические технологии, использованные в продуктах версии 2009, заслужили статус Advanced (продвинутый).

**Файловый Антивирус** перехватывает обращение пользователя или некоторой программы к каждому файлу при его открытии, сохранении и запуске, и проверяет этот файл. Файловый антивирус обладает уникальными возможностями обнаружения и устранения вредоносного ПО в упакованных файлах и архивах: продукты версии 2009 поддерживают более 2000 форматов архиваторов и упаковщиков. Кроме того, в продуктах версии 2009 появилась возможность обнаруживать объекты, упакованные с помощью средств, обычно используемых вирусописателями. Это позволяет обнаружить вредоносную программу даже в том случае, когда ее сигнатуры нет в базе, поскольку сам факт использования подозрительного упаковщика свидетельствует о вредоносности анализируемого объекта.

**Почтовый Антивирус** обеспечивает проверку «на лету» почтовых сообщений, поступающих по различным почтовым протоколам (POP3/SMTP/NNTP/IMAP) и по протоколам ICQ/MSN еще до их получения пользователем, что снижает риск заражения. Эта функция также позволяет проверять трафик вне зависимости от используемого почтового или ICQ/MSN клиента.

**Веб-Антивирус** осуществляет проверку «на лету» объектов в интернет-трафике еще до того, как они попадают на компьютер пользователя. Эта технология позволяет обнаруживать вирусы, способные запуститься без создания файла на локальном диске пользователя (такие вирусы не могут быть обнаружены обычным файловым антивирусом). Веб-Антивирус проверяет интернет-трафик вне зависимости от используемого браузера.

**Технология лечения активного заражения** позволяет эффективно лечить уже зараженный компьютер. Современные вредоносные программы могут внедряться на самые низкие уровни операционной системы, что делает процесс их удаления чрезвычайно сложным. Продукты версии 2009 способны проводить специальную расширенную процедуру лечения, которая позволяет даже в самых сложных случаях успешно обезвредить и удалить с компьютера вредоносное ПО.

## Контроль приложений (программ)

Новый уникальный модуль Фильтрации активности, входящий в состав KIS 2009, позволяет при первом запуске приложения в системе проанализировать уровень его опасности, определить индекс опасности и, в случае необходимости, наложить ограничения на его доступ к конфиденциальным данным, файлам и папкам пользователя, ресурсам операционной системы (реестру, системным папкам и файлам), USB- и Bluetooth-устройствам, а также установить привилегии приложения в системе (права на управление процессами других приложений, внедрение в процессы других приложений и т.д.). Степень ограничений зависит от присвоенного приложению индекса опасности.

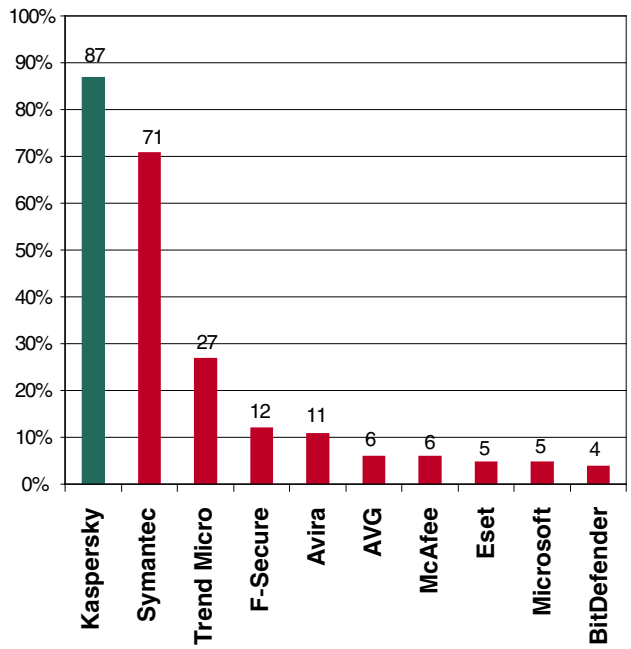
В итоге, даже если потенциально опасное приложение не определено антивирусом как однозначно вредоносное, оно, как правило, получает высокий индекс опасности и в результате наложенных на него ограничений не может выполнить вредоносные действия, а значит, заражение компьютера не происходит. В ходе теста, проведенного лабораторией *AV-Comparatives.org*, модулем Фильтрации активности был проактивно заблокирован запуск 68% вредоносных программ, что существенно превышает результаты, полученные при тестировании модулей проактивного обнаружения в продуктах большинства конкурентов.

**Модуль Проактивной защиты,** реализованный в продуктах версии 2009, в отличие от **модуля Фильтрации активности** контролирует не отдельные действия программ, а распознает новые, еще не известные вирусным аналитикам угрозы по последовательности выполняемых ими действий. Если в результате анализа активности программы последовательность ее действий вызывает подозрение, то активность данной программы блокируется. Например, такие действия, как самокопирование некоторой программы на сетевые ресурсы, в каталог автозапуска и системный реестр с последующей рассылкой копий, позволяют с большой долей вероятности утверждать, что эта программа – червь.

**База «белых» программ**, используемая продуктами версии 2009, позволяет легко определять доверенные программы и в дальнейшем не ограничивать их права на работу в системе, что значительно повышает скорость работы, снижает частоту обращений продуктов к пользователю и уровень ложных срабатываний.

**Сетевой экран (файервол)**, входящий в состав KIS 2009, защищает от проникновения в систему и от утечки информации, гибко регулирует сетевую активность запущенных программ, контролирует входящий и исходящий трафик через любые порты. В тестах на оценку сетевых экранов, проведенных ресурсом *matousec.com*, сетевой экран «Лаборатории Касперского» получил оценку «очень хорошо», показав лучшие результаты среди сетевых экранов, входящих в состав интегрированных решений класса Internet Security.

**Рейтинг сетевых экранов**




*Источник: Matousec.com, 2008*

**Мастер анализа безопасности** осуществляет поиск уязвимостей в установленных на компьютере программах, а также повреждений и аномалий в настройках параметров операционной системы и браузера, причиной которых могут служить активность вредоносных программ, системные сбои и т.д.

## Онлайн-защита

**Анти-Фишинг** позволяет эффективно противодействовать такому виду мошенничества, как фишинг, при котором злоумышленники различными способами предлагают пользователю перейти на сайт, как две капли воды похожий на официальный сайт банка или онлайн-магазина, и ввести там в веб-форму свои конфиденциальные данные: номер счета или кредитной карты, логин и пароль. Компонент Анти-Фишинг продуктов версии 2009 блокирует переход на такие подложные (фишинговые) сайты, а также отфильтровывает письма со ссылками на них. Кроме того, специальная Виртуальная клавиатура, входящая в состав KIS 2009, позволяет избежать перехвата конфиденциальных данных при их вводе.

**Защита от сетевых атак** позволяет противостоять сетевым атакам, использующим уязвимости как операционной системы, так и иного установленного на компьютере ПО системного и прикладного характера. Данный функционал реализован только в KIS 2009.

**Анти-Дозвон** контролирует попытки создания скрытых модемных соединений. Данный функционал реализован только в KIS 2009. Скрытым считается соединение, не инициированное пользователем и оставляющее его в неведении о факте звонка. Как правило, скрытые соединения устанавливаются с платными телефонными номерами.

## Фильтр содержимого

(данный функционал реализован только в KIS 2009)


**Анти-Спам** включает в себя обучаемый на письмах конкретного пользователя модуль, а также обновляемые с серверов «Лаборатории Касперского» базы фраз, типичных для спама в целом. Технология GSG позволяет анализировать изображения, вложенные в сообщения, с целью обнаружения признаков, характерных для спама. В продукте использованы технологии, реализованные в антиспам-решениях «Лаборатории Касперского» для серверов, получившие сертификаты ICSA Labs Certified и Checkmark Anti-Spam Premium.

**Анти-Баннер** блокирует рекламную информацию, размещенную на баннерах в интернете или на баннерах, встроенных в интерфейс различных программ, установленных на компьютере пользователя.

**Родительский контроль** позволяет ограничить доступ детей к сайтам, предназначенным для взрослой аудитории: затрагивающим темы порнографии, оружия, наркотиков, провоцирующим жестокость, насилие и т.д. Предусмотрено также ограничение пользования интернетом по времени.

**Мастер Устранения следов активности** удаляет с компьютера пользователя информацию о его действиях, которая может заинтересовать злоумышленников (список посещаемых веб-сайтов, открываемых файлов, cookies и т.д.).

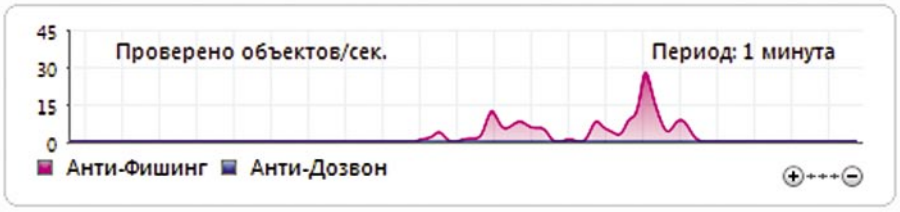
## Пользовательский интерфейс

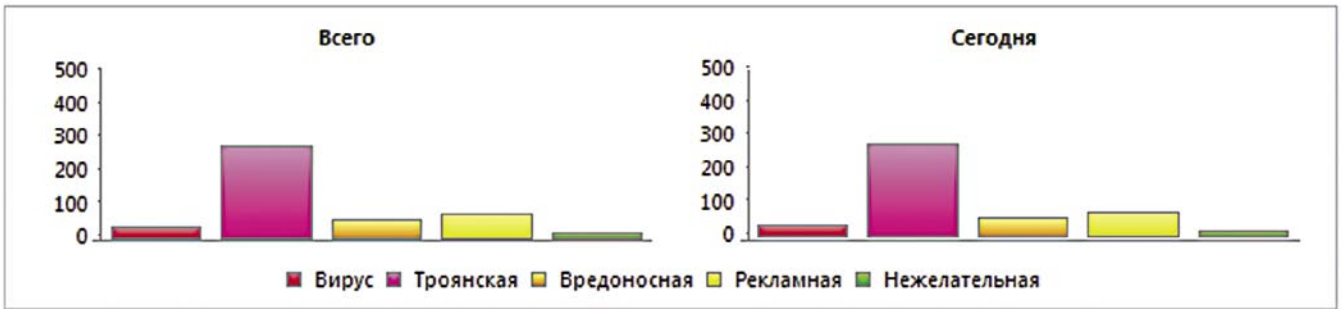
**Пользовательский интерфейс** продуктов версии 2009 полностью обновлен, благодаря чему работа с продуктами стала значительно проще как для начинающих пользователей, так и для профессионалов.

**При автоматическом режиме** работы, установленном по умолчанию, продукты версии 2009 самостоятельно принимают все решения о необходимых действиях и не беспокоят пользователя лишними запросами. При переходе в интерактивный режим приложение уведомляет пользователя обо всех опасных и подозрительных событиях в системе, после чего пользователь определяет, разрешить или запретить то или иное действие.

**При работе с полноэкранными приложениями** (игры, показ презентаций и т.д.) продукты версии 2009 не мешают пользователю уведомлениями о событиях в системе.

Информация о состоянии защиты и о необходимых действиях представлена в наглядной и доступной форме.




**Возможность использования альтернативной графической оболочки** позволяет изменять цвета, шрифты, пиктограммы и тексты в интерфейсе продуктов версии 2009. При желании пользователь также может создать собственные графические оболочки для продуктов и локализовать их на другой язык.

## Техническая поддержка и сервисы

**Бесплатная круглосуточная служба технической поддержки**, доступная как по телефону, так и через систему обработки клиентских запросов HelpDesk.

**Ежечасные обновления** баз данных различных угроз и возможность **бесплатно получать новые версии** установленных продуктов в период действия подписки.

**Постоянно обновляемая база** знаний на сайте компании *http://support.kaspersky.ru/*.

**Бесплатные лечащие утилиты** для наиболее распространенных и опасных вирусов, доступные всем желающим.