Обзор SafenSoft SysWatch Deluxe

29 апреля, 2011 - 16:41 — Александр Панасенко

Теги: Обзоры Домашние пользователи SafenSoft SafenSoft SysWatch Deluxe Антивирус Комплексная защита ПК

SafenSoft SysWatch Deluxe – система защиты компьютера от вредоносного ПО. Она позволяет предотвращать проникновение в систему вирусов, троянских коней, руткитов и других угроз, тем самым обеспечивая безопасную работу пользователей. SafenSoft SysWatch Deluxe значительно отличается от привычных антивирусов. Дело в том, что он является одним из немногочисленных представителей класса HIPS-решений. В основе его работы лежит не база данных сигнатур, а контроль активности приложений, то есть проактивная защита.

Введение

На сегодняшний день существует два основных подхода к детектированию вредоносных программ. В одном из них используется проверка его кода (сигнатурные и эвристические методы), а в другом – анализ и контроль активности, то есть выполняемых действий. В традиционных антивирусах в основном используется первый способ. Контроль активности, называемый проактивной защитой, тоже есть, но играет больше вспомогательную роль. В отличие от них существует отдельный класс продуктов, в которых применяется сугубо контроль поведения запускаемых приложений – Host-based Intrusion Prevention System (HIPS). Именно к этому классу средств защиты и относится программа SafenSoft SysWatch Deluxe.

Практика показывает, что HIPS-решения отличаются очень высокой степенью защиты. Не привязанные к сигнатурным базам данных, они могут с одинаковой [степенью] эффективности предотвращать проникновение в систему как старых, так и абсолютно новых вредоносных программ. Эта их особенность является серьезным преимуществом, особенно для домашних пользователей. Ведь многие из них, несмотря на все предупреждения, до сих пор обновляют используемые антивирусные продукты редко или вообще лишь время от времени. Кроме того, HIPS-решения, которым не нужно постоянно сканировать исходный код большого количества файлов, выгодно отличаются низким потреблением системных ресурсов.

Однако, при этом считается, что HIPS-решения сложны в использовании, ввиду того, что многие из них выдают достаточно большое число запросов пользователям, заставляя их самостоятельно принимать решения о правомерности деятельности того или иного программного обеспечения. Естественно, для неискушённого пользователя это может оказаться достаточно нетривиальной задачей. Кроме того, неверно принятые решения способны заметно снизить надежность защиты.

Однако этого нельзя сказать о SafenSoft SysWatch Deluxe. Данный продукт может опровергнуть сложившийся стереотип о сложности управления HIPS-решениями. С одной стороны SafenSoft SysWatch Deluxe обеспечивает высокую, свойственную продуктам данного класса, степень эффективности, а с другой – простоту использования. Это достигается благодаря использованию собственной запатентованной технологии V.I.P.O.®.

В основе работы V.I.P.O.® лежит драйвер SafenSoft, который загружается до всего остального ПО и перехватывает вызовы системных функций на уровне нулевого кольца безопасности ядра Windows. Это позволяет ему контролировать деятельность всех остальных приложений. Отличительной особенностью данной технологии является трехуровневая система защиты. На первом (он называет D.I.C. - Dynamic Integrity Control) осуществляется контроль запуска неизвестных программ, что позволяет предотвратить скрытую установку или выполнение приложений. Вторым уровнем (D.S.E. - Dynamic Sandbox Execution) является изолированная среда для запуска потенциально опасного ПО. На третьем уровне (D.R.C. - Dynamic Resource Control) осуществляется контроль файловой активности ПО, попыток изменения системного реестра, доступа к внешним устройствам и другие инструменты для предотвращения вредоносных действий.

Кроме того, в SafenSoft SysWatch Deluxe есть и традиционный антивирусный сканер, который осуществляет поиск вредоносных программ с использованием базы данных сигнатур, обновляемой ежесуточно. Помимо него, в рассматриваемом продукте есть целый ряд других инструментов: «песочница» для запуска потенциального опасных программ, система самозащиты и прочее, подробнее см. раздел Возможности SysWatch Deluxe. Наличие перечисленных функциональных возможностей делает SysWatch Deluxe весьма эффективным продуктом, который может обеспечить надёжную защиту домашнего компьютера.

Системные требования SafenSoft SysWatch Deluxe

Поскольку принцип работы SafenSoft SysWatch Deluxe основан на анализе процессов, минимальные системные требования для установки и эксплуатации данного продукта зависят от используемой операционной системы. Таблица соответствия приведена ниже.

Операционная система	Процессор	Память	Дисковое пространство
Microsoft Windows XP	Частота от 300 МГц	Не менее 256 Мб	

Microsoft Windows XP	Частота от 300 МГц	Не менее 256 Мб	Не менее 150 Мб
Microsoft Windows Vista/7	Частота от 800 МГц	Не менее 512 Мб	

Возможности SafenSoft SysWatch Deluxe

Продукт SafenSoft SysWatch Deluxe обладает следующими функциональными возможностями, предназначенными для защиты системы от вредоносного ПО.

Технология V.I.P.O.®

В основе работы SafenSoft SysWatch Deluxe лежит использование патентованной технологии V.I.P.O.®, созданной разработчиками программы. Она представляет собой трехуровневую систему проактивной защиты системы от проникновения в нее вредоносного программного обеспечения. V.I.P.O.® позволяет предотвращать выполнение таких действий, как несанкционированный запуск или блокировка процессов, получение системных привилегий, доступ к папкам, файлам, реестру, внешним устройствам и сетевым ресурсам.

Автоматическая настройка

В SafenSoft SysWatch Deluxe реализована система автоматической настройки, в ходе которой программа ищет и собирает информацию обо всех исполняемых файлах и используемых модулях DLL, идентифицирует их и автоматически создает для них правила. Это заметно облегчает применение продукта домашними пользователями, которые не являются специалистами в области информационной безопасности.

Постоянная защита от проникновения вредоносного ПО

После установки и настройки SafenSoft SysWatch Deluxe автоматически запускается при старте операционной системы и осуществляет постоянный контроль работы всех процессов, не требуя к себе внимания со стороны пользователя. Запросы будут выдаваться в относительно в редких случаях, например, при установке нового приложения.

Антивирусный сканер

В состав SysWatch Deluxe входит традиционный антивирусный сканер, основанный на сигнатурном и эвристическом поиске вредоносного ПО. Он способен обнаруживать как традиционные вирусы, так и программы-шпионы, а также руткиты. Данный модуль может быть полезен в качестве дополнительного средства защиты. Он позволяет проверять систему до или в любой момент после установки SysWatch Deluxe по запросу пользователя. Базы данных, необходимые работы антивирусного сканера, обновляются регулярно (с периодичностью 1 раз в сутки).

Контроль активности приложений

SafenSoft SysWatch Deluxe может контролировать активность приложений, операции с файловой системой, с системным реестром, сетевую активность, устройства, а также привилегии и взаимодействие процессов. При этом пользователю доступна возможность создания очень гибких правил. В частности, можно ограничить список подключаемых к компьютеру устройств (с указанием не только самих устройств, но и пользователей, временного интервала работы правила, исключений и пр.), действия, выполняемые с определенными файлами и целыми папками, операции с конкретными объектами системного реестра и пр.

«Песочница»

В SafenSoft SysWatch Deluxe есть «песочница», которая представляет собой изолированную среду исполнения. В ней осуществляется запуск потенциально опасных, уязвимых (например, браузеры) и неизвестных приложений. При этом любые их действия не могут нанести вред основной системе или как-то повлиять на работу других программ и процессов.

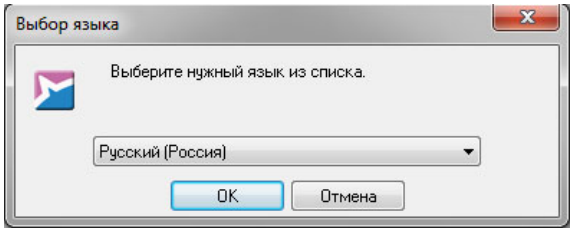
Система самозащиты

В SafenSoft SysWatch Deluxe реализована система защиты исполняемых модулей и других файлов, используемых программой, от несанкционированного изменения. Кроме того, владелец компьютера может защитить паролем настройки приложения для предотвращения неправомерного доступа к ним других пользователей.

Процесс установки SafenSoft SysWatch Deluxe

Процедура установки и первоначальной настройки осуществляется с помощью удобного пошагового мастера. Благодаря этому, она достаточно проста, и справиться с ней может любой, даже неподготовленный пользователь. В первую очередь нужно загрузить дистрибутив с официального сайта программы (со страницы http://www.safensoft.ru/download/home/deluxe/, на которой требуется регистрация) и запустить его. При этом на экране появится окно выбора языка установки. Устанавливаем в выпадающем списке вариант «Русский (Россия)» и нажимаем на кнопку «OK».

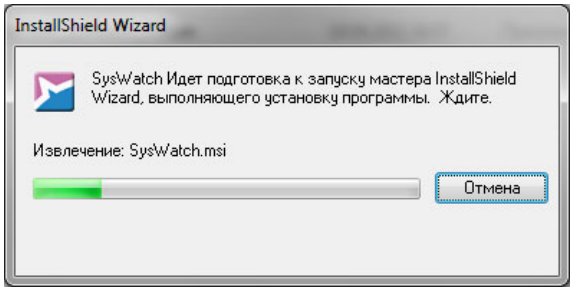
Рисунок 1. Выбор языка установки



При этом будет запущена процедура распаковки файлов дистрибутива и подготовка к запуску

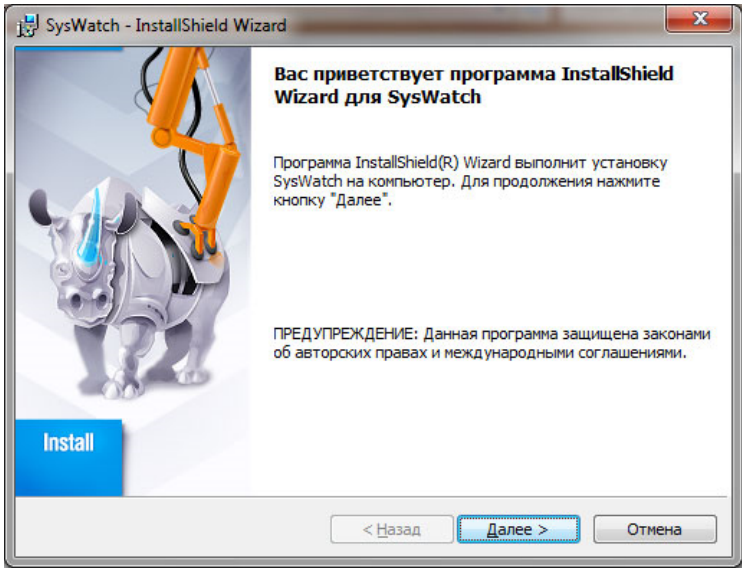
При этом будет запущена процедура распаковки файлов дистрибутива и подготовка к запуску мастера установки.

Рисунок 2. Подготовка к запуску мастера установки SysWatch Deluxe



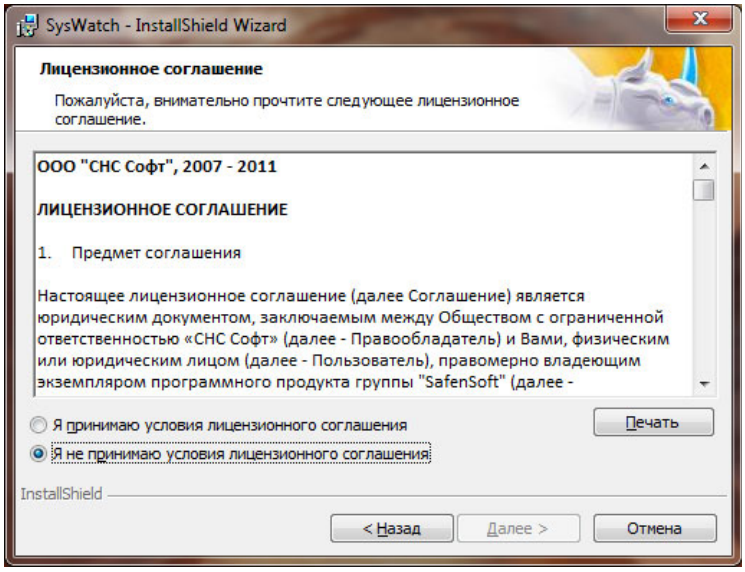
После завершения процесса на экране появится стартовое окно мастера установки. В нем просто нажимаем на «Далее».

Рисунок 3. Стартовое окно мастера установки SysWatch Deluxe



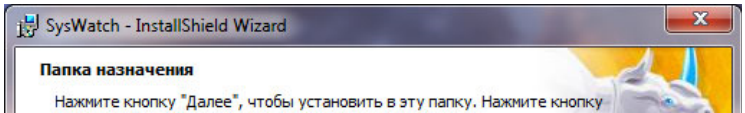
Следующий шаг опять же привычен подавляющему большинству пользователей. Это чтение лицензионного соглашения и принятие его.

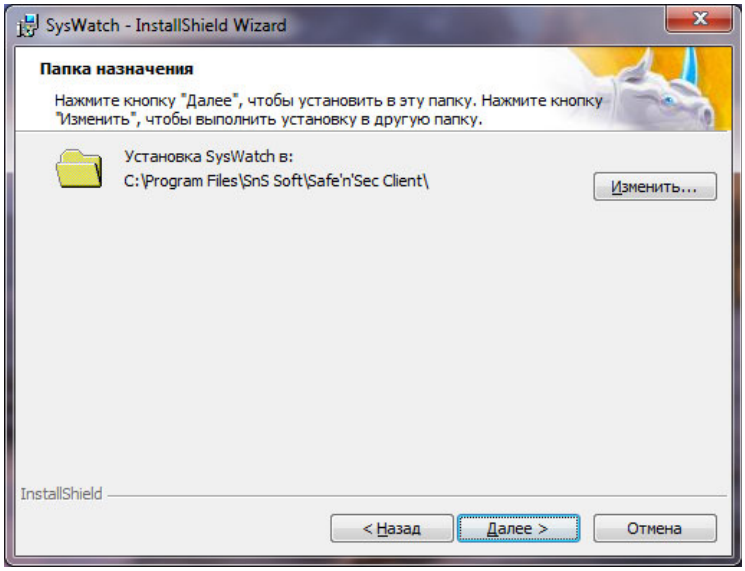
Рисунок 4. Принятие лицензионного соглашения SysWatch Deluxe



Далее выбираем папку, в которую будет установлена программа. Хотя, конечно же, обычно смысла менять директорию, установленную по умолчанию (это папка C:\Program Files\SnS Soft\Safe'n'Sec Client\), нет.

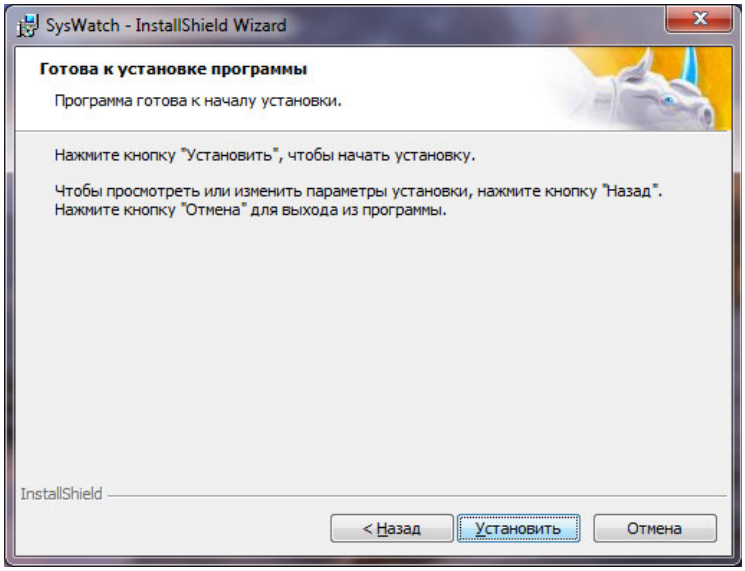
Рисунок 5. Выбор папки установки SysWatch Deluxe





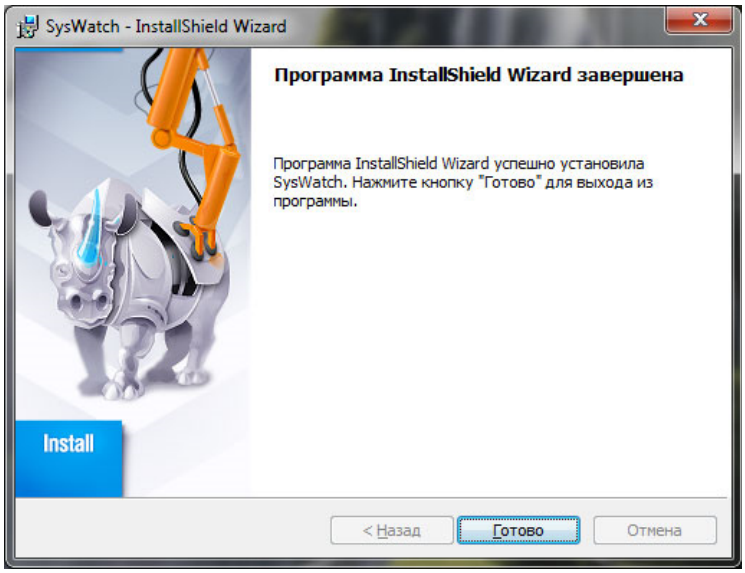
После этого настройка инсталляции считается законченной. При нажатии на кнопку «Установить» запустится сама процедура. Время ее выполнения зависит от многих факторов, включая операционную систему, доступные системные ресурсы компьютера и пр.

Рисунок 6. Запуск процедуры инсталляции SysWatch Deluxe



При завершении своей работы мастер выдаст на экран окно с сообщением об успешной установке программы.

Рисунок 7. Завершающее окно мастера установки SysWatch Deluxe

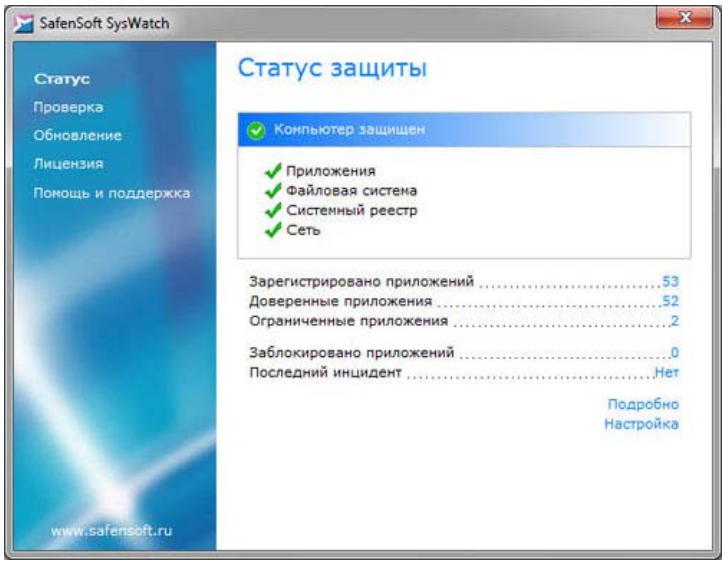


Обратите внимание, что SysWatch Deluxe приступает к защите компьютера непосредственно после установки, даже не требуя его перезагрузки. При этом будет выполнена процедура автонастройки, в ходе которой программа обнаружит все исполняемые файлы и создаст для них подходящие правила. То есть, после установки мы получаем полностью готовую к работе систему защиты.

Работа с SafenSoft SysWatch Deluxe

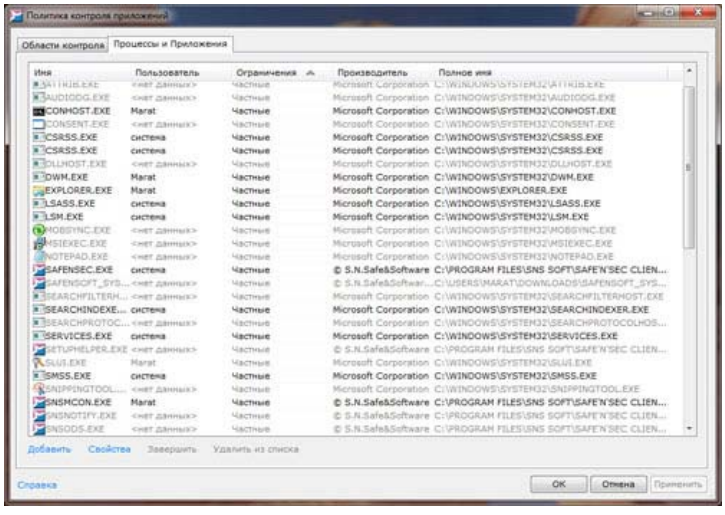
Главное окно программы SafenSoft SysWatch Deluxe состоит из нескольких вкладок. Основная из них – «Статус». На ней отображается текущее состояние системы защиты, число зарегистрированных, доверенных и ограниченных приложений, а также некоторая другая информация. Она же может использоваться для включения отключения компонентов безопасности и просмотра списка программ.

Рисунок 8. Вкладка «Статус» главного окна SysWatch Deluxe



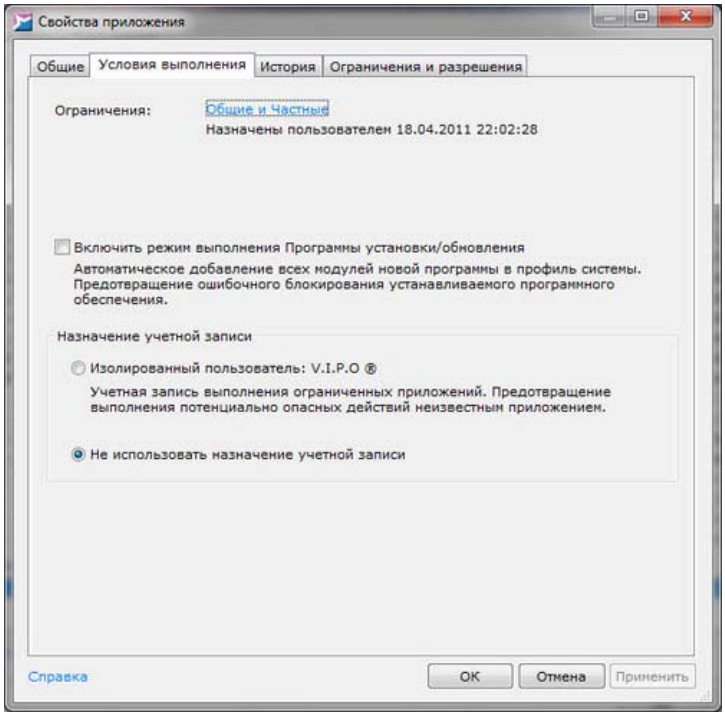
Как мы уже говорили, в процессе установки SysWatch Deluxe выполняется процедура автонастройки, в ходе которой программа создает так называемый профиль системы. В нем перечислены все обнаруженные приложения, которые подразделяются на две группы – доверенные и ограниченные. К первой относятся известные и заведомо безопасные программы, а ко второй – неизвестные системе защиты или же потенциально опасное ПО. Ограниченные приложения разрешены для использования, однако они запускаются в собственной изолированной среде («песочнице») и не могут нанести вред системе. Для просмотра списков достаточно кликнуть по соответствующей части экрана. При этом будет открыто окно настройки политики контроля приложений.

Рисунок 9. Список приложений в окне настройки политики контроля приложений



Список приложений используется не только для просмотра, но и для управления правилами тех или иных приложений. В частности, пользователь может перенести программу из группы доверенных в ограниченные или наоборот, а также вообще запретить ее выполнение. Помимо этого можно открыть свойства приложения и включить или отключить разрешение на его обновление, активировать хранение истории активности, настроить частные ограничения на доступ к тем или иным областям и пр. В общем, речь идет о возможности полной настройки.

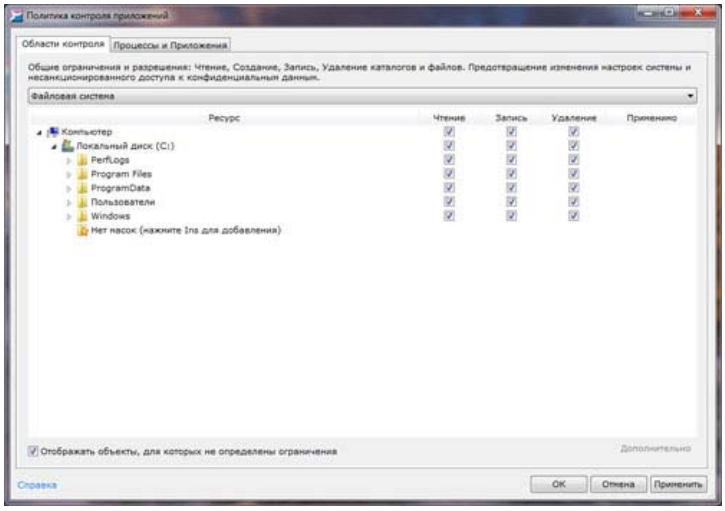
Рисунок 10. Окно свойств приложения



Помимо списка правил в окне настроек политик контроля приложений есть еще одна вкладка, которая позволяет настраивать области контроля. Речь идет об установке прав доступа ограниченных приложений. Всего существует шесть типов областей, выбор которых осуществляется с помощью выпадающего списка.

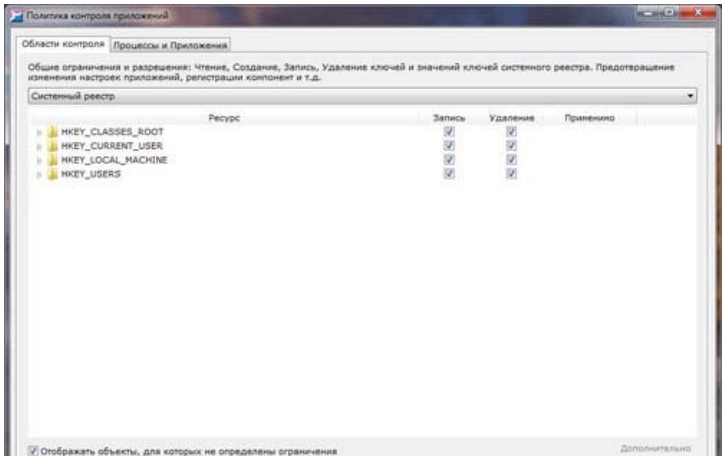
Файловая система. Позволяет включать и отключать разрешение на чтение, запись и удаление содержимого определенных папок или же отдельных файлов, задаваемых с помощью масок.

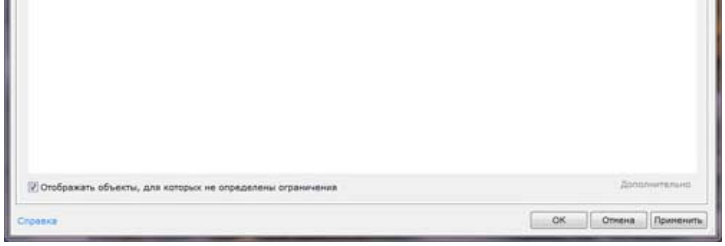
Рисунок 11. Настройка контроля файловой системы



Системный реестр. Предназначен для установки прав доступа на чтение и удаление ключей системного реестра.

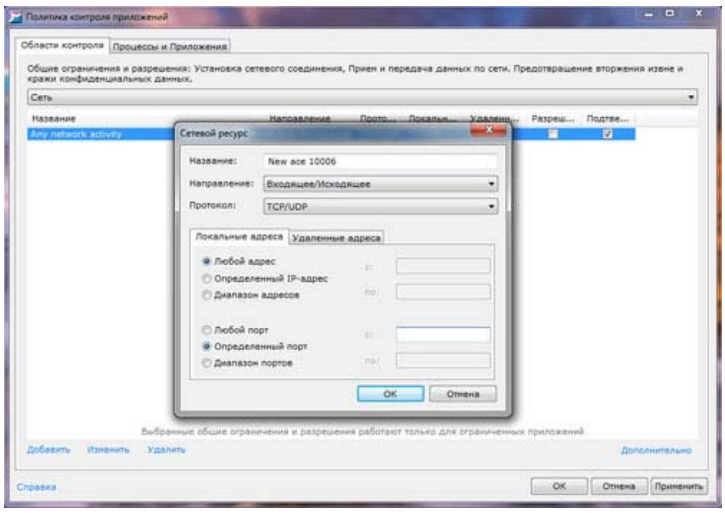
Рисунок 12. Настройка контроля системного реестра





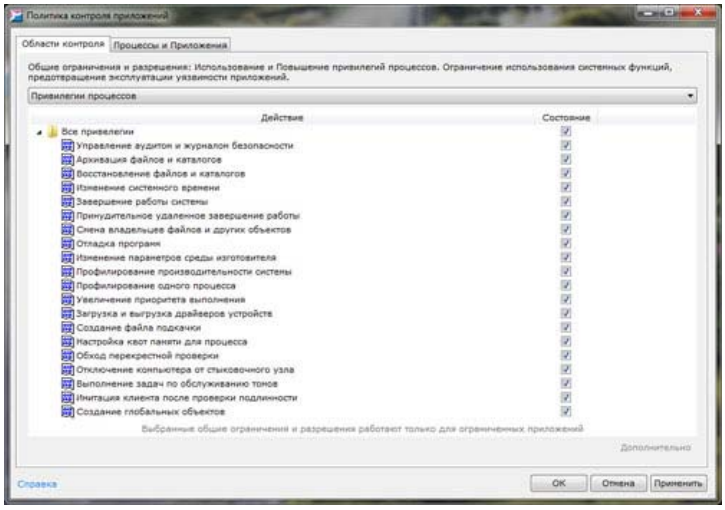
Сеть. Используется для разрешения или запрета таких действий, как установка сетевого соединения по определенным TCP или UDP портам с возможностью дополнительного указания одного IP-адреса или диапазона адресов.

Рисунок 13. Настройка сетевого контроля



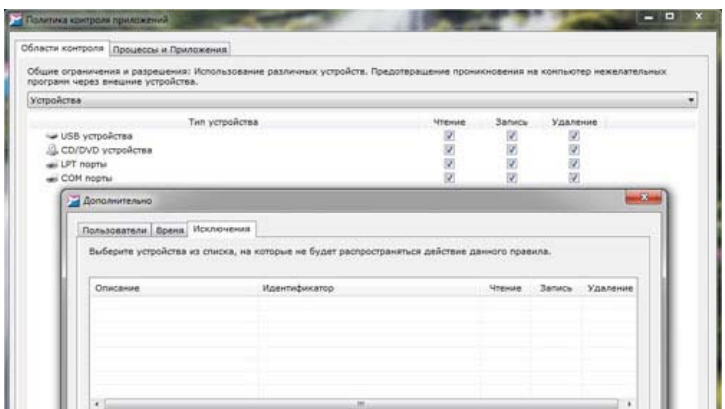
Привилегии процессов. Позволяет разрешить или запретить процессам выполнение определенных действий.

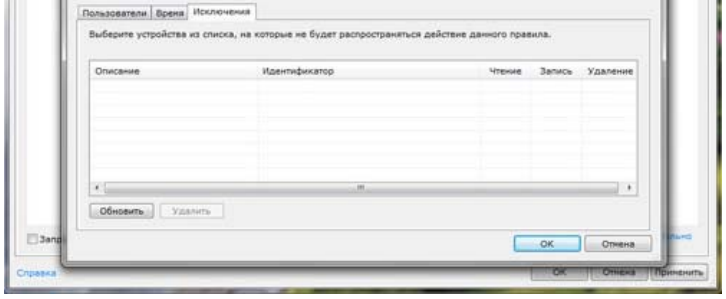
Рисунок 14. Настройка привилегий процессов



Устройства. Применяется для контроля различных портов и устройств, которые могут использоваться для хранения информации. Можно разрешать или запрещать чтение, запись и удаление данных на них. Дополнительно можно устанавливать время работы правил, круг пользователей, на который они действуют, а также исключения (устройства, к которым правила не применяются.)

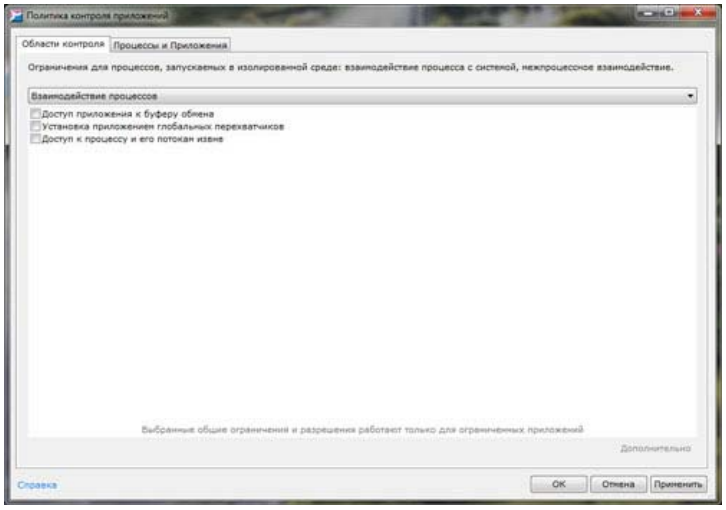
Рисунок 15. Настройка контроля устройств





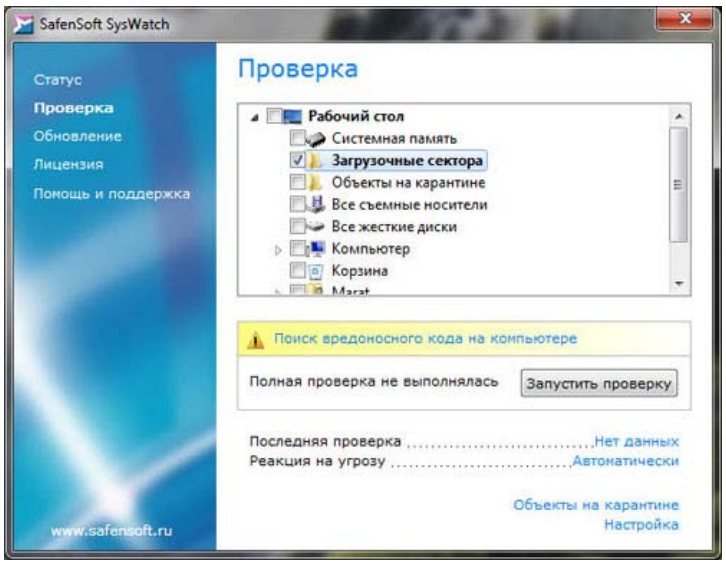
Взаимодействие процессов. Используется для разрешения или запрета доступа ограниченных процессов к взаимодействию с системой и обмена данными между процессами.

Рисунок 16. Настройка контроля взаимодействия процессов



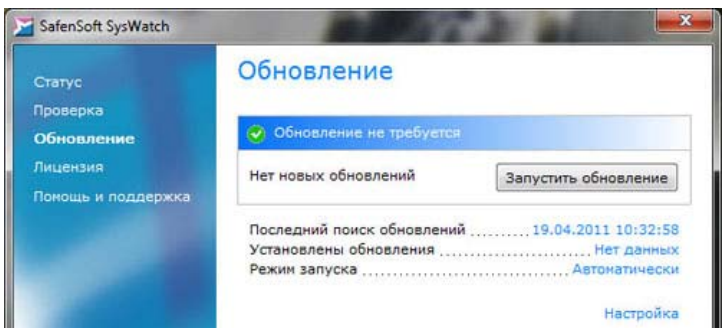
Следующая вкладка главного окна программы – «Проверка». Она применяется для сканирования компьютера или отдельных его областей встроенным антивирусным сканером. Кроме того, на ней же можно просмотреть информацию о дате последней проверки, а также перейти к работе с карантином, в который помещаются найденные подозрительные объекты.

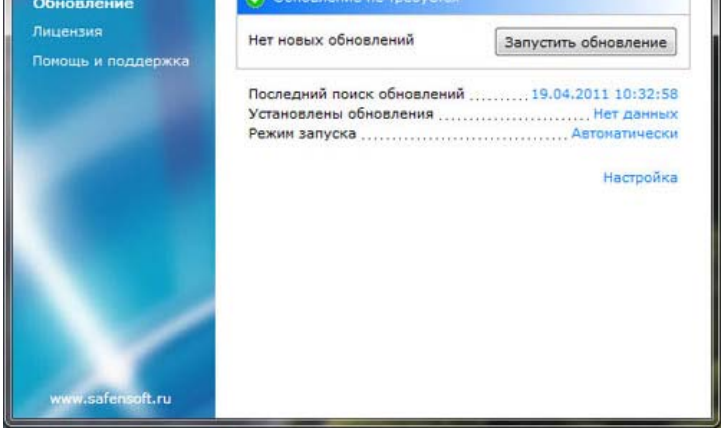
Рисунок 17. Вкладка работы с антивирусным сканером



Третья вкладка главного окна называется «Обновление». Она используется для периодической актуализации антивирусных баз сканера. Обратите внимание, что эффективность работы проактивной защиты никак не зависит от обновлений данного модуля защиты.

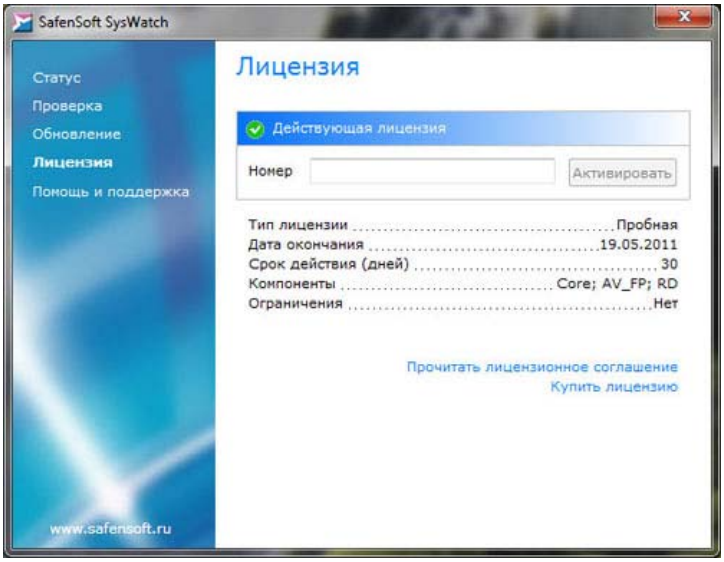
Рисунок 18. Вкладка обновления базы антивирусного сканера





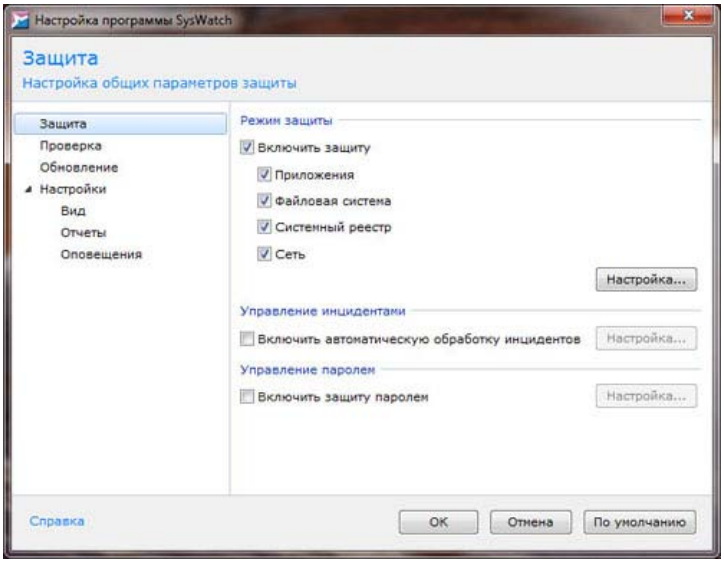
Последние две вкладки главного окна можно назвать сугубо информационными. Они нужны для просмотра сведений о текущей лицензии, а также доступа к справочным данным.

Рисунок 19. Вкладка просмотра лицензии



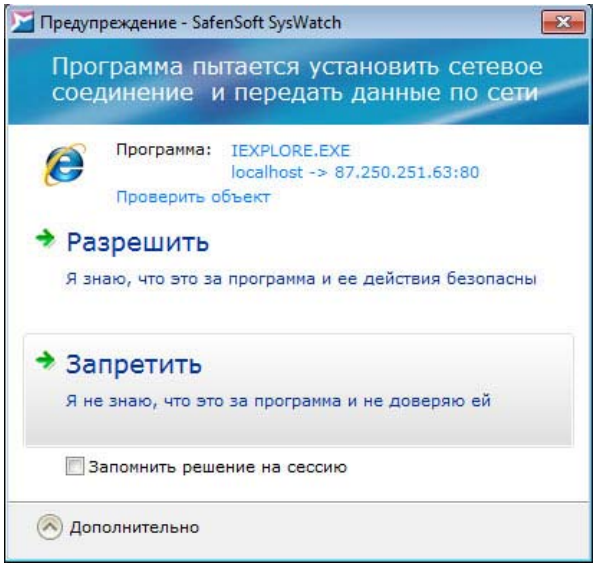
Для установки параметров работы SysWatch Deluxe используется специальное окно настройки, попасть в которое можно непосредственно из главного окна. Оно, в свою очередь, состоит из нескольких вкладок. Первая используется для установки параметров проактивной защиты, вторая – антивирусного сканера, а третья – системы обновления. Кроме того, в этом же окне можно установить пароль для защиты рабочей конфигурации программы, включить или отключить внешнее управление, выбрать язык интерфейса, настроить работу системы оповещения и т.п.

Рисунок 20. Окно работы программы



В процессе работы SafenSoft SysWatch Deluxe может выдавать пользователю некоторые запросы, например, при попытке приложений из ограниченной группы выполнить потенциально опасные действия.

Рисунок 21. Попытка приложения из ограниченной группы установить сетевое соединение



Выводы

Ну а теперь пришла пора подвести итог нашего сегодняшнего разговора. Подробно рассмотрев возможности и особенности использования программы SafenSoft SysWatch Deluxe можно сказать следующее. Данная система действительно является полноценным HIPS-решением, принцип действия которого основан на контроле активности процессов и приложений. Реализованные в ней технологии позволяют предотвращать проникновение в систему вредоносных программ различного типа, а также запускать потенциально опасные программы в изолированной среде (т.н. «песочнице»), где они точно не смогут нанести вред системе.

Интересной особенностью SafenSoft SysWatch Deluxe является возможность очень тонкой настройки доступа процессов и приложений к файлам и папкам, системному реестру, сети, устройствам и пр. Это не только повышает надежность защиты от вредоносных программ, но и позволяет обезопасить конфиденциальную информацию, в частности, персональные данные.

Также можно отметить и традиционный антивирусный сканер. В нем реализован как сигнатурный поиск вирусов, так и эвристические технологии. Использование сканера не обязательно, поскольку проактивная защита надёжно предотвращает заражение системы. Однако он может пригодиться при установке программы (на тот случай, если вдруг система была инфицирована до инсталляции SysWatch Deluxe), при активной работе со съемными накопителями (в сканере есть функция их автоматической проверки) и т.п.

При всем при этом SafenSoft SysWatch Deluxe остается достаточно простым в использовании продуктом. Функция автонастройки создает правила для приложений автоматически, так что система защиты начинает работать сразу после установки. При последующей своей работе программа выдает относительно малое количество запросов, большинство из которых касается работы ограниченных приложений.

Тем не менее, надо понимать, что использование SafenSoft SysWatch Deluxe, как и любого другого решения HIPS, несколько отличается от применения традиционных антивирусов. В этом и с точки зрения рядового обывателя заключается его основной минус.

Так, например, после установки, все сетевые приложения, включая Internet Explorer, считаются доверенными. Если же пользователь хочет ограничить какие-то из них, то сделать это надо вручную. Также надо понимать, что SysWatch Deluxe хоть и выдает минимум для HIPS-решения запросов пользователю, их количество все равно будет больше, чем у традиционных антивирусов. Так что в целом использовать данный продукт несколько сложнее.

Другой особенностью SafenSoft SysWatch Deluxe является то, что он не является по своей сути продуктом комплексной защиты, т.е. не способен защитить от всего спектра современных угроз. Да, HIPS-решение может обезопасить компьютер от вредоносных программ. Но нельзя забывать еще и про спам, фишинговые атаки и многие другие опасности, с которыми сталкиваются пользователи Интернета. Это нельзя считать серьезным минусом рассмотренного сегодня продукта. Ибо HIPS-решения предназначены для решения узкой задачи - контроля приложений. Тем не менее, для домашних пользователей такой подход может привести к некоторым неудобствам из-за необходимости использования дополнительных инструментов защиты.

Продукт получает итоговую оценку 9 из 10 баллов.

Продукт получает награду Approved by Anti-Malware.ru