Единство двух миров

Что такое гибридная защита, как она используется в новых пользовательских продуктах «Лаборатории Касперского»?

Сегодня, когда ежедневно появляется более 35 000 новых вредоносных программ, одним из главных вопросов, стоящих перед разработчиками антивирусных решений, является внедрение новых методов обнаружения неизвестных угроз и максимально быстрого обновления антивирусных баз. В подобной ситуации наиболее эффективным решением является сочетание традиционных антивирусных методов и новейших «облачных» технологий. В новой версии продукта Kaspersky Internet Security 2012 реализован инновационный подход гибридной защиты, который объединяет силу антивирусных технологий и скорость облачной защиты, обеспечивая оптимальный уровень безопасности компьютера, эффективно защищая его от современных интернет-угроз.

«ЛК» уходит в облака

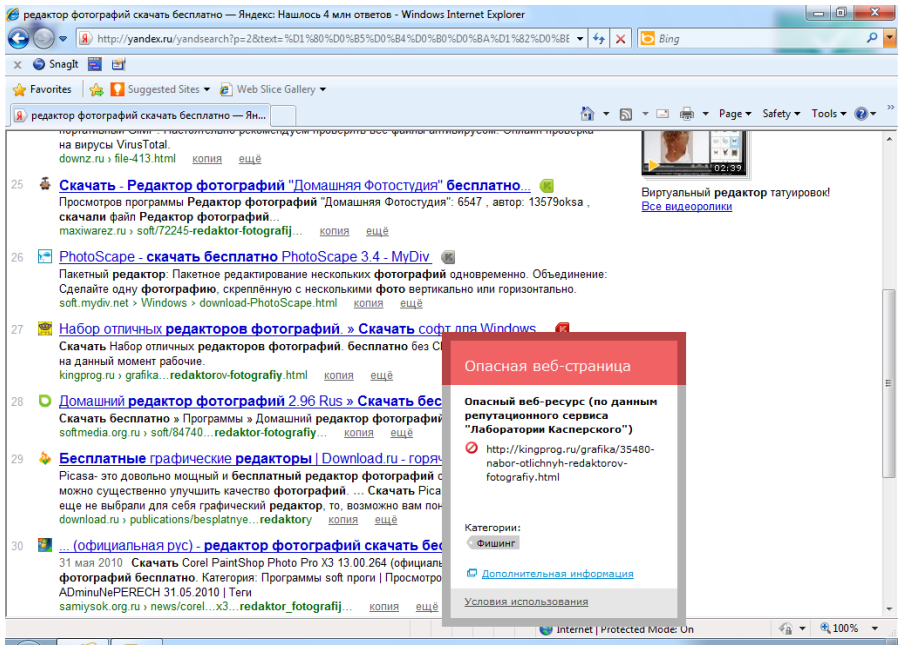
В современных условиях, когда количество новых вредоносных программ стремительно растет, применение исключительно традиционных методов защиты компьютера становится малоэффективным. Ресурсы компьютера не безграничны, пользователи не должны отводить гигабайты жесткого диска для хранения антивирусных баз, а всю оперативную память — для анализа активности на компьютере и определения потенциально опасного поведения. Таки образом, одним из самых удачных подходов к вопросу обеспечения безопасности стала облачная защита. В продуктах «Лаборатории Касперского» она реализована с помощью Kaspersky Security Network (KSN), специальной сети, объединяющей пользователей домашних продуктов. KSN собирает и доставляет на централизованные серверы «Лаборатории Касперского» информацию обо всех попытках заражения и подозрительного поведения на миллионах пользовательских машин, защищенных продуктами компании. К этим данным добавляется информация из многих других источников, и таким образом осуществляется постоянный мониторинг вирусной ситуации во Всемирной Паутине. Стоит новой вредоносной программе попытаться заразить хотя бы один компьютер, как информация о ней и ее действиях мгновенно поступает к экспертам «Лаборатории Касперского» через Kaspersky Security Network. Программа получает соответствующий статус, после чего данные о ней рассылаются всем пользователям, и последующие попытки заражения исключаются. В результате такого оперативного взаимодействия элементов антивирусной системы пользователь всегда располагает самой актуальной защитой от новых угроз, поступившей из облака, независимо от графика обновления антивирусных баз.

Использование облачных технологий позволило реализовать в Kaspersky Internet Security 2012 следующие функции:

- **Веб-фильтр**

Веб-фильтр, входящий в состав Kaspersky Internet Security 2012, предназначен для ограничения соединений пользовательского компьютера с вредоносными и мошенническими интернет-ресурсами. Веб-фильтр проверяет ссылки на веб-страницах и выставляет рядом с ними индикаторы-иконки разного цвета в соответствии с категорией опасности. Сайты делятся на опасные, безопасные и недостаточно известные системе. Интернет-ресурсы проверяются в первую очередь в локальной базе фишинговых и вредоносных веб-сайтов. Если там они не обнаружены, поиск ведется в онлайновых «черных списках» системы глобального мониторинга и быстрого реагирования на угрозы KSN. Если ресурс неизвестен и там, применяется эвристический анализ на наличие признаков, характерных для фишинговых ссылок.

Веб-фильтр только ограничивает, но не запрещает переходы на опасные сайты. В режиме блокирования опасных ссылок пользователь может вернуться на предыдущую страницу или все же выполнить соединение.



Ссылки на опасные ресурсы помечаются красным индикатором, на сайты с неопределенной степенью опасности — серым, на безопасные — зеленым; нажав на значок можно получить дополнительную информацию

Благодаря Kaspersky Security Network 2012-е версии Kaspersky Internet Security предоставляют больше информации о ресурсах, на которые ведут помеченные ссылки. При наведении курсора мыши на иконку-индикатор выводится окно с сообщением о том, в какой базе найден ресурс и к какой категории он относится. На основе полученной информации пользователь может принять обоснованное решение о том, стоит ли посещать сайт.

В качестве приятного дополнения можно отметить тот факт, что в новых версиях персональных продуктов расширен список браузеров, поддерживаемых Веб-фильтром. Теперь это не только актуальные версии Microsoft Internet Explorer и Mozilla Firefox, но и Google Chrome.

- **Анти-Спам**

В предыдущих версиях Kaspersky Internet Security требовалось обучить антиспамовый модуль на некотором количестве писем перед началом его работы. В версии 2012 такое обучение не требуется, поскольку информация для работы модуля берется из облака, где уже имеется актуальная база образцов спам-сообщений. Из баз Kaspersky Security Network на пользовательские компьютеры поступают шаблоны новых рассылок спама и новые адреса вредоносных, спамерских и фишинговых ресурсов. Это позволяет быстро приспосабливаться к изменениям тактики спамеров и налаживать адекватную защиту.

- **Контроль программ**

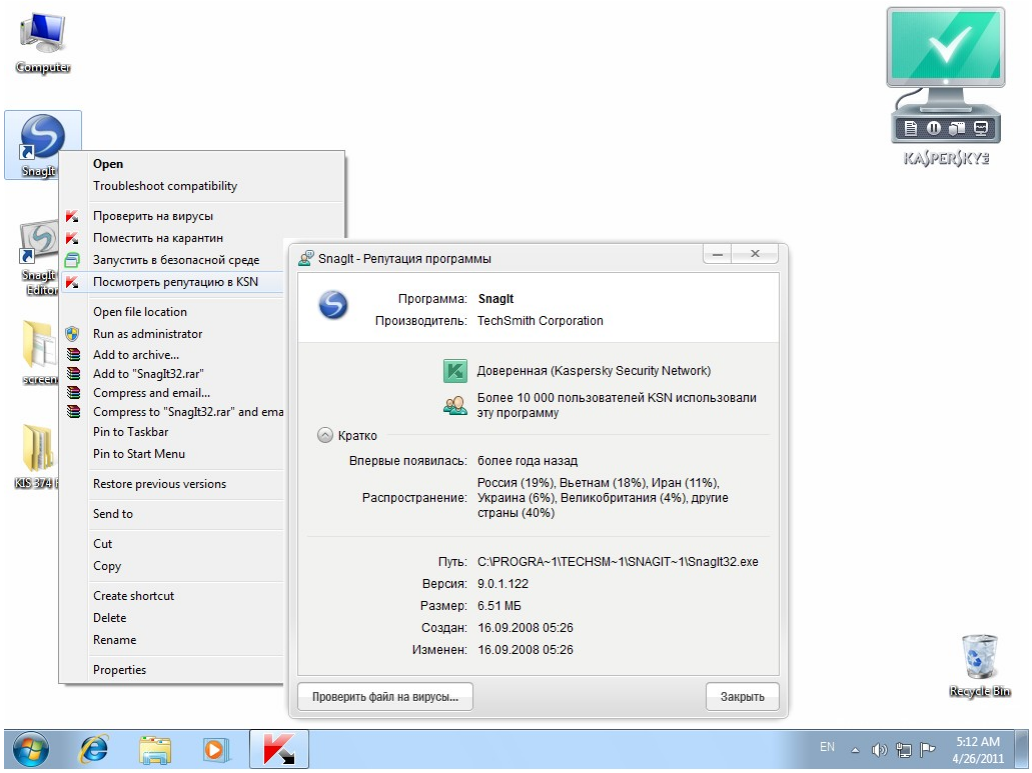
Система Kaspersky Security Network участвует в определении рейтингов опасности программ. Такие рейтинги используются при назначении прав доступа различного ПО к ресурсам компьютера и персональным данным пользователя. В Kaspersky Internet Security 2012 информация о новом ПО поступает сразу из нескольких источников: системы KSN и различных компонентов обновленных продуктов, таких как Контроль программ, Мониторинг активности программ и эвристический анализатор. Активный обмен данными обеспечивает максимальную полноту и актуальность анализируемой информации.

- **Анти-Фишинг**

Пользователям Kaspersky Internet Security 2012 предоставлена улучшенная защита от фишинговых ссылок, заманивающих на поддельные банковские сайты. В новом персональном продукте в облаке содержатся все новые адреса вредоносных и фишинговых ресурсов, базы характерных фраз и слов, используемых злоумышленниками при попытке кражи ценных данных. Эту информацию использует продукт на пользовательском компьютере, обращаясь к облаку в реальном времени. В совокупности с проактивными технологиями анализа сайтов применение облака позволяет быстрее приспосабливаться к изменениям тактики и приемов злоумышленников и поддерживать высочайший уровень защиты.

- **Проверка репутации программ**

С помощью всего одного нажатия клавиши мыши пользователь Kaspersky Internet Security 2012 может узнать репутацию любого исполняемого файла на локальном компьютере и обоснованно решить, стоит ли его использовать. Для этого нужно лишь кликнуть правой кнопкой мыши по иконке файла и выбрать в контекстном меню опцию «Посмотреть репутацию в KSN». Но даже если вы этого не сделаете, все необходимые проверки будут проведены автоматически. Информация о каждой программе мгновенно попадает в облачную сеть, даже если эта программа только что появилась в Интернете.



Итак, преимущества использования облачных технологий для защиты пользователя очевидны:

- Высокая скорость реакции на угрозы — до считанных десятков секунд.
- Обладая практически неограниченными вычислительными ресурсами, облако позволяет выполнять параллельную обработку данных, то есть быстро проводить исследование сложных угроз.
- При работе с облаком загрузка пользовательского компьютера минимальна, так как обмен информации с ним, как правило, осуществляется в фоновом режиме.

Возникает вопрос: можно ли обойтись только облачными технологиями защиты, не используя в целях безопасности антивирус, установленный на пользовательской машине? Казалось бы — вот оно, идеальное решение: практически мгновенная реакция на новые угрозы без нагрузки на локальные ресурсы компьютера. Увы, это не так, и на то есть несколько причин.

Традиционные технологии защиты

Во-первых, чем больше информации поступает в облако, тем более эффективную защиту оно может предоставить, поэтому огромную роль в реагировании на новые угрозы играют источники поступления информации о новых вредоносных программах и сценариях. Большая часть этой информации собирается в KSN с компьютеров пользователей. Понятно, что для того, чтобы эта информация поступала, надо иметь средство ее сбора и анализа на стороне пользователя, то есть антивирусный продукт.

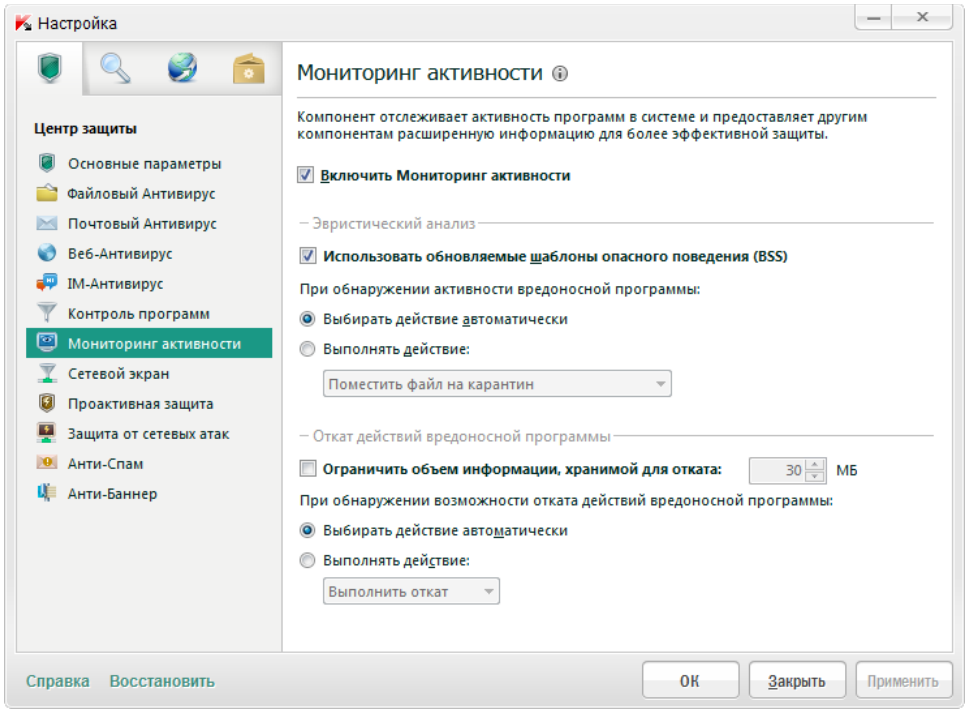
Во-вторых, облачная защита ограничена наличием интернет-соединения: если компьютер не подключен к Сети, она не может функционировать. При этом остается риск заражения компьютера пользователя вредоносным ПО по локальной сети, с переносных USB-накопителей и т. п.

Более того, если заражение все-таки произошло, вылечить зараженный компьютер через интернет часто представляется невозможным — хотя бы потому, что вредоносное ПО, получив контроль над системой жертвы, может блокировать всю входящую информацию и запросы, кроме собственных.

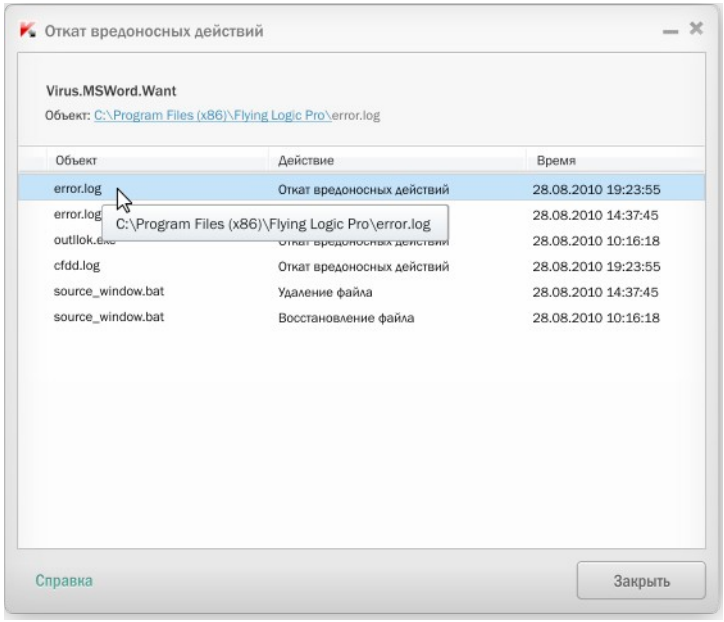
Именно поэтому в Kaspersky Internet Security 2012 применены не только облачные, но и традиционные средства защиты, установленные на компьютере пользователя.

- **Мониторинг активности программ**

Система мониторинга активности программ наблюдает за подозрительными действиями программ на компьютере и выявляет ПО с вредоносным поведением. Преимущество системы заключается в том, что она позволяет получать полную картину происходящих событий и успешно детектировать новые вредоносные объекты, для которых еще нет сигнатур.



Мониторинг активности программ Kaspersky Internet Security 2012 способен отслеживать и анализировать больше событий на компьютере по сравнению с предыдущей версией. Обновленный монитор отслеживает реальные действия каждого объекта во время не только текущего, но и предыдущих сеансов работы с компьютером. Эти действия сравниваются с шаблоном, свойственным вредоносному объекту. Если объект признан вредоносным, система может отменить совершенные им критические действия, даже если они были произведены в течение предыдущей сессии. При этом под журнал событий отведено 30 Мб, которых будет достаточно для того, чтобы сохранить историю действий за целый месяц.

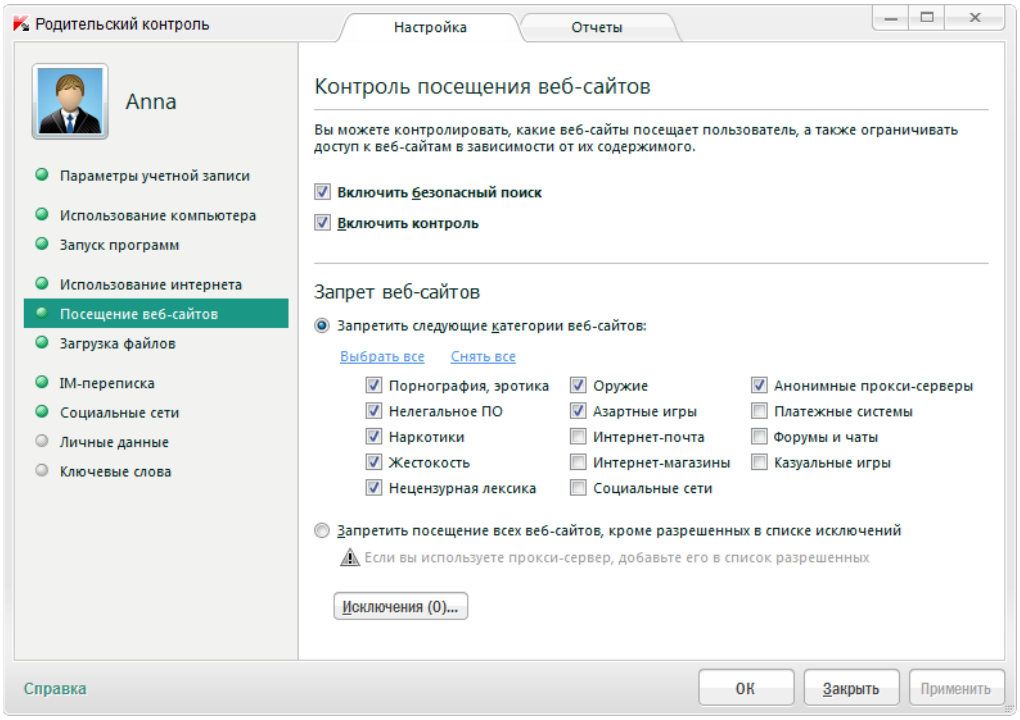


- **Откат вредоносных действий**

В новой версии продукта расширен список отменяемых действий. Теперь в него входят: создание вредоносной программой исполняемых файлов, удаление файлов и их модификация (например, переименование), изменения в системном реестре и другие. Осуществляется принудительное завершение процессов, запущенных вредоносной программой. Расширен и список превентивно блокируемых вредоносных действий. Отмена действий осуществляется автоматически или в интерактивном режиме, при этом все действия системы отката документируются. Сохраняются и резервные копии файлов, удаляемых при откате, — то есть откат можно отменить.

- **Родительский контроль**

Для защиты детей и подростков от угроз, связанных с пребыванием в Интернете, в продукте Kaspersky Internet Security 2012 реализован модуль Родительский контроль. Он позволяет контролировать время использования компьютера и Интернета ребенком и запуск им определенных программ, ограничивать загрузку файлов из Интернета, а также контролировать общение в социальных сетях и через программы мгновенного обмена сообщениями. Контроль общения ребенка в социальных сетях заключается в определении контактов, с которыми общение разрешено, блокировании переписки с нежелательными контактами, а также в возможности просмотра истории переписки. С помощью этого модуля родители могут сформировать списки разрешенных и запрещенных контактов, задать ключевые слова, наличие которых будет проверяться в сообщениях (с возможностью блокирования сообщений, содержащих эти слова), а также указать личные данные, передача которых будет запрещена. Кроме того, Родительский контроль позволяет просматривать статистические отчеты о действиях, совершенных ребенком на компьютере.



Единство двух миров

Очевидно, что современное защитное решение должно объединить в себе весь арсенал актуальных технологий, как облачных, так и традиционных. Kaspersky Internet Security 2012 полностью отвечает современным требованиям пользователей по эффективности и скорости. Так, благодаря свойствам гибридной защиты, совмещающей облачные технологии и преимущества классического антивирусного продукта, время обнаружения и ликвидации угрозы снижено до 40 секунд. В то же время оптимизация совместного использования с современными программами на компьютере позволила увеличить скорость выполнения некоторых операций на 50 % по сравнению с предыдущими версиями. Таким образом, Kaspersky Internet Security 2012 стал еще проще в использовании, эффективнее борется с угрозами и меньше «тормозит» работу компьютера.

«Новая, 2012-я версия Kaspersky Internet Security достойно продолжила эстафету наших персональных продуктов. В продукте реализованы первоклассные – и концептуально, и по качеству исполнения – технологии защиты от самых сложных угроз. В то же время продукт стал еще более простым и дружественным для пользователей. Мы сделали очередной шаг вперед по защите пользователей интернета от неизвестных, наиболее опасных угроз: многие модули Kaspersky Internet Security 2012, такие как веб-антивирус, эвристики, подсистема рейтингов опасности, анти-руткит и другие стали легко обновляемыми и более эффективно задействуют облачные технологии», – утверждает Евгений Касперский, и после прочтения данной статьи у нас есть все основания ему верить.