Обзор Safe'n'Sec TPSecure

14 июля, 2010 - 07:05 — Александр Панасенко

Теги: Обзоры Корпорации S.N.Safe&Software Safe'n'Sec Safe'n'Sec Enterprise Suite HIPS Антивирус TPSecure

Не так давно мы писали о комплексном решении Safe'n'Sec Enterprise Suite. В этом обзоре мы решили подробнее рассказать о Safe'n'Sec TPSecure, специализированной системе защиты банкоматов и платёжных терминалов от вредоносных программ и внедрения несанкционированных приложений для.

Введение

Продукт Safe'n'Sec TPSecure создан на основе технологии V.I.P.O. (Valid Inside Permitted Operations). Технология V.I.P.O. объединяет в себе адаптивное профилирование, выполнение приложений в защищенной среде (Sandbox) и подсистему поведенческого анализа (HIPS), гарантируя динамическое проактивное обеспечение целостности приложений. Поддержание безопасной работы приложений в режиме реального времени обеспечивает непрерывное исправное состояние сетей обработки транзакций и защиту от вторжения известных и новых вредоносных программ, включая угрозы "нулевого дня" от внешних и внутренних источников.

Поскольку эффективность защиты не зависит от обновлений сигнатур, в управлении системой не требуется оперативность, что создает идеальное решение для автоматических систем, таких как банкоматы, кассовые терминалы и терминалы систем электронного голосования. После установки и приведения системы в исходное исправное состояние, администрирование в постоянном режиме больше не требуется, система может автоматически блокировать атаку.

Системные требования

Операционные системы	Аппаратные требования
▪ Microsoft Windows XP Home Edition (SP 3) ▪ Microsoft Windows XP Professional Edition (SP 3) ▪ Microsoft Windows XP Professional x64 Edition (SP3)	▪ Процессор Intel Pentium x86/x64 с тактовой частотой 300 МГц или совместимый с ним ▪ Оперативной памяти не менее 256 МБ ▪ Не менее 40 МБ свободного дискового пространства
▪ Microsoft Windows Vista Home Basic x86/x64 (SP1) ▪ Microsoft Windows Vista Home Premium x86/x64 (SP1) ▪ Microsoft Windows Vista Business x86/x64 (SP1) ▪ Microsoft Windows Vista Ultimate x86/x64 (SP1)	▪ Процессор Intel Pentium x86/x64 с тактовой частотой 800 МГц или совместимый с ним ▪ Оперативной памяти не менее 512 МБ ▪ Не менее 40 МБ свободного дискового пространства

Основные возможности

- Легкость защиты терминала посредством удаленной или локальной установки (включая возможность "тихой" установки с импортом предустановленных настроек).
- Возможность настройки графического пользовательского интерфейса для любого размера экрана, что облегчает использование системы на широком спектре различных терминалов.
- График доступа к системным ресурсам позволяет выделить для обслуживания терминалов специальные периоды времени, повышая защиту от несанкционированного доступа.
- Наличие гибких настроек и правил доступа к данным предоставляет отдельным пользователям или группам пользователей многоуровневый доступ к информации.
- Настройка политик доступа приложений к файловой системе с использованием масок (например, возможность запретить изменение всех файлов с именем *.xml).
- Запрет доступа к системным ресурсам для всех приложений, кроме специально выбранных, существенно упрощает настройку системы.
- Возможность создания индивидуальных политик контроля для приложений.
- Обнаружение и предотвращение запуска вредоносных программ со съемных носителей.
- Централизованное формирование отчетов обо всех системных событиях, включая статус программы защиты на удалённых терминалах.
- Мониторинг в теневом режиме обеспечивает постоянное присутствие программного обеспечения на терминале. Оно не может быть обнаружено или удалено.
- Запись снимков экрана обеспечивает возможность просмотра и записи состояния экрана терминала в любой момент - как в онлайн-режиме, так и в ходе ретроспективного анализа.

- использование малого количества ресурсов и места в памяти ооеспечивает минимальные требования к производительности.

Установка

Возможна установка в трёх различных режимах – удалённая установка через консоль администрирования, являющуюся компонентом TPSecure, установка в тихом режиме, позволяющая сконфигурировать приложение на эталонном терминале и провести установку на другие терминалы из командной строки и обычный режим установки с использованием графического интерфейса на терминале.

Остановимся подробно на обычном режиме установки. Установка очень проста, в ходе которой используется installshield.

Рисунок 1: Начало установки Safe'n'Sec TPSecure

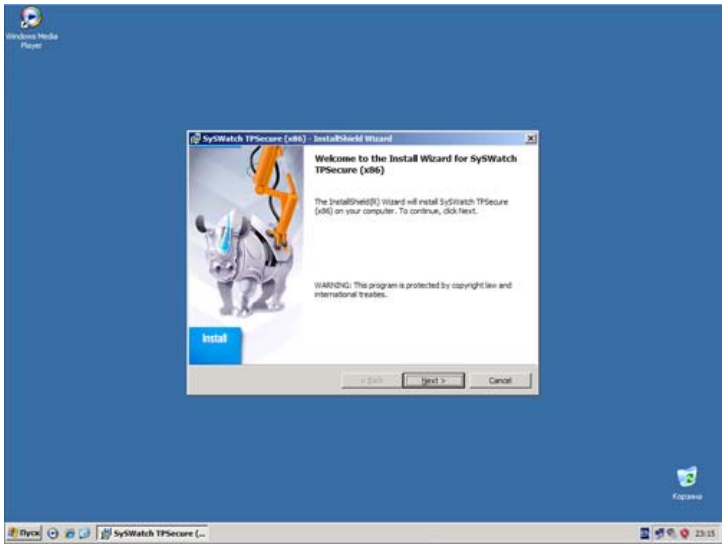


Рисунок 2: Выбор каталога для установки Safe'n'Sec TPSecure

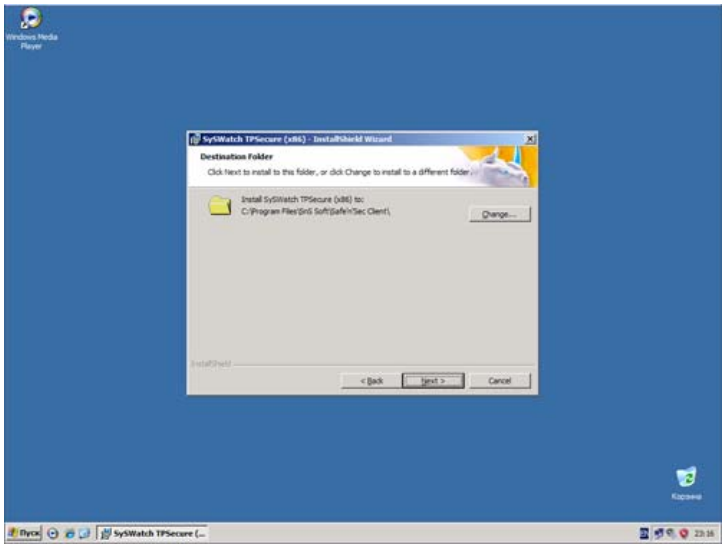
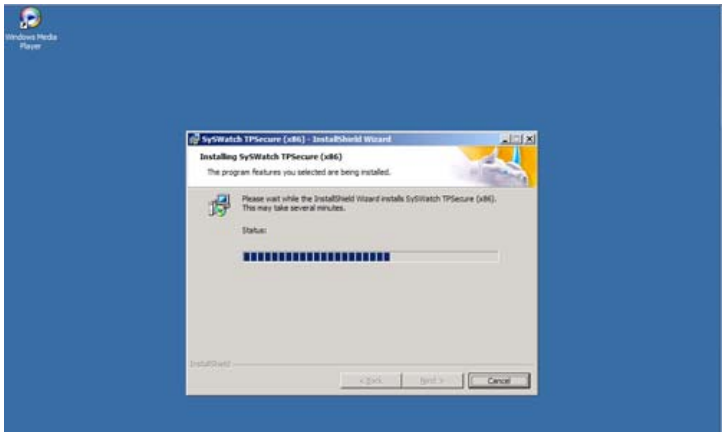


Рисунок 3: Ход установки Safe'n'Sec TPSecure



На этом с установкой всё. Как видим, никаких шаманств не нужно, всё проходит гладко и быстро.

Теперь переходим к настройке и работе этого продукта.

Настройка и работа Safe'n'Sec TPSecure

Safe'n'Sec TPSecure может работать как в автономном режиме, так и в режиме централизованного управления с помощью консоли администрирования Safe'n'Sec Admin Explorer. Для начала рассмотрим вариант автономного режима работы.

Перед началом работы с Safe'n'Sec TPSecure, необходимо провести его автоматическую настройку. Об этом мы уже рассказывали в обзоре Safe'n'Sec Enterprise Suite, в разделе про настройку клиентской части.

Для начала, обновим Safe'n'Sec TPSecure. Это можно сделать, щёлкнув правой кнопкой мыши на иконке в системном трее, и выбрав команду меню "Обновление". В открывшемся окне нужно нажать кнопку "Запустить обновление" (см. рисунок 4). Также, можно задать параметры обновление, в том числе и параметры прокси-сервера для соединения с сетью интернет (см. рисунок 5).

Рисунок 4: Окно Обновление Safe'n'Sec TPSecure

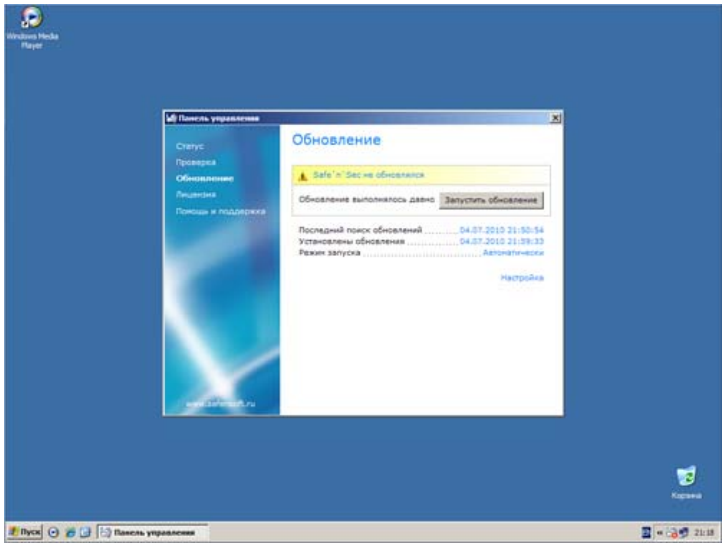
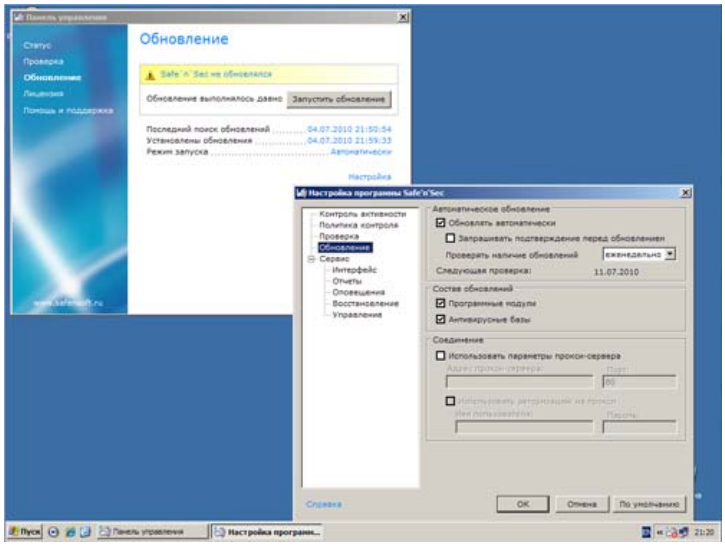
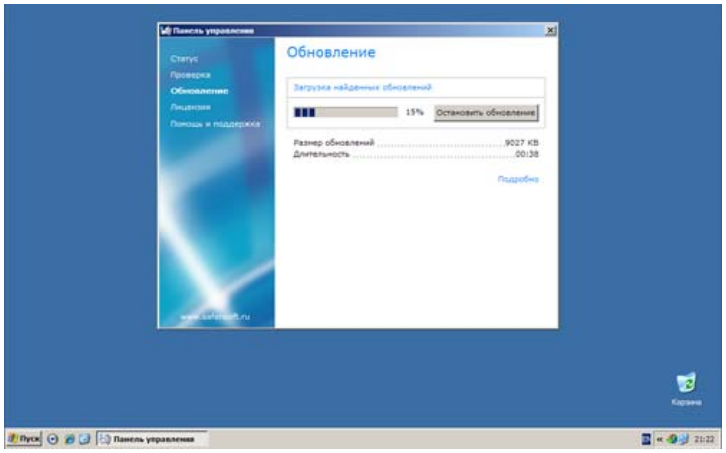


Рисунок 5: Настройка параметров обновления Safe'n'Sec TPSecure



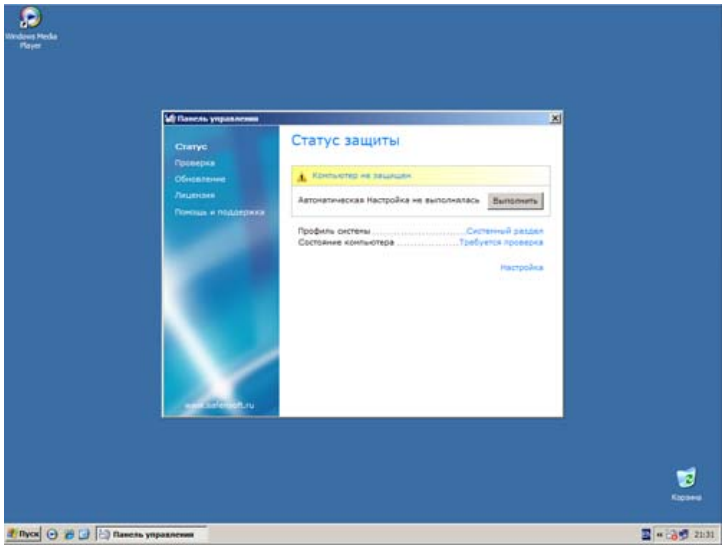
На рисунке 6 показан ход обновления Safe'n'Sec TPSecure.

Рисунок 6: Ход обновления Safe'n'Sec TPSecure



Чтобы провести автоматическую настройку Safe'n'Sec TPSecure необходимо открыть панель управления Safe'n'Sec TPSecure. Для этого нужно щёлкнуть правой кнопкой мыши на иконке в трее и выбрать команду меню "Safe'n'Sec TPSecure".

Рисунок 7: Панель управления Safe'n'Sec TPSecure



Как видим, необходимо выполнить автоматическую настройку.

Для эффективной защиты компьютера и проверки установленных приложений, Safe'n'Sec создает Профиль системы при первом запуске программы. Использование Профиля системы позволяет:

- Разделить все выполняющиеся на терминале приложения на безопасные/известные и потенциально опасные/неизвестные
- Выполнить неизвестные приложения в ограниченной среде или автоматически блокировать.

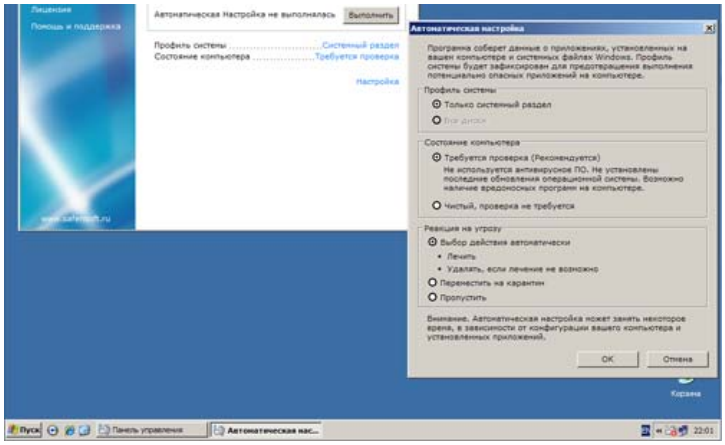
Создание Профиля системы состоит из нескольких этапов:

- Обновление компонентов автоматической настройки программы через Интернет. Если невозможно установить соединение с Интернет, то используются компоненты, входящие в поставку продукта.
- Поиск и сбор информации обо всех исполняемых файлах (exe, com, dll и т.д.) на терминале.
- Идентификация файлов приложений по следующим признакам:
  - наличие доверенного сертификата (цифровой подписи) у приложения;
  - наличие записи о приложении в файлах каталога (cat -файлы) Windows;
  - наличие записи о приложении в "белом" списке приложений Safe'n'Sec.
- Назначение ограничений выполнения приложения:
  - доверенное или известное приложение (выполняется только с Частными ограничениями);
  - ограниченное приложение (выполняется с Общими и Частными ограничениями);
  - заблокированное приложение (выполнение запрещено).
- Проверка файлов приложения антивирусным модулем.

После создания профиля системы программа отслеживает выполнение новых или неизвестных приложений (информации о которых нет в профиле системы), блокирует опасные действия и предупреждает о подозрительной активности.

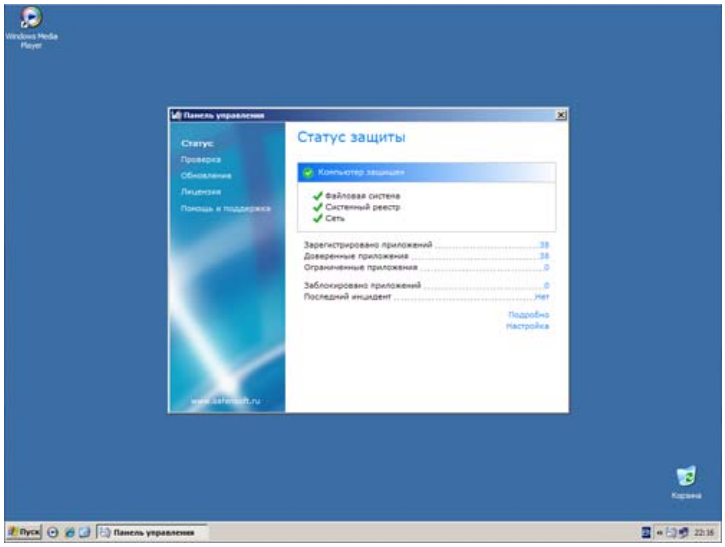
Перед запуском автоматической настройки можно настроить профиль исследования системы (см. рисунок 8).

Рисунок 8: Настройка профиля исследования системы Safe'n'Sec TPSecure



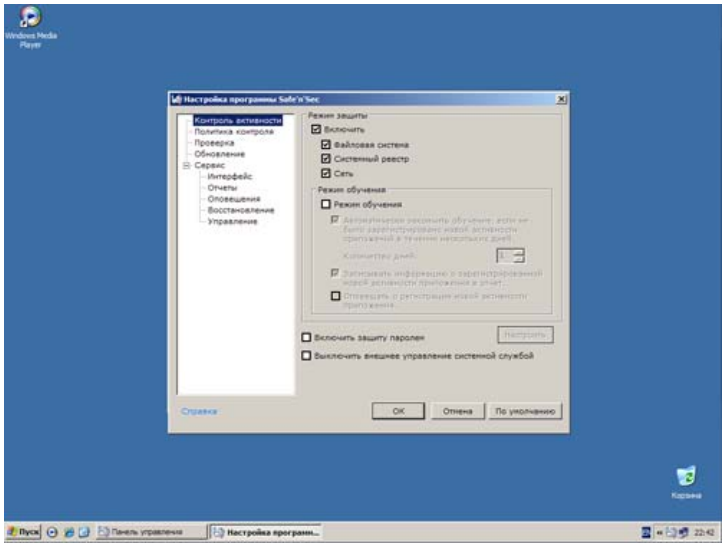
Для создания профиля системы требуется некоторое время. Скорость проверки и настройки зависит от количества установленных приложений и мощности аппаратной части.

Рисунок 9: Окончание автоматической настройки Safe'n'Sec TPSecure



Теперь можно перейти к настройкам. Для этого можно нажать на ссылку "Настройка" в этом же окне или воспользоваться контекстным меню приложения используя иконку приложения в трее. Первый пункт настроек – контроль активности (рисунок 10).

Рисунок 10: Настройки контроля активности Safe'n'Sec TPSecure



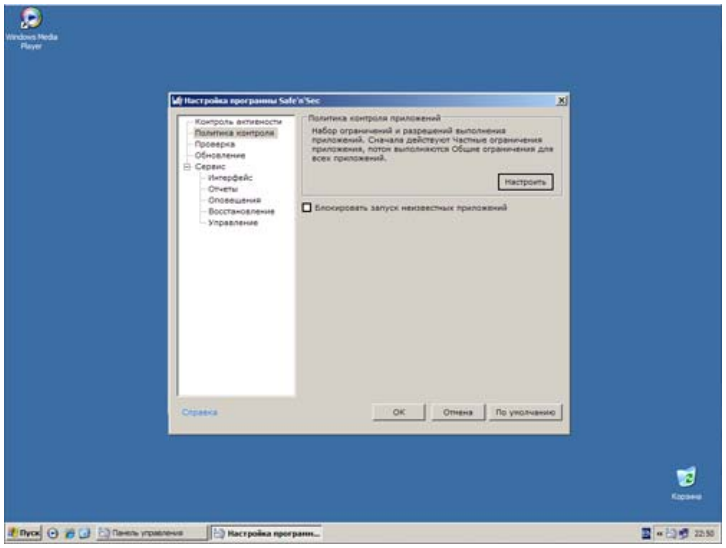
По умолчанию Safe'n'Sec TPSecure контролирует файловую систему, системный реестр и сеть. Вендор не рекомендует отключать защиту какой-либо из этих областей, так как это снизит уровень безопасности.

После установки программы, Safe’n’Sec TPSecure использует встроенную базу наиболее известных приложений и политик контроля этих приложений, которая периодически пополняется

через обновления программы.

Однако на теминале могут быть установлены неизвестные Safe'n'Sec TPSecure программы, и некоторые действия таких программ могут быть расценены Safe'n'Sec TPSecure как потенциально опасные. Режим обучения предназначен для автоматического исследования и создания политики контроля активности неизвестного приложения. В процессе обучения Safe'n'Sec TPSecure самостоятельно создает политику контроля активности такого приложения.

Рисунок 11: Настройки политики контроля Safe'n'Sec TPSecure



Политика контроля это набор правил, на основании которых осуществляется контроль активности приложений и их анализ, а также выносится заключение об опасности приложения. Именно политика определяет, какие действия и какую их последовательность считать опасной.

Превентивные технологии, на которых построен **Контроль активности приложений**, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред компьютеру. В отличие от реактивных технологий, где анализ выполняется на основании сигнатурных баз вредоносных приложений, превентивные технологии распознают новую угрозу по последовательности действий, выполняемой некоторой программой. Safe'n'Sec TPSecure блокирует потенциально опасную активность неизвестных или уязвимых приложений, сохраняя целостность системы.

Например, при обнаружении таких действий как копирование некоторой программы в системный каталог, в каталог автозапуска, системный реестр, а также последующая рассылка копий, можно с большой долей вероятности предположить, что это программа – червь. К опасным последовательностям действий также относятся:

- действия, характерные для троянских программ;
- попытки перехвата ввода с клавиатуры;
- скрытая установка драйверов;
- попытки изменения ядра операционной системы.

Рисунок 12: Области контроля Safe'n'Sec TPSecure

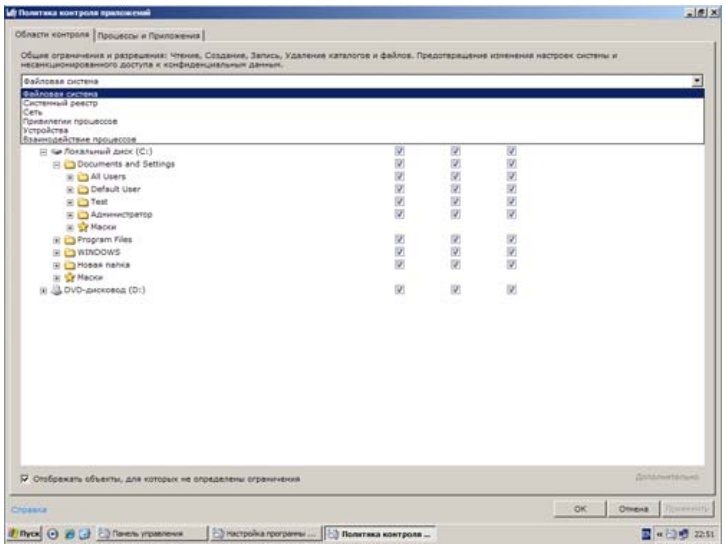
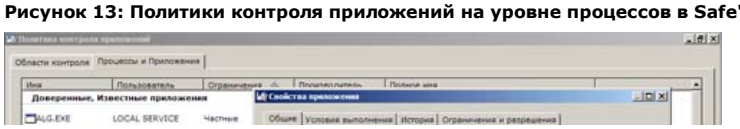
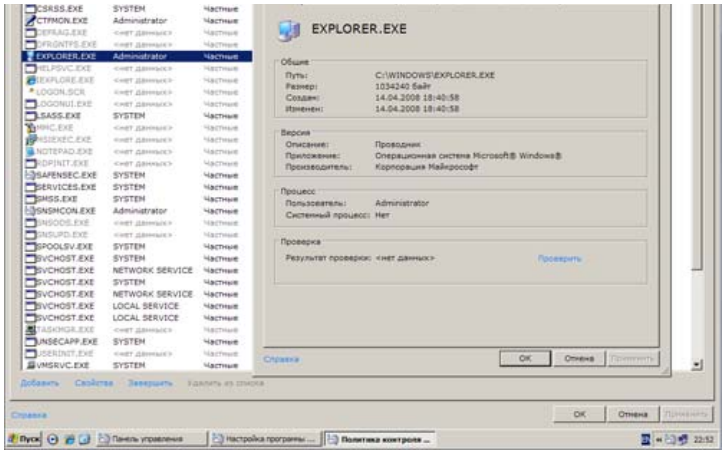


Рисунок 13: Политики контроля приложений на уровне процессов в Safe'n'Sec TPSecure



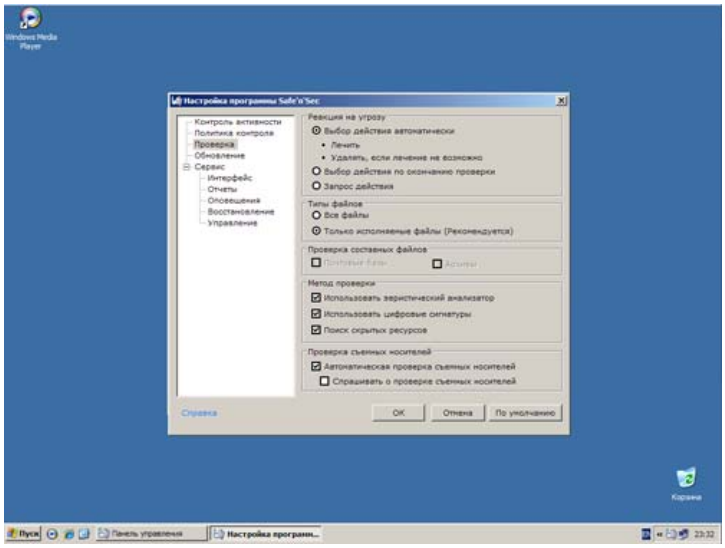


Настройка прав доступа в областях контроля, работа со списком доверенных приложений, задание разрешений, правила работы с сетью – всё это подробно описано **в обзоре Safe'n'Sec Enterprise Suite**

Логика работы Safe'n'Sec TPSecure основывается на жёстком разграничении прав доступа и списке доверенных приложений. Банкоматы и платёжные терминалы относятся к системам с очень редким изменением установленных приложений. Поэтому выполнив автоматическую настройку, отредактировав права доступа, запретив работу со съёмными устройствами и отредактировав список доверенных приложений в соответствии с требованиями безопасности, можно запретить запуск всем недоверенным приложениям. Таким образом, мы исключаем возможность запуска вредоносного кода или несанкционированных программ со стороны персонала.

Для проверки системы на наличие вредоносного кода используется могут быть использованы встроенные антивирусные модули VBA32 или Bitdefender.

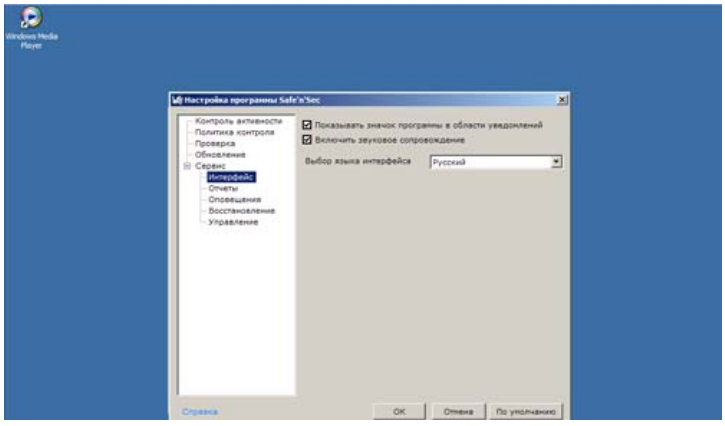
Рисунок 14: Настройка параметров антивирусной проверки в Safe'n'Sec TPSecure



Меню **Сервис** включает в себя несколько подменю.

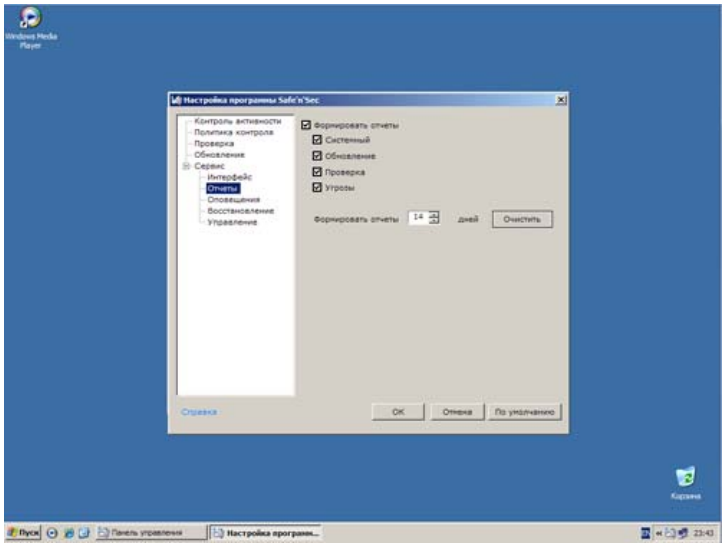
Интерфейс. Можно указать, нужно ли отображать значок интерфейса в трее; включить звуковое сопровождение событий и выбрать язык интерфейса программы.

Рисунок 15: Настройки интерфейса в Safe'n'Sec TPSecure



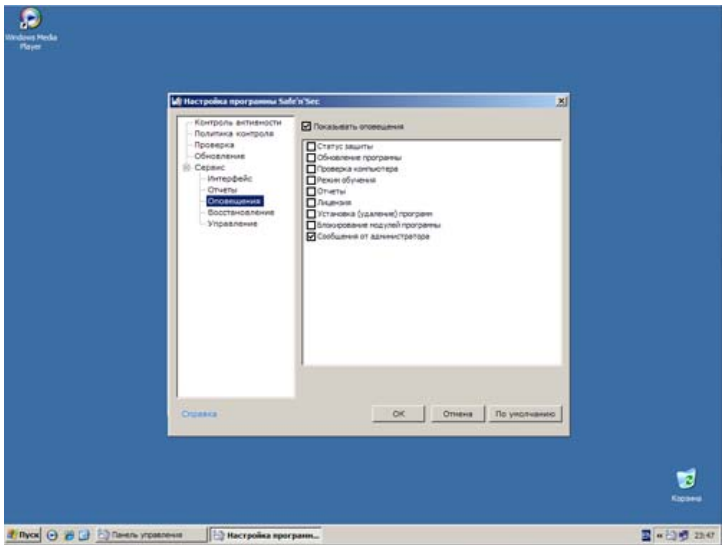
Отчёты. Safe'n'Sec TPSecure позволяет вести отчёты, записывая в них события о тех или иных инцидентах, результаты обновления и пр. Также, можно указать сроки хранения отчётов.

Рисунок 16: Настройки отчётов в Safe'n'Sec TPSecure



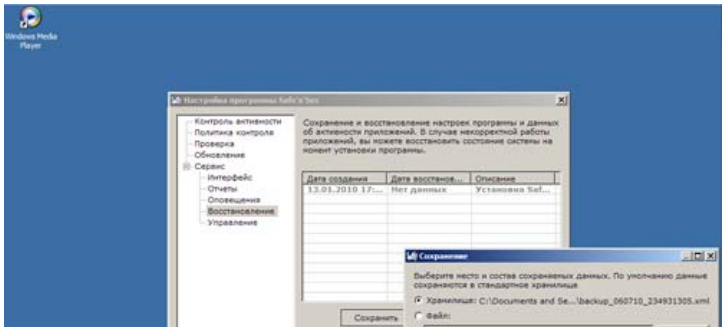
Оповещения. Safe'n'Sec TPSecure позволяет отображать оповещения о тех или иных событиях. По умолчания включены только лишь оповещения от администратора.

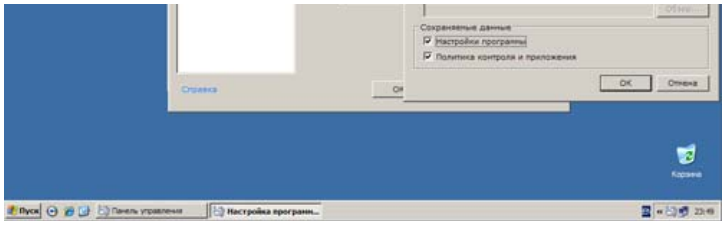
Рисунок 17: Настройки оповещений Safe'n'Sec TPSecure



Восстановление. Учитывая обширность и сложность настроек политик и прочего, разработчики Safe'n'Sec TPSecure предусмотрели возможность сохранения всех настроек и их восстановления из резервной копии.

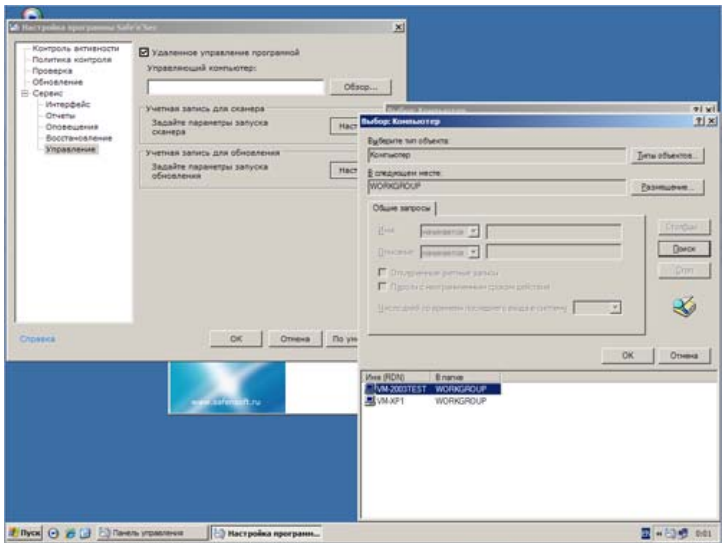
Рисунок 18: Сохранение конфигурации и правил Safe'n'Sec TPSecure





Управление. Safe'n'Sec TPSecure поддерживает удалённое централизованное управление. Для того, чтобы подключить Safe'n'Sec TPSecure к центру управления, необходимо найти и выбрать его в списке компьютеров и указать с какими учётными данными будет осуществляться запуск сканера и обновления (см. рисунок 19).

Рисунок 19: Настройка параметров удалённого управления Safe'n'Sec TPSecure



После того, как указаны параметры удалённого управления, Safe'n'Sec TPSecure автоматически подключиться к выбранному серверу (см. рисунок 20). Для включения конечной точки с установленным Safe'n'Sec TPSecure в список обслуживаемых, в консоли управления необходимо нажать на ссылку "Добавить компьютер".

Рисунок 20: Конечная точка с установленным Safe'n'Sec TPSecure подключена к серверу управления

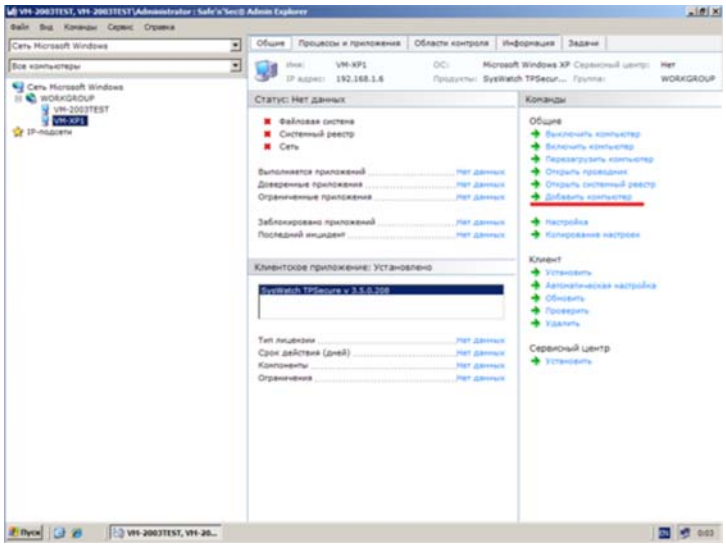
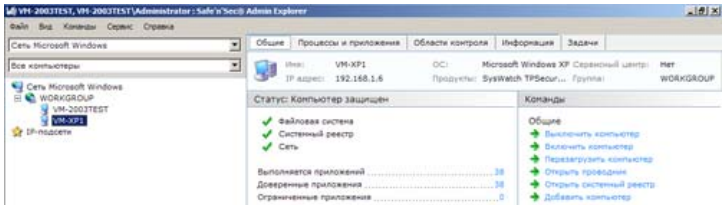
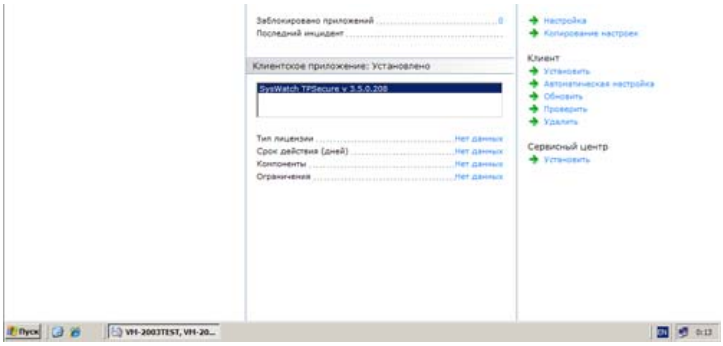


Рисунок 21: Конечная точка с установленным Safe'n'Sec TPSecure авторизована на сервере управления





Как видно на рисунке 21, мы теперь получаем данные с этой точки и можем ею управлять. Подробно об управлении конечной точкой сети с установленным клиентом Safe'n'Sec можно прочитать в обзоре **"Safe'n'Sec Enterprise Suite".**

Сразу отметим, что дополнительный модуль DLP Guard, с помощью которого осуществляется удалённое наблюдение за терминалом, в рамках данного обзора не рассматривался. Подробное описание модуля можно прочитать в обзоре **"Safe'n'Sec Enterprise Suite".** Используя централизованное управление, служба безопасности получает множество преимуществ в контроле над соблюдением режима безопасности на столь важных объектах как банкоматы и платёжные терминалы.

На этом мы заканчиваем обзор Safe'n'Sec TPSecure. В данном обзоре мы постарались максимально информативно рассказать об этом продукте и осветить основные аспекты работы и настройки.

Выводы

Safe'n'Sec TPSecure является перспективным отраслевым решением, предназначенным специально для защиты банкоматов и платёжных терминалов под управлением ОС Windows от внедрения вредоносных программ и их несанкционированной активности. Safe'n'Sec TPSecure разработан на основе принципиального нового подхода по сравнению с классическими антивирусами. Он не требует постоянного обновления. В его основе лежат технологии поведенческого анализа и контроля целостности приложений (HIPS с использованием sandbox (песочницы) и whitelisting (белые списки)). В результате такого подхода. Safe'n'Sec TPSecure при работе отнимает минимальное количество системных ресурсов и не требователен к каналу связи, что очень важно именно для защиты банкоматов и платежных терминалов.

Safe'n'Sec TPSecure способен контролировать файловую систему, системный реестр и сеть, обеспечивая активный мониторинг всех операций системы, одновременно защищая ее от внедрения несанкционированных приложений и вредоносного ПО через сеть.

Однако технологическая новизну продукта можно отнести и к его относительным недостаткам, так как его установка и настройка политик безопасности требует от персонала достаточно высокого уровня знаний и квалификации. Несмотря на это Safe'n'Sec TPSecure можно считать оптимальным для банкоматов, платежных систем и других типовых конфигураций.

Наша субъективная оценка решения Safe'n'Sec TPSecure - 9 из 10 баллов.

Продукт получает награду Approved by Anti-Malware.ru

Список рекомендуемых нами продуктов »

Автор обзора:
Алексей Баранов

Средняя оценка: 5 (голосов: 7)