Новые свойства продукта Антивирус Касперского 6.0

Антивирус Касперского 6.0- простая в использовании, быстрая, надежная, легкая, система защиты от вирусов, шпионских программ и неизвестных угроз.

Продукт Антивирус Касперского 6.0 обладает следующими новыми свойствами:

	Функциональность	Описание
	Модуль проактивной защиты	
	Анализ активности приложений	Модуль проактивной защиты осуществляет контроль: 1. Опасная активность процессов 2. Запуск браузера с параметрами 3. Внедрение в процесс 4. Появление скрытого процесса (rootkit) в системе 5. Внедрения оконного перехватчика 6. Подозрительные значения в реестре 7. Подозрительная активность в системе
	Контроль Опасной активности	Анализирует поведение всех процессов, запущенных в системе, сохраняя все изменения, производимые в файловой системе и реестре. При выполнении некоторым приложением набора подозрительных действий выдаётся предупреждение пользователю об опасности данного процесса.
	Откат изменений после определения опасной активности в системе	Технология, позволяющая восстанавливать систему после вредоносных действий, возвращая ее к незараженному состоянию.
	Контроль запуска браузера с параметрами	Позволяет перехватить скрытый запуск браузера с передачей ему параметров, что может быть использовано вредоносными программами.
	Контроль внедрения кода в чужые процессы	Позволяет перехватить все возможности внедрения программного кода в чужие процессы.
	Технология борьбы с руткитами (контроль появления скрытого процесса)	Позволяет обнаруживать большинство из реализаций современных руткитов, которые могут скрывать от пользователя файлы, папки и ключи реестра, скрывать запущенные программы, системные службы, драйверы и сетевые соединения, скрывать сетевую активность.
	Контроль внедрения оконного перехватчика	Перехватывает попытку внедрения динамической библиотеки во все активные процессы в системе.
	Подозрительные значения в реестре	Позволяет перехватить попытку создания «скрытых» ключей в реестре, не отображаемых обычными программами (типа regedit).
	Подозрительная активность в системе	Отслеживает большое число различных изменений в системе, указывающих на присутствие активного вредоносного кода.
	Контроль целостности приложений (монитор приложений)	Позволяет задавать ряд приложений, для которых будет контролироваться компонентный состав.

	Контроль системного реестра (монитор реестра)	Контролирует изменения ключей реестра. Содержит предустановленный список из 6 групп критических ключей. Также пользователь может добавить свои группы ключей и настроить правила доступа к ним для различных приложений.
	Проверка VBA- макросов	Проверка опасных макросов Visual Basic for Application.
	Расширенная технология задания исключений для приложений	Позволяет настраивать доверительные отношения не только к файлам, которые не будут проверяться при выполнении условий, но и что наиболее важно- для приложений. Также, при определении пользователем доверенного приложения, можно указать следующие действия программы по отношению к нему: • Не проверять файлы, открываемые этим приложением • Не контролировать активность этого приложения • Не контролировать обращения к реестру • Не проверять сетевой трафик
Новые свойства модуля Антивирус. Антивирус состоит из четырех модулей, контролирующих все каналы проникновения вирусов на компьютер: **Файловый антивирус, Почтовый антивирус, Веб- антивирус, сканирование по-требованию**		
	Проверка только новых и изменённых файлов (настраиваемая по типам объектов)	Проверка только новых и измененных файлов обеспечивает оптимизацию и ускорение антивирусной проверки без снижения её качества за счет использования новых технологий.
	Технологии ускорения антивирусной проверки iSwift и iChecker	Использование данных технологий обеспечивает ускорение антивирусной проверки за счёт интеллектуального кеширования данных от предыдущих антивирусных проверок.
	Гибкие возможности антивирусной проверки для составных объектов	Позволяет оптимизировать производительность системы при проверке сложных составных объектов.
	Технология приостановки сканирования при увеличении пользовательской активности	Механизм отслеживания пользовательской активности, позволяющий принудительно приостановить задачу сканирования, до тех пор пока загрузка системы не снизится. Таким образом балансируется загрузка системы и сканирование не забирает себе все ресурсы.
	Технология восстановления системы (долечивание после вредоносного воздействия, в частности Spyware-модулей)	При нахождении вредоносного объекта и его удаления, позволяет уничтожать все записи о нем в системных файлах и реестре.
	Проверка IMAP, NNTP, SMTP, POP3 трафика	Осуществляет антивирусную проверку почтового трафика по наиболее распространенным почтовым протоколам.
	Плагины в почтовых клиентах Microsoft Outlook и TheBat!	Антивирусные плагины в Outlook и The Bat дают возможность осуществлять антивирусную проверку писем до прихода их в почтовую базу на локальном диске.

	Фильтр почтовых вложений	Позволяет переименовывать или удалять вложения определённых типов в письмах.
	Проверка HTTP трафика	Антивирусная проверка данных в режиме «на лету», передаваемых по протоколу HTTP, позволяет предотвратить заражение компьютера пользователя ещё до момента сохранения файлов на локальном диске.
	Гибкая настройка Веб-Антивируса	Позволяет задать типы сканирования: потоковое сканирование и буферизированное (с задаваемым временем буферизации). Также пользоватлеь может задать доверенные адреса.
	Технология уменьшения размеров обновлений	Позволяет существенно уменьшить размер скачиваемых обновлений баз, за счет применения технологии инкрементальных обновлений.
	Увеличенная и обновляемая база объектов, загружаемых при старте системы	Позволяет отслеживать и оперативно обновлять максимальное число мест в ОС, в которых может находиться вредоносный код для автоматического запуска в момент старта системы.
	Задача “Сканирование критических областей системы”	Позволяет проверить большинство важных системных областей, которые больше всего подвержены заражению. Позволяет значительно экономить время пользователя и сначала проверить критические области.
	Задача “Сканирование объектов автозапуска”	Позволяет проверить объеткы автозапуска для предотвращения запуска вредоносного кода при старте системы.
	Технология борьбы со сложными механизмами самозащиты вирусов от обнаружения антивирусом	Данная технология направлена на борьбу со сложными вредоносными программами, которые используют различные ухищрения для самозащиты от антивирусных программ. Решение осуществляет антивирусную проверку «залоченных» файлов, т. е. файлов, которые уже используется неким другим приложением и не могут быть проверены обычным способом, так как к ним невозможно получить доступ. Новая технология позволяет получить доступ к таким файлам и проверять их на присутствие вредоносного кода.
	Установка программы на уже зараженный компьютер и лечение вредоносных программ, активных в оперативной памяти	Данная технология направлена на лечение системы от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают антивирусу удалить их с помощью разных методов, в том числе метода перекрестного слежения двух процессов друг за другом.
	Увеличенная и обновляемая база объектов, загружаемых при старте системы	Новый механизм, использующийся для получения системной информации обо всех объектах, запускающийся при старте системы, направленный на борьбу со скрытыми процессами, в частности rootkits.
	Средства создания аварийного диска	Данная возможность позволяет создавать образ загрузочного диска для восстановления работоспособности системы после вирусной атаки и невозможности загрузки системы. Технология представляет собой средства создания образа загрузочного диска, используя Microsoft Windows PE или Bart PE Builder, а также установочный диск Microsoft Windows XP SP 2.
	Оптимизированный алгоритм проверки часто используемых файлов и архивов в отложенном режиме	Данный алгоритм используется для разрешения конфликтов, возникающих при проверке часто используемых файлов, осуществляет проверку архивов в отложенном режиме, а также позволяет избежать конфликтов с прикладным ПО

		(файловыми менеджерами, 1С,...)
	Новые сервисные свойства продукта	
	Компонентная архитектура приложения	Позволяет выбрать необходимые для работы модули в процессе установки продукта.
	Мастер настройки продукта после инсталляции	Позволяет произвести базовую настройку продукта непосредственно после установки.
	Активация продукта	Предназначена для присвоения пользователю личного ключа и решению проблем с лицензированием.
	Расширенная настройка информационных сообщений продукта	Позволяет задать варианты уведомления при наступлении определённых событий (вывод информационного сообщения, отсылка письма, звуковой сигнал).
	Возможность отсылки писем по событиям в продукте	Позволяет отсылать письма при наступлении событий, происходящим в программе, а также задать режим рассылки: при наступлении события и групповой по расписанию.
	Гибкая парольная защита	Позволяет управлять сервисом ограничения доступа к программе и настроить область действия парольной защиты.
	Настройки питания и производительности	Управление сервисом экономии заряда аккумулятора для мобильных пользователей.
	Технология скинования для построения пользовательского интерфейса	Позволяет полностью изменять элементы графического интерфейса.
	Возможность сохранять некритические события только для активной задачи сканирования	Позволяет решить проблему с увеличением размеров отчётов, не лишая пользователя возможности просматривать все события текущей задачи.
	Улучшенная технология самозащиты	Новая профессиональная технология максимально затрудняет вредоносным программам противодействие продукту.
	Возможность оставить антивирусные базы и лицензионный ключ при деинсталляции продукта	Данная функция позволяет оставить AV-базы и лицензионный ключ при деинсталляции продукта и при последующей инсталляции продукта подключить найденный ключ.
	4 режима окончания сканирования	Возможность после завершения сканирования перевести компьютер в один из следующих режимов: • Перезагрузка • Режим ожидания • Спящий режим • Выключить компьютер