Обзор Safe'n'Sec Enterprise Suite

6 апреля, 2010 - 15:11 — Александр Панасенко

Теги: Обзоры Корпорации S.N.Safe&Software Safe'n'Sec Enterprise Suite HIPS Антивирус Защита от утечек Политики

В данном обзоре мы рассмотрим Safe'n'Sec Enterprise Suite – новое поколение корпоративных систем защиты конечных точек от вредоносных программ и действий инсайдеров, базирующееся на проактивных технологиях сохранения целостности системы и поведенческом анализе. В первую очередь решение ориентировано на защиту типовых рабочих станций, банкоматов и платежных терминалов на базе Microsoft Windows.

1. Введение
2. Системные требования
3. Концепция корпоративных продуктов Safe'n'Sec
4. Основные функции Safe'n'Sec Enterprise Suite
5. Установка Safe'n'Sec Enterprise Suite
6. Настройка и примеры использования Safe'n'Sec Enterprise Suite
7. Выводы

Введение

Основное назначение Safe'n'Sec Enterprise Suite – это защита информационного актива компании от внешних угроз, таких как вторжения хакеров и вредоносные программы, и внутренних угроз, таких как неосторожные или умышленно деструктивные действия сотрудников.

В основе Safe'n'Sec Enterprise Suite лежит передовая разработка компании S.N.Safe & Software - технология V.I.P.O. (Valid Inside Permitted Operations), которая построена на гибком разграничении системных привилегий при работе компьютера. Продукты, использующие технологию проактивной защиты V.I.P.O, вообще не требуют никакой настройки для начала полноценного функционирования, они оснащены прочным запасом правил поведения (составленных и постоянно обновляемых специалистами по информационной безопасности компании S.N. Safe&Software), достаточным для большинства пользователей.

Использование проактивной технологии поведенческого анализа, списков доверенных приложений (whitelisting - белый список), безопасной виртуальной среды (sandbox - песочница), контроля приложений, доступа к данным и аппаратным компонентам конечных точек, совместимость со многими сторонним антивирусным программным обеспечением и оптимизированная консоль управления делают Safe'n'Sec Enterprise Suite мощным комплексом защиты с широкими возможностями.

С помощью Safe'n'Sec Enterprise Suite можно эффективно защитить типовые рабочие станции, сервера, банкоматы или POS-терминалы, работающие на операционной системе Microsoft Windows.

Системные требования

Системные требования для Safe'n'Sec Service Center

Аппаратные требования:

- 2 МБ свободного пространства на жестком диске для программных модулей;
- дополнительно 1 Гб свободного пространства на жестком диске для базы данных;
- дополнительно 50 МБ свободного пространства на жестком диске для хранения обновлений;

Для Microsoft Windows XP Professional (Service Pack 2)/XP Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

- Microsoft SQL 2005 Express (Service Pack) и выше;
- Microsoft Windows Instal ler v 4.5 и выше;
- Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Системные требования для Safe'n'Sec Client

Аппаратные требования:

- 20 МБ свободного пространства на жестком диске;
- 50 МБ свободного пространства на жестком диске для хранения антивирусных баз;

Для Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

- Microsoft SQL Reporting Services для отчетов DLP Guard
- Microsoft Windows Instal ler v 4.5 и выше;
- Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Системные требования для Safe'n'Sec Admin Explorer

Аппаратные требования:

- 2 МБ свободного пространства на жестком диске или сменном носителе;

Для Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:

- Процессор Intel Pentium III 800 МГц;
- 256 МБ свободной оперативной памяти;

Для Microsoft Windows Vista (x86) Home Premium Edition/ Business Edition/ Enterprise Edition/Ultimate Edition, Microsoft Windows 7:

- Процессор Intel Pentium III 1 ГГц;
- 512 МБ свободной оперативной памяти;

Программные требования:

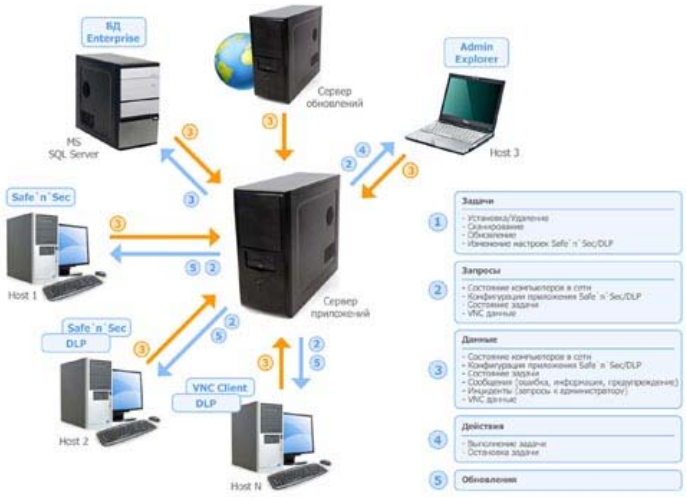
Microsoft Internet Explorer 6.0 или выше (для обновления программных модулей через интернет).

Концепция корпоративных продуктов Safe'n'Sec

Интегрированный программный продукт Safe'n'Sec Enterprise Suite состоит из двух модулей SysWatch и DLP Guard, каждый из которых выполняет определенный набор функций и может быть приобретен отдельно как самостоятельный программный продукт. При использовании этих модулей вместе с консолью администрирования вы получаете единый продукт, обеспечивающий многоцелевую защиту корпоративной сети от внешних и внутренних угроз, а также экономию бюджета вследствие оптимального использования ресурсов.

Рисунок 1: Концепция Safe'n'Sec Enterprise Suite

Риснок 2: Схема работы Safe'n'Sec Enterprise Suite



Основные функции Safe’n’Sec Enterprise Suite

Основные функциональные компоненты и их возможности:

Как мы уже говорили, Safe'n'Sec Enterprise Suite состоит из двух модулей SysWatch и DLP Guard + консоль управления + сервисные центры.

Клиентские агенты SysWatch и DLP Guard устанавливаются на любой компьютер корпоративной сети. Они позволяют проводить анализ активности приложений, блокируют опасные действия, обеспечивают защиту от вредоносного кода и хакерских атак. Осуществляют

опасные действия, обеспечивают защиту от вредоносного кода и хакерских атак. Осуществляют контроль доступа и использование системных ресурсов. Версии агентов с интегрированными антивирусными модулями дополнительно способны лечить зараженные системы или выполнять функцию второго антивируса в корпоративной среде, если это необходимо для удовлетворения требований безопасности. Давайте рассмотрим возможности этих модулей более подробно.

Safe'n'Sec SysWatch

Модуль Safe'n'Sec SysWatch – это новое поколение систем защиты конечных точек, базирующееся на проактивных технологиях сохранения целостности системы и поведенческом анализе. Он решает проблемы защиты конфиденциальной информации от хакерских вторжений и внедрения вредоносного кода. **SysWatch** можно приобрести в комплекте с антивирусным сканером BitDefender, VBA32 или Dr.Web.

Модуль обеспечивает защиту конечных точек корпоративной сети, работающих на операционной системе Microsoft Windows от новейших (zero-day) и специально написанных (целевые атаки) вредоносных программ.

Основной функционал Safe'n'Sec SysWatch:

- защита от направленных хакерских атак любой сложности;
- защита от всех типов известных вредоносных программ, таких как вирусы, черви, трояны, программы-шпионы, руткиты, кейлоггеры и прочие;
- защита от новейших вредоносных программ (zero-day), сигнатуры которых еще не внесены в антивирусные базы;
- анализ активности приложений и автоматическая блокировка опасных действий, которые могут привести к неработоспособности системы или порче/потере конфиденциальной информации.
- создание правил, реализующих политики безопасности по доступу к данным, USB устройствам, установке стороннего ПО.

Safe'n'Sec DLPGuard

Модуль DLP Guard осуществляет постоянный мониторинг и контроль сетевой активности пользователей, имеющих доступ к конфиденциальной информации предприятия. Продукт защищает от утечек информации, происходящих вследствие неосторожных действий сотрудников и злоумышленных действий инсайдеров.

DLP Guard контролирует реализацию политики безопасности путем создания правил контроля доступа пользователей (или групп пользователей) к определенным информационным ресурсам. Возможность скрытной установки системы мониторинга обеспечит постоянное присутствие программы без возможности ее обнаружения и удаления.

Также DLP Guard обеспечивает офицера службы безопасности информацией обо всех действиях, осуществляемых пользователем в локальной сети, фиксирует все сетевые события и создает аналитический отчет для ретроспективного анализа и расследования конкретного инцидента.

Основные функции Safe'n'Sec DLPGuard:

- мониторинг использования конфиденциальных файлов (операции чтения, записи, удаления файлов);
- мониторинг использования внешних устройств, например, USB-накопителей (операции чтения, записи, удаления файлов с USB устройств);
- просмотр экрана пользователя в режиме реального времени;
- видеозапись и воспроизведение записи экрана пользователя для анализа в случае подозрения на инсайдерский инцидент;
- запись текста, введенного с клавиатуры для любого приложения с помощью клавиатурного регистратора нажатия клавиш (отчет "Клавиатурный шпион");
- учет рабочего времени пользователя (общего и с каждым приложением);
- мониторинг изменений системного реестра;
- мониторинг всех сетевых событий;
- учет всех отправленных пользователем e-mail;
- мониторинг файлов, отправленных для печати на принтер;
- теневое копирование данных и сохранение на специальном ресурсе всех скопированных пользователем на внешние съёмные носители (CD, DVD, USB) файлы *;
- мониторинг посещаемых пользователем Интернет ресурсов и возможность подсчета расхода входящего и исходящего сетевого трафика, запрет использования определенных web-сайтов *;
- создание аналитических отчетов;

*- функция в разработке

Консоль управления и дополнительные сервисные центры

Централизованная система удаленного управления и организации рабочей области администрирования корпоративной сети необходима для эффективного управления и мониторинга современных комплексов защиты. А дополнительные сервисные центры позволяют сегментировать сетевую инфраструктуру на несколько рабочих областей.
Вот список основных задач, которые можно выполнять с помощью консоли управления:

- удаленная установка и настройка клиентских агентов, их автоматическому обновление;
- поиск и удаление известного вредоносного кода на удаленных компьютерах;
- групповые политики, единые настройки и общие задачи для группы компьютеров;
- импорт/экспорт настроек для последующего использования;
- разграничение прав администраторов на выполнение сервисных задач и изменение настроек клиентских программ;
- сервисные задачи и отчеты.

Установка Safe'n'Sec Enterprise Suite

Поскольку Safe'n'Sec Enterprise Suite продукт корпоративный, перед началом установки необходимо внимательно ознакомиться с Руководством по установке Safe'n'Sec Enterprise Suite, чётко и последовательно выполнять процесс установки и первоначальной настройки.

Для начала необходимо определиться с базой данных, которую нужно установить и настроить перед установкой Safe'n'Sec Enterprise Suite. Выбор базы данных прост — или Microsoft SQL Express (до 1000 клиентов), или Microsoft SQL Server (уже за деньги) при количестве клиентов больше 1000. Каждый экземпляр Safe'n'Sec Service Center, использующий Microsoft SQL Server, поддерживает до 5000 клиентов. Если требуется поддержка более 50 000 клиентов, то необходимо установить другой Safe'n'Sec Service Center.

Удалённая установка агентов на конечные точки сети требует соблюдение следующих условий:

- наличие прав локального администратора на компьютере, где осуществляется установка;
- работающая служба «Удалённый реестр»;
- настройка брандмауэра (открытие портов);
- для конечных точек на Windows Vista и Windows Server 2008, необходимо разрешить общий доступ к файлам и принтерам.

Список портов, которые используются приложением Safe'n'Sec Enterprise по умолчанию

Номер порта и протокол	**Описание**
TCP 3846	Связь между Safe'n'Sec Admin Explorer и Safe'n'Sec Service Center Связь между Safe'n'Sec Service Center и Safe'n'Sec Cl ient
TCP 80	Обновление Safe'n'Sec Client через Safe'n'Sec Service Center
TCP 1433	Связь между Safe'n'Sec Service Center и сервером базы данных

Может потребоваться изменить некоторые параметры операционной системы на клиентских компьютерах, на которых будут устанавливаться модули клиентских агентов.

Операционная система	**Конфигурация**
Windows XP в рабочей группе	Выключите простой общий доступ к файлам. Простой общий доступ к файлам может препятствовать развертыванию клиента.
Windows Vista и Windows Server 2008	Выключите мастер общего доступа к файлам. Включите поиск компьютеров в сети с помощью окна "Сеть и общий доступ". Проверьте наличие повышенного уровня прав доступа у вашей учетной записи.
Windows Vista и Windows Server 2008 в домене Active Directory	Учетная запись, применяемая для развертывания клиента, должна являться администратором домена и иметь повышенные права доступа на клиентском компьютере.

Сама установка не вызывает особых сложностей и проходит в несколько этапов. Вначале устанавливается Safe'n'Sec Admin Explorer, далее с его помощью - Safe'n'Sec Service Center. Затем уже через Safe'n'Sec Service Center происходит удаленная установка клиентских агентов Safe'n'Sec Client на конечные точки сети.

Рисунок 3: Окно установки Safe'n'Sec Admin Explorer

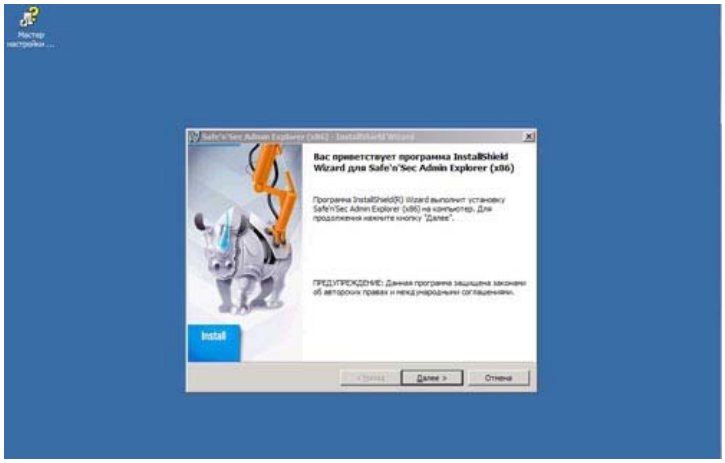
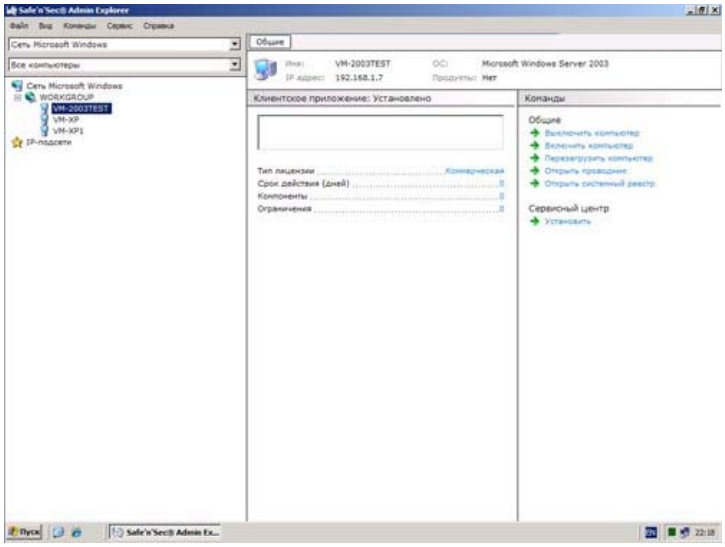
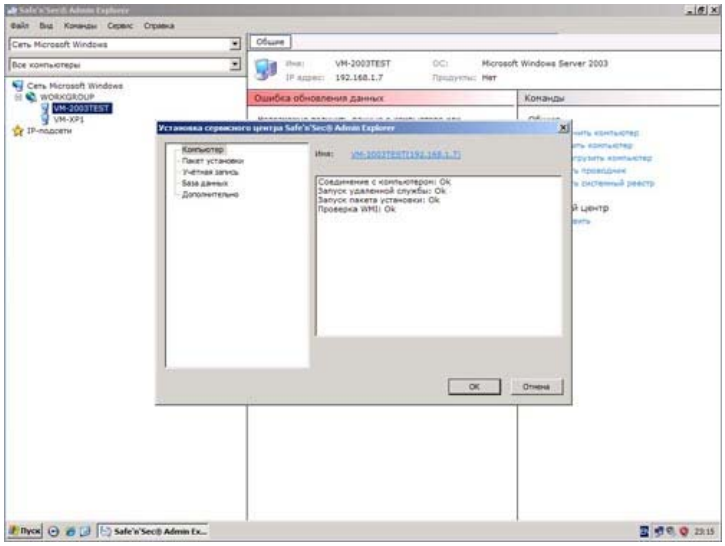


Рисунок 4: Главное окно Safe'n'Sec Admin Explorer



После того, как мы установили Safe'n'Sec Admin Explorer, необходимо из него установить Safe'n'Sec Service Center. Для этого, в Safe'n'Sec Admin Explorer необходимо выбрать точку сети, на которую мы будем устанавливать сервисный центр. В нашем примере это будет VM-2003TEST (см. рисунок 5).

Рисунок 5: Выбор точки сети и задание параметров установки сервисного центра

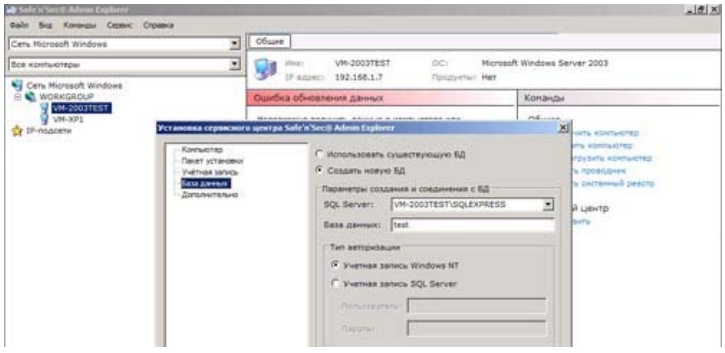


Как мы видим, можно сразу проверить возможность удалённой установки на конечную точку сети.

Важно не забыть создать новую базу данных перед установкой. Micrsoft SQL Server должен быть уже установлен на один из серверов в сети, проверен и настроен.

В параметрах установки указываем и лицензионный ключ.

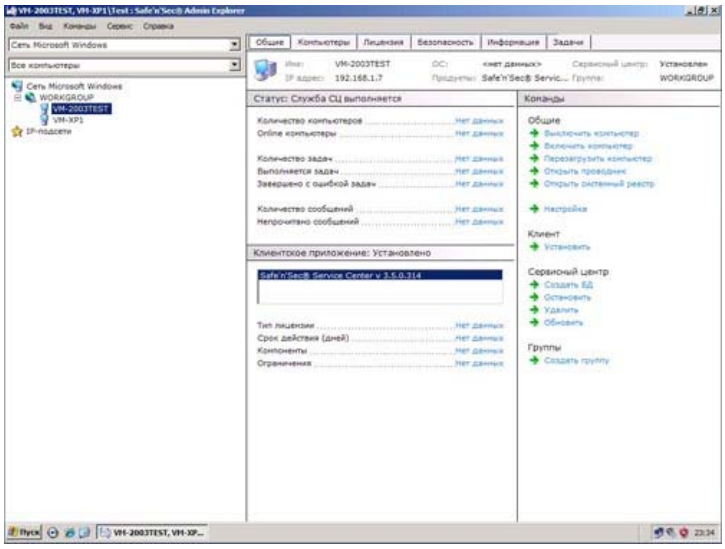
Рисунок 6: Создание базы данных для сервисного центра



Не забываем проверить соединение с сервером базы данных, кликнув по ссылку внизу окна установки сервисного центра.

После того, как был заданы все параметры, можно начинать установку сервисного центра. В итоге, при выборе в Safe'n'Sec Admin Explorer конечной точки сети, куда мы устанавливали сервисный центр, мы увидим полученный результат - сервисный центр запущен, проблем нет (клиентская часть ещё не установлена). Также можно просмотреть информацию о лицензии, а также список команд, которые можно выполнить на удалённой точке сети.

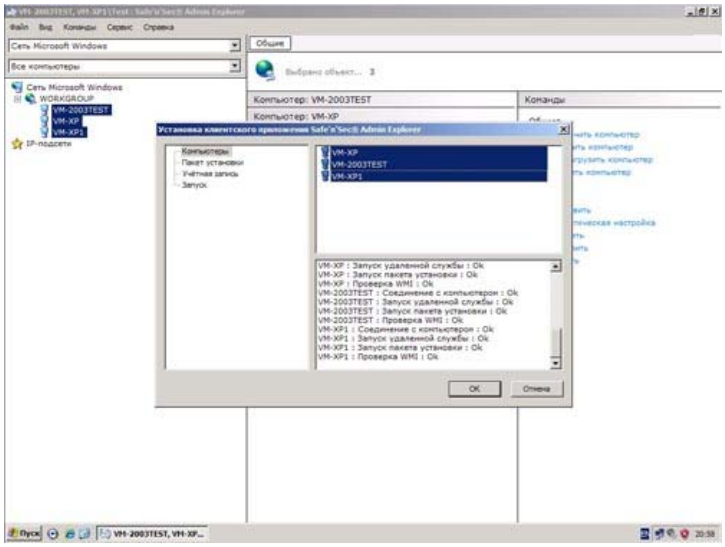
Рисунок 7: Просмотр статуса удаленной точки сети



Когда сервисный центр успешно установлен, можно приступать непосредственно к развертыванию защиты конечных точек сети, т.е. установке модулей SySWatch и DLP Guard. Ее можно производить сразу на несколько конечных точек сети.

Перед установкой Safe'n'Sec Admin Explorer проверяет ее возможность, выводы экспресс-отчет. Как видим на рисунке 8, проблем не возникло.

Рисунок 8: Выбор конечных точек сети для установки SySWatch и DLP Guard



Далее необходимо указать какой именно пакет установки (SySWatch или DLP Guard) мы собираемся использовать и указать лицензионный ключ.

Рисунок 9: Выбор пакетов для установки (SySWatch или DLP Guard)

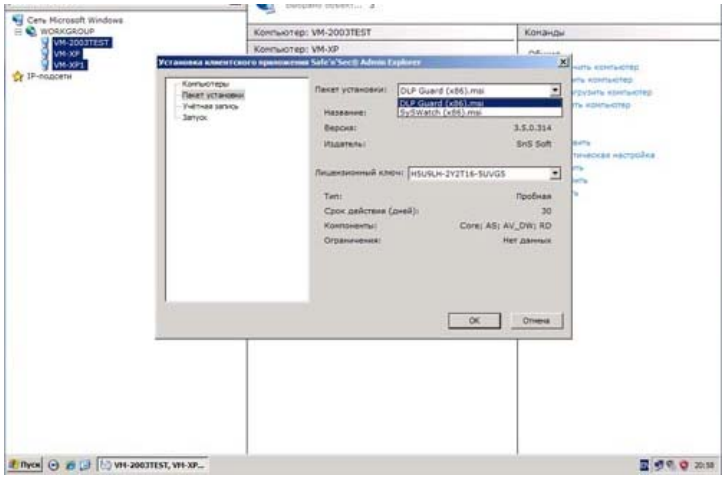
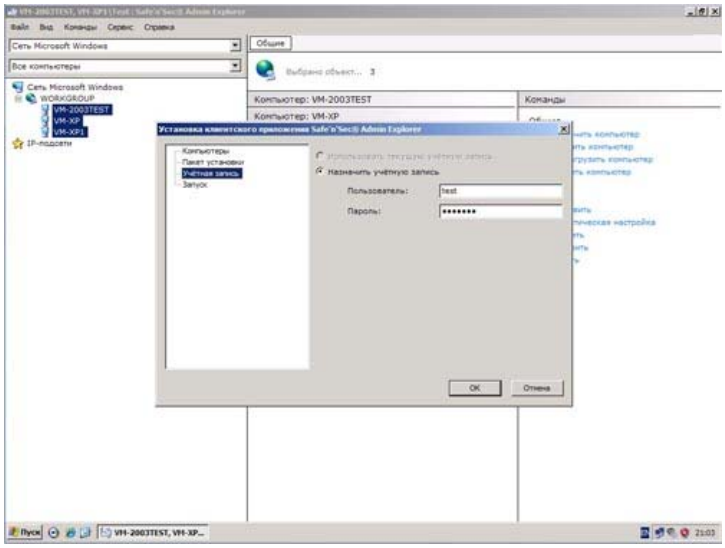
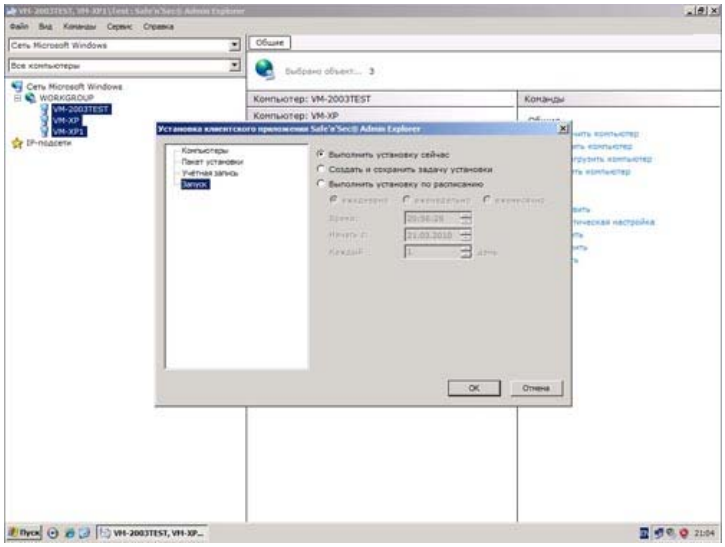


Рисунок 10: Задание учётной записи, от имени которой будет производиться установка



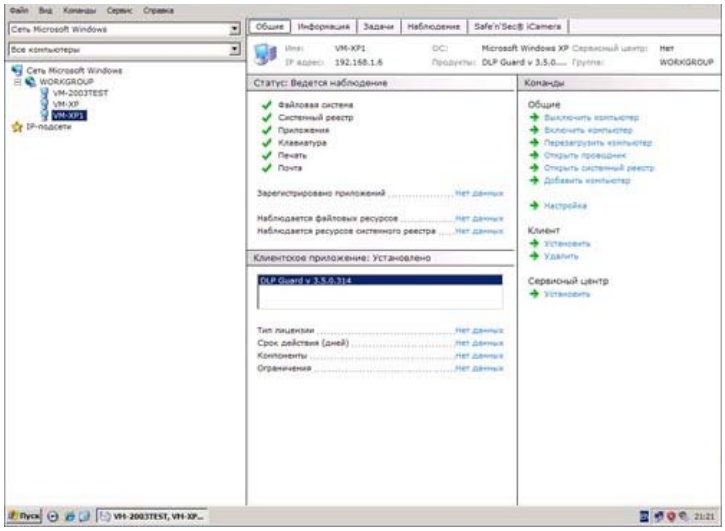
В завершение процедуры нужно указать время установки пакетов. Есть возможность сделать это немедленно или запланировать установку на определенное время, например, когда нагрузка на сеть и сами удаленные точки сети будет минимальная.

Рисунок 11: Выбор времени установки



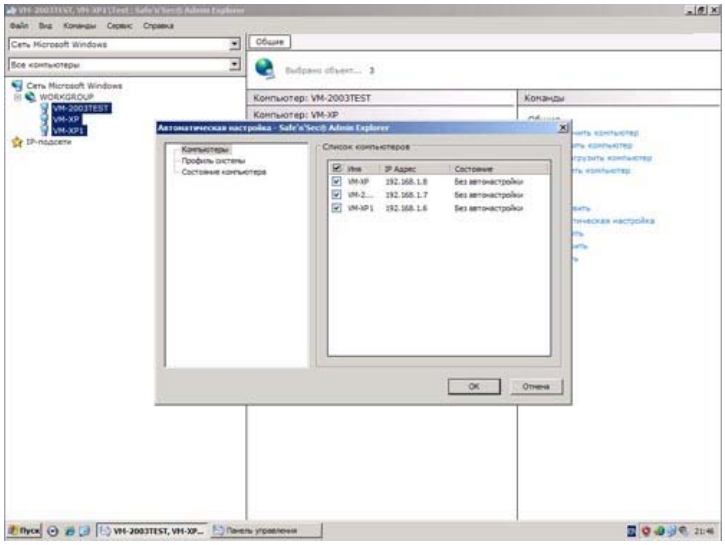
Для корректной работы модуля DLP Guard после его установки на конечных точках, их необходимо перезагрузить. После перезагрузки в Safe'n'Sec Admin Explorer увидим радостную картину в виде работающего модуля (галочки зелёного цвета возле областей контроля системы показывают, что DLP Guard ведёт за ними наблюдение).

Рисунок 12: Модуль DLP Guard, общее состояние



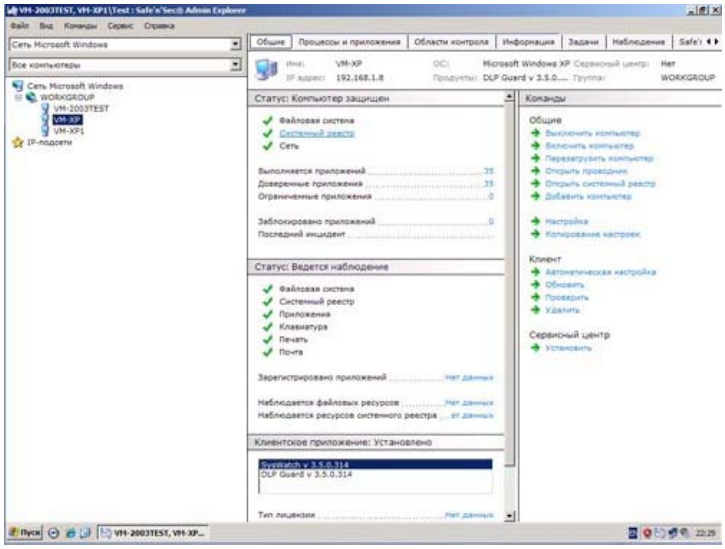
Установка модуля SysWatch проходит аналогично. После установки клиентов SySWatch, SySWatch + BitDefender или SySWatch TPSecure необходимо выполнить автоматическую настройку клиентов.

Рисунок 13: Задание параметров автоматической настройки клиентов SySWatch, SySWatch + BitDefender, SySWatch TPSecure



Автоматическая настройка займёт некоторое время. После ее окончания мы увидим, что в окне состояния конечной точки сети добавился модуль SysWatch, а также список областей системы, за которыми он ведёт наблюдение (рисунок 14).

Рисунок 14: Окно состояния после автоматической настройки



Теперь наши рабочие станции находятся под контролем. Давайте теперь посмотрим, на возможности продукта в действие, да и настроить весь этот комплекс не мешало бы под наши потребности. Мы ведь хотим контролировать доступ к важной информации, а также отслеживать какие неблагонадежные сотрудники решили за бочку варенья и корзину печенья разжиться конфиденциальной информацией :)

Настройка и примеры использования Safe'n'Sec Enterprise Suite

Ну что ж, начнём настройку решения. Напоминаем, что мы работаем в консоли Safe'n'Sec Admin Explorer. Во вкладке **Общие** (см. рисунок 14) можно увидеть какие области системы контролируются, исключать из наблюдения ту или иную область, удалённо выключать/перезапускать компьютер, выполнять настройку установленных клиентских модулей (см. рисунок. 15), а также осуществлять антивирусную проверку рабочей станции (см. рисунки 16, 17) и ряд других задач.

Рисунок 15: Окно настройки установленных клиентских модулей

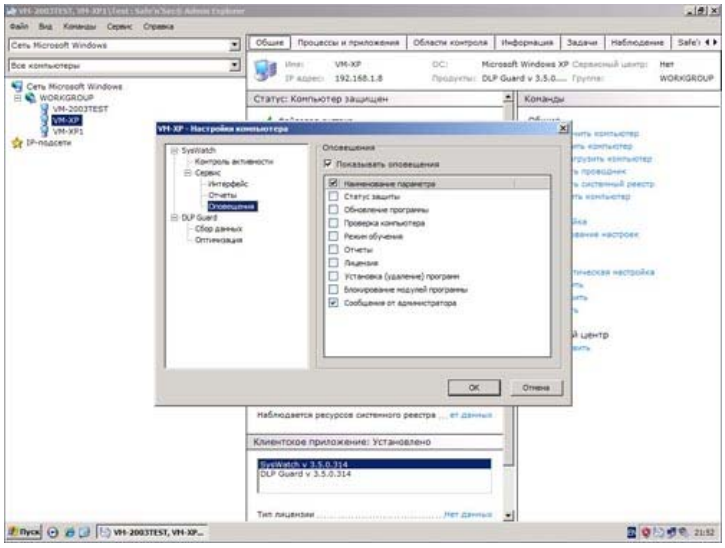


Рисунок 16: Задание области проверки антивирусным сканером

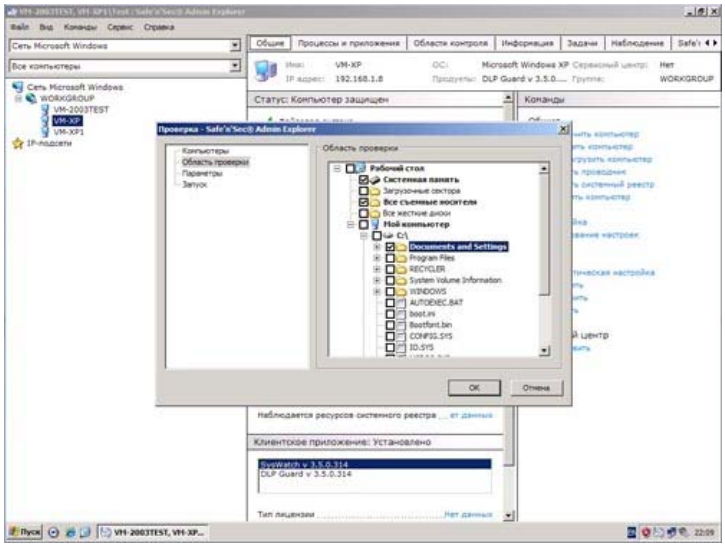
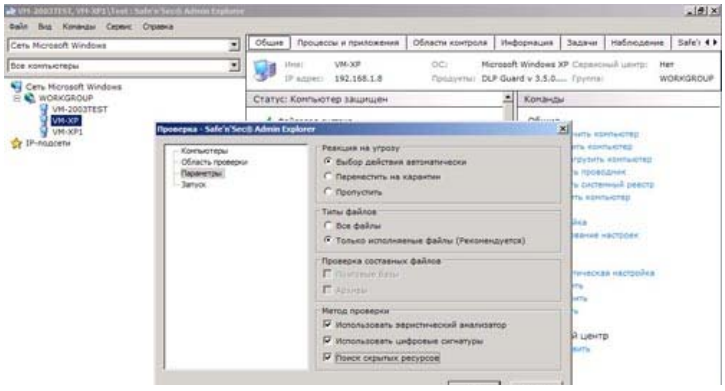
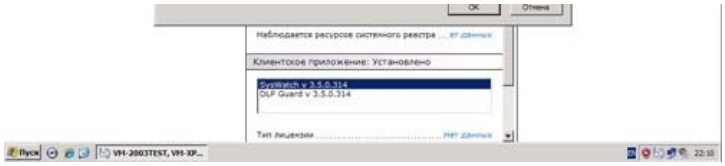


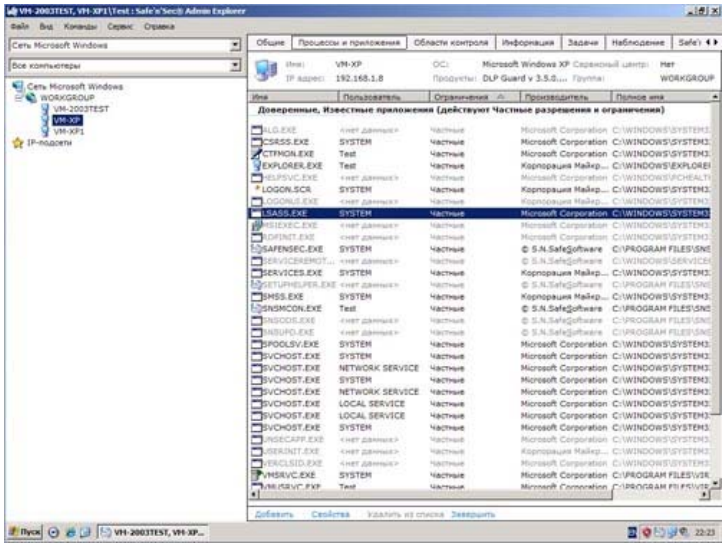
Рисунок 17: Задание параметров проверки антивирусным сканером





Во вкладке **Процессы и приложения** отображаются все запущенные и известные приложения и процессы на выбранной нами конечной точке сети. Часть из них находится в списке Доверенных. Для Доверенных и известных приложений действуют частные правила разрешений и ограничений.

Рисунок 18: Процессы и приложения, общий вид



Приложения и процессы можно удаленно завершать, просматривать их свойства, задавать частные условия выполнения и ограничения, вести историю активности. Также можно проверить запущенное приложение антивирусным сканером, добавлять/удалять приложение в/из доверенных.

Рисунок 19: Просмотр свойств запущенного приложения

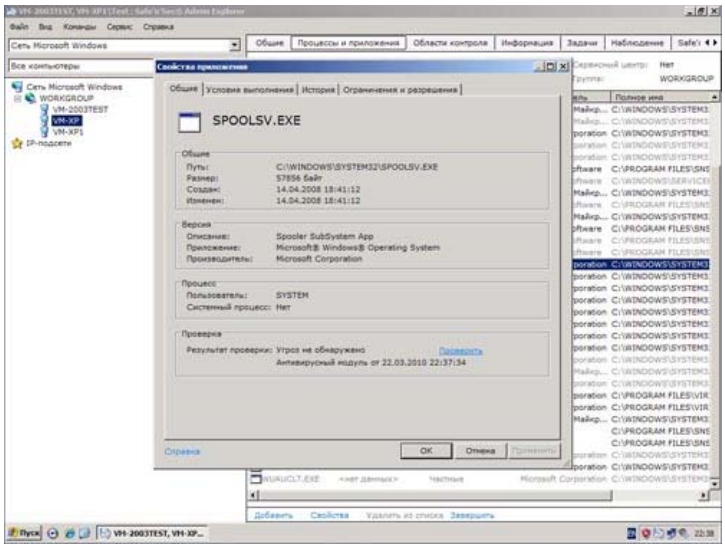
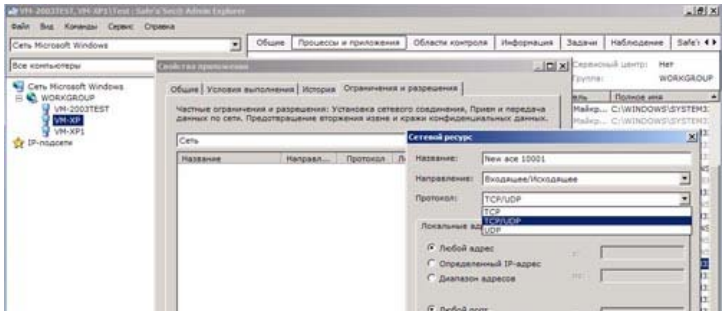


Рисунок 20: Задание частных ограничений работы приложения с сетью



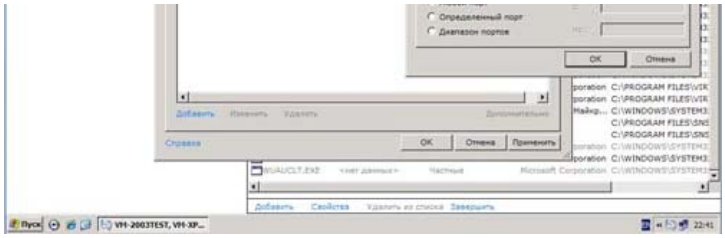
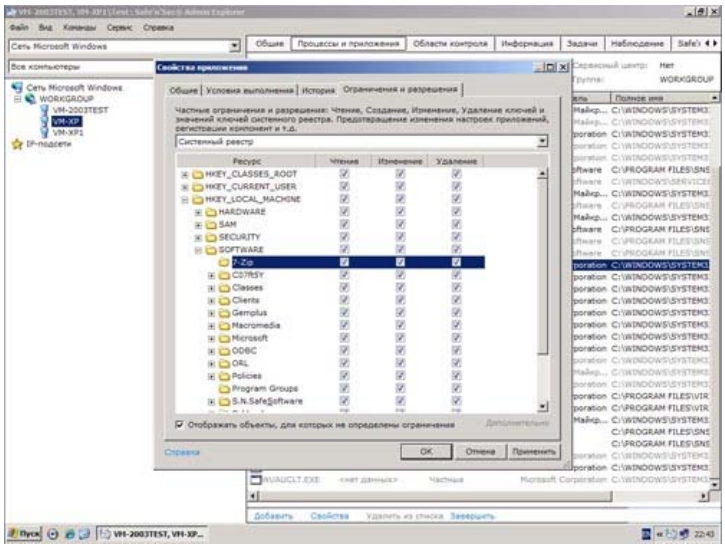


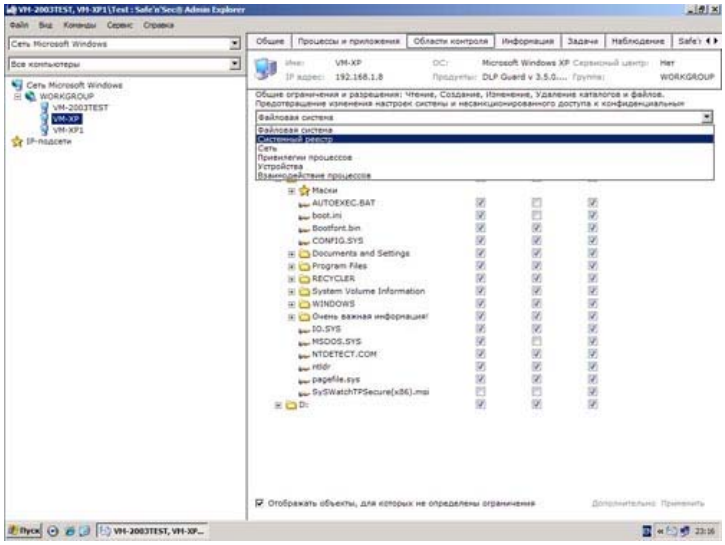
Рисунок 21: Задание частных ограничений работы приложения с реестром



Во вкладке **Области контроля** задаются общие ограничения и разрешения: чтение, изменение, удаление каталогов и файлов, ключей и ветвей системного реестра. Это даёт возможность предотвратить доступ к конфиденциальной информации, а также предотвратить несанкционированное изменение настроек системы. В том числе предусмотрена возможность блокировки работы с USB устройствами, отслеживание использования привилегий процессов основными группами пользователей, настройка работы с сетью (задание сетевых правил) и взаимодействие процессов с системой. Всё это позволяет гибко настроить доступ к наиболее важным данным и критическим областям системы.

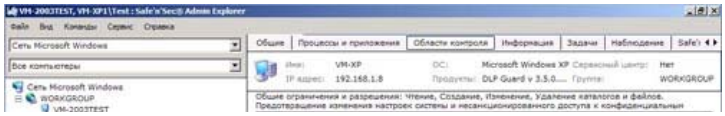
Общие правила действуют для всех приложений, которые не находятся в списке Доверенных и известных.

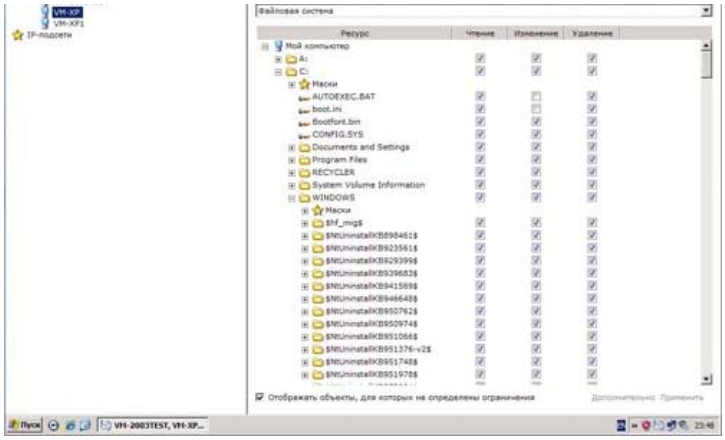
Рисунок 22: Общий вид окна Области контроля



Можно выбрать какую область контроля мы хотим просмотреть и настроить (файловая система, системный реестр, сеть, привилегии процессов, устройства, взаимодействия процессов).
Рассмотрим настройки области контроля более подробно.

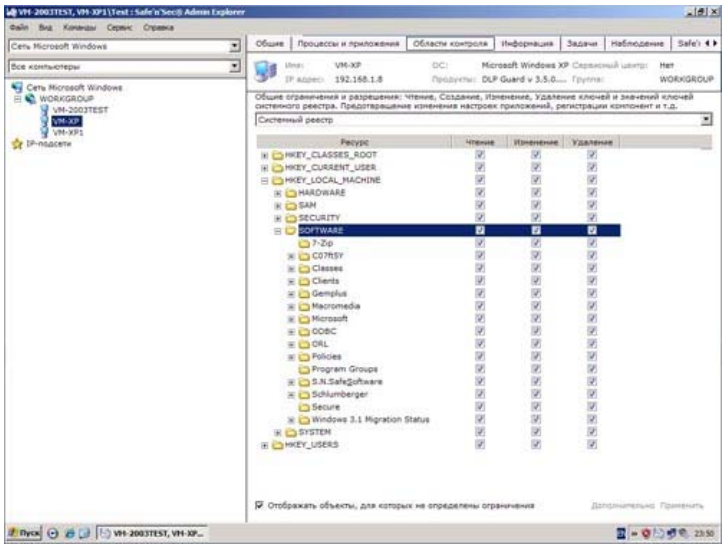
Рисунок 23: Области контроля, файловая система





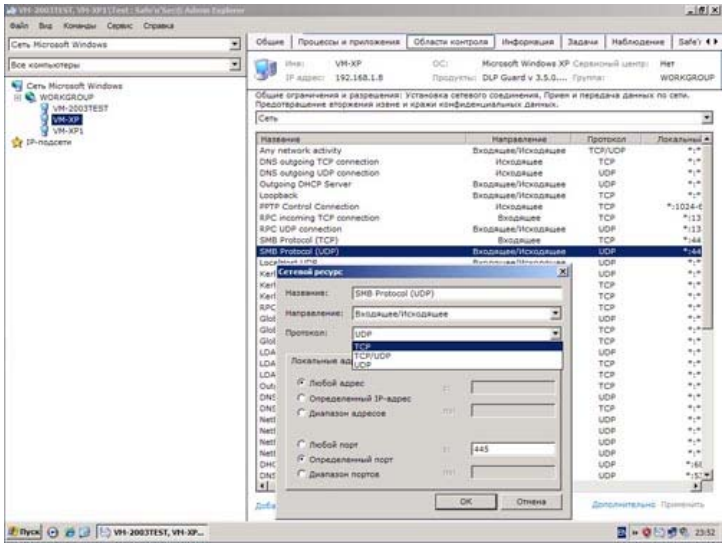
Настройка разрешений может проводиться как для одного файла, так и для каталога. Главное чётко понимать, что делаем иначе можно наломать дров.

Рисунок 24: Области контроля, системный реестр



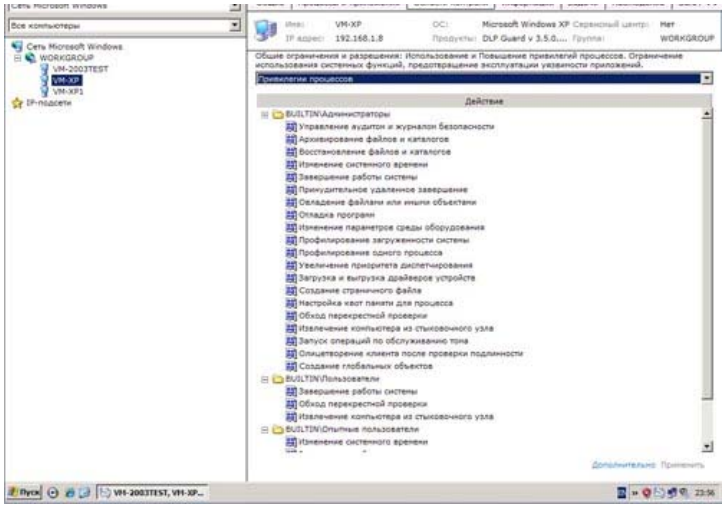
Здесь всё аналогично контролю файловой системы. Работаем внимательно и аккуратно, крайне желательно вести документирование своих действий.

Рисунок 25: Области контроля, сеть



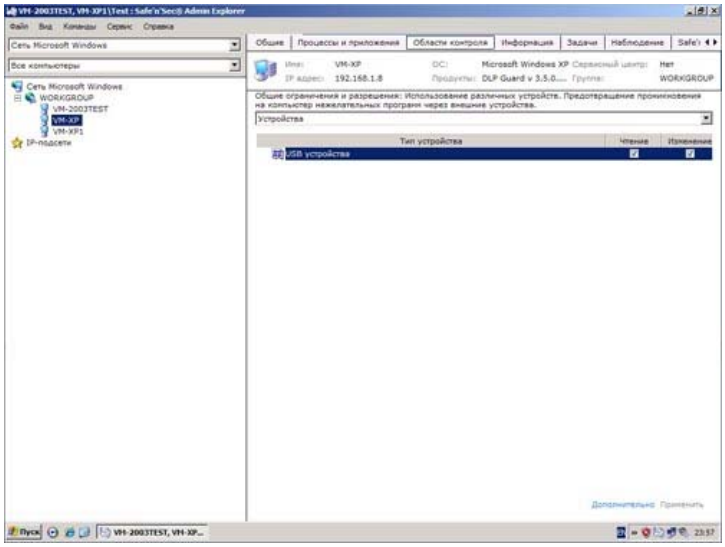
Для сети набор готовых правил обширен. Если вдруг, чего-то не хватает, то можно создавать свои собственные правила.

Рисунок 26: Области контроля, привилегии процессов



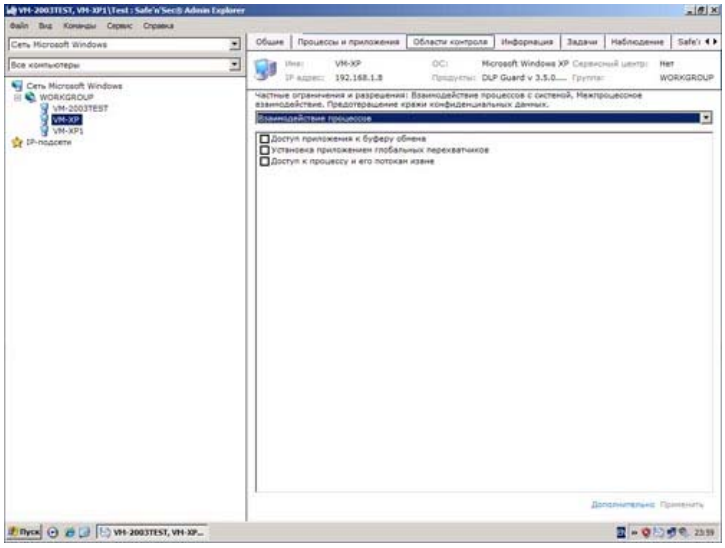
Как видим, в настройках области контроля привилегий процессов уже учтено все самое необходимое, разработчики экономят наше время.

Рисунок 27: Области контроля, устройства



В плане возможностей контроля устройств пока что выбор небогатый, но по заявлениям вендора разработка в этом направлении активно идет.

Рисунок 28: Области контроля, взаимодействие процессов



В настройке взаимодействия процессов для каждого правила можно выбрать пользователя, для которого оно будет действовать, а также период его действия (см. рисунок 29). Обратите внимание, что можно задать несколько периодов действия правила.

Рисунок 29: Выбор пользователей, на которых будет распространяться данное правило

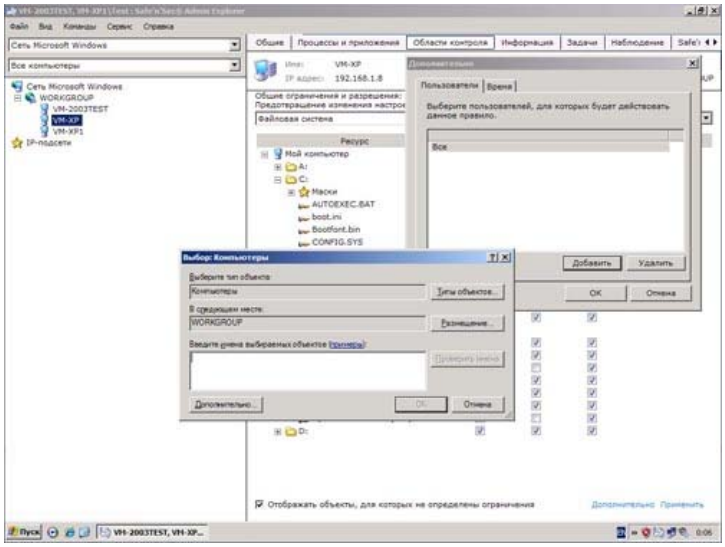
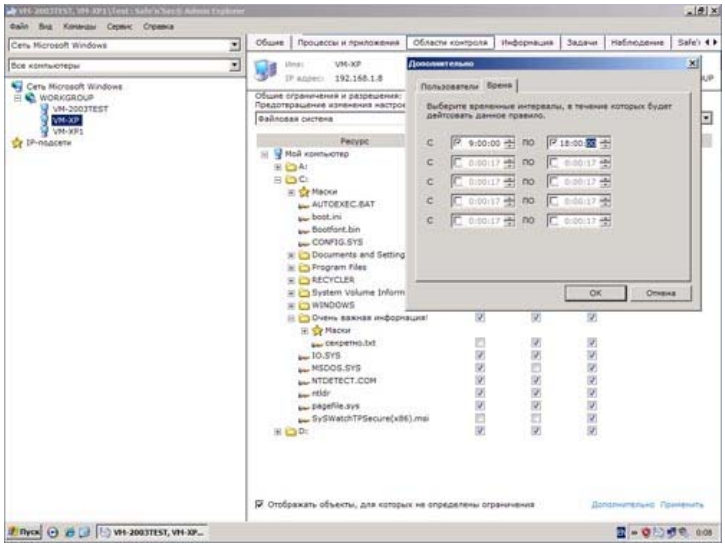


Рисунок 30: Задание периода времени для действия правила



Давайте, в качестве примера, запретим пользователям использовать USB-диски. Для этого открываем **Область контроля — Устройства** и снимаем галочки «Чтение» и «Изменение», после чего нажимаем **Применить**.

Рисунок 31: Изменение разрешений для USB-устройств

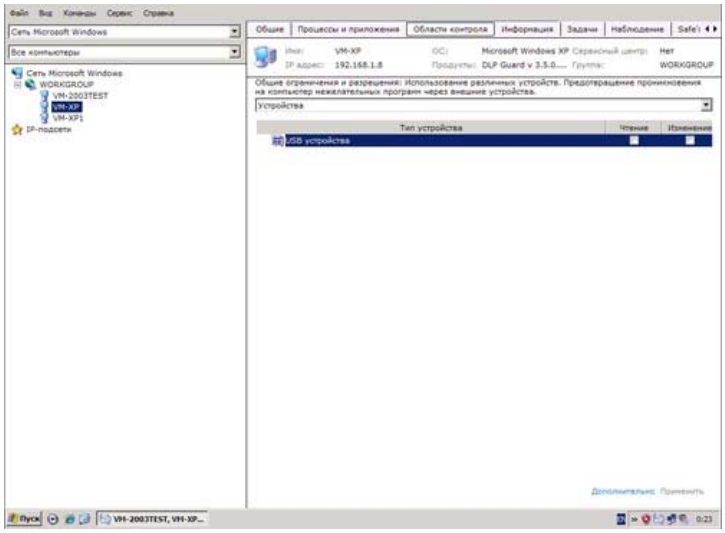
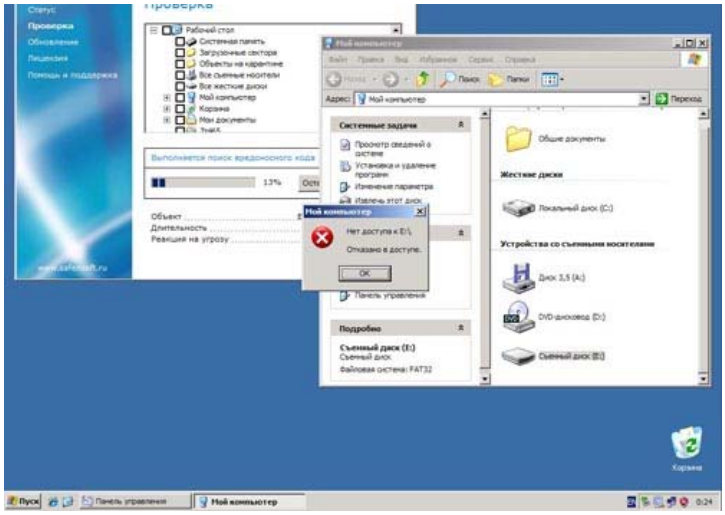


Рисунок 32: Результат действия настроенного правила для USB-устройств

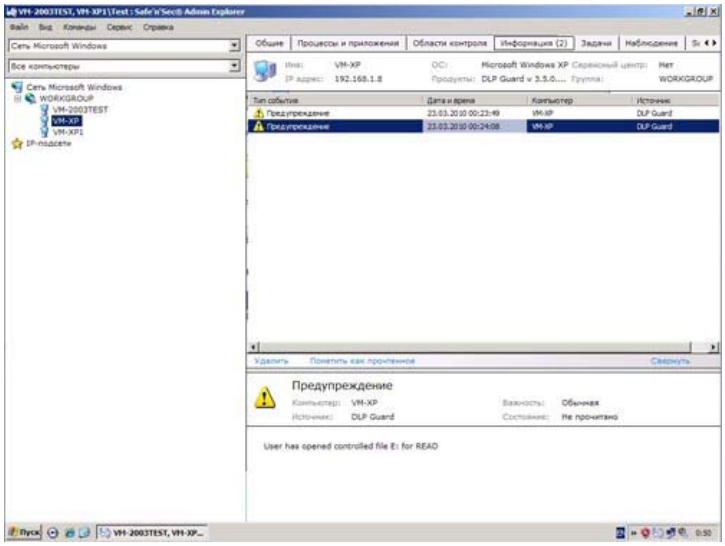


Как видим, при подключении USB-устройства запускается автоматическая проверка накопителя на наличие вредоносного кода. А вот с самим устройством мы работать не можем — отказано в доступе. Это сработало наше только что созданное правило. Теперь «слить» что-либо на флэшку не выйдет. Кстати, заодно получилось кардинальное решение проблемы Autorun-вирусов. Нет зубов - нет кариеса. Ещё один плюс к уровню защиты сети.

Аналогично действуем и для других областей контроля. Не забываем, что это общие правила, которые действуют для всех недоверенных и неизвестных приложений. Для доверенных и известных приложений существую частные ограничения, правила в которых создаются аналогично.

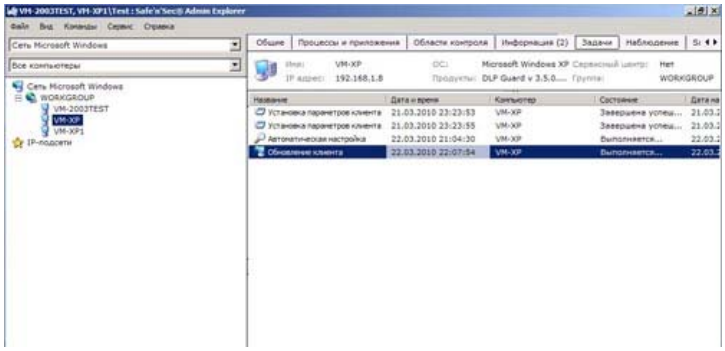
Во вкладке **Информация** отображаются сообщения и предупреждениях о различных событиях на подконтрольной точке сети. На **рисунке 33** мы видим два предупреждения сообщения о том, что сработало наше созданное выше правило — запрет работы с USB-устройствами. Пользователь попытался открыть подключенный внешний диск.

Рисунок 33: Сообщения от модуля DLP Guard - пользователь пытался открыть флэшку



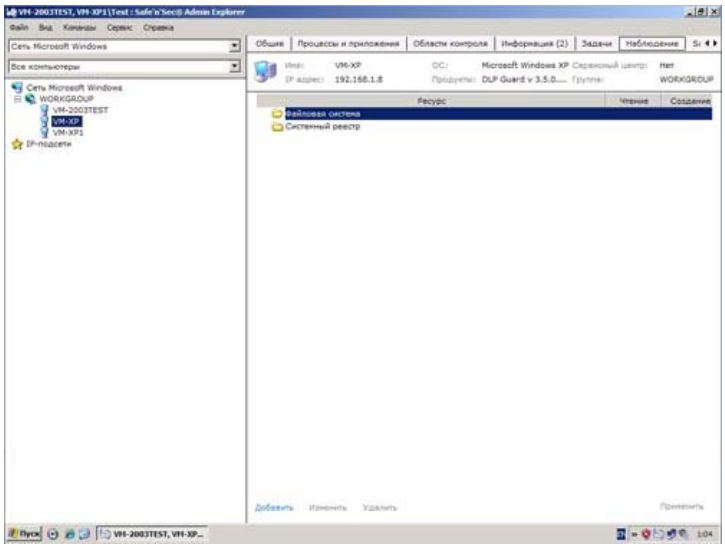
Во вкладке **Задачи** отображаются все выполненные, текущие и запланированные задания на конечной точке. Задания можно запускать, останавливать, удалять и просматривать их свойства. Отображается время начала и окончания выполнения, а также состояние выполнения (см. рисунок 34). В нашем случае видим, что выбранной точки сети ряд задач уже присутствует.

Рисунок 34: Список задач и их состояние



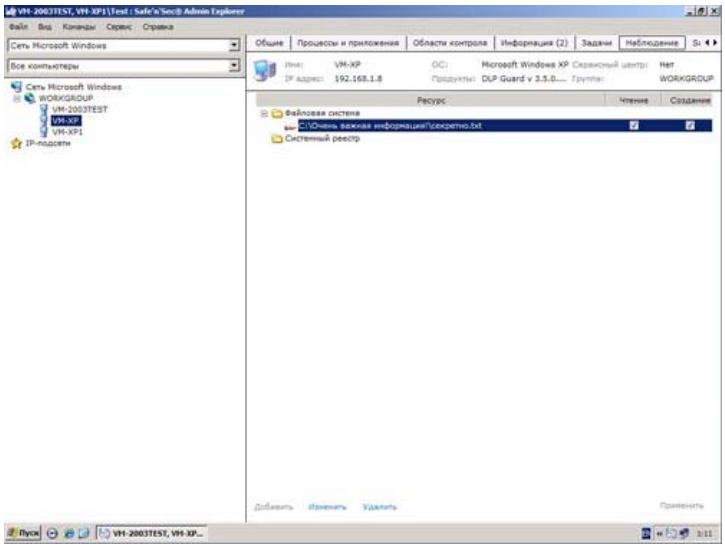
Во вкладке **Наблюдения** мы можем создавать правила слежения за объектами системного реестра и файловой системы – это очень важная функция. По-молчанию здесь нет никаких правил, их нужно создавать самостоятельно.

Рисунок 35. Окно наблюдения, правила ещё не созданы



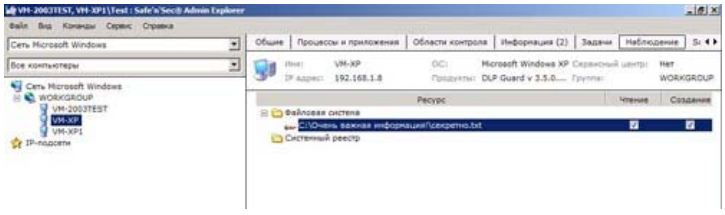
Давайте создадим пару правил для наблюдения и посмотрим на результат. Для начала, создадим правило для слежения за текстовым файлом, который находится на рабочей станции пользователя. Для этого достаточно щёлкнуть правой кнопкой мыши на разделе **Файловая система** и выполнить команду **Добавить**. В открывшемся окне выбираем объект файловой системы, за которым будем вести слежение (см. рисунок 36).

Рисунок 36: Выбираем объект для правила наблюдения



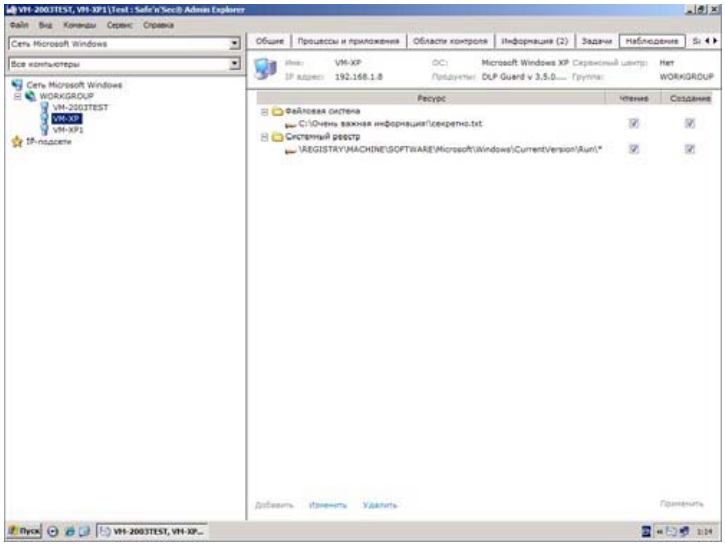
Правило создано, не забываем кликнуть по ссылке **Применить** в нижней части экрана.

Рисунок 37: Созданное правило наблюдения



Аналогично создадим правило и для системного реестра. Будем отслеживать манипуляции с одной из веток автозапуска.

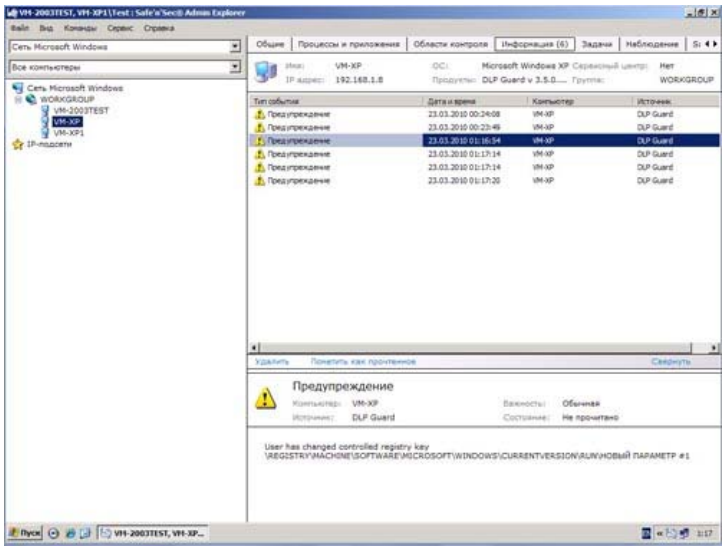
Рисунок 38: Правила для файловой системы и системного реестра готовы



Не стоит излишне увлекаться созданием правил и попытками контроля всего и вся, иначе в ворохе сообщений мы пропустим действительно важные события.

Теперь пришло время посмотреть на результат наших действий. Заходим во вкладку **Информация** и видим так новые сообщения о том, что подконтрольный файл открывался и изменялся, а в подконтрольной ветке реестра появился новый параметр. Подобным образом может быть отслежен несанкционированный доступ к конфиденциальной информации или установка вредоносной программы.

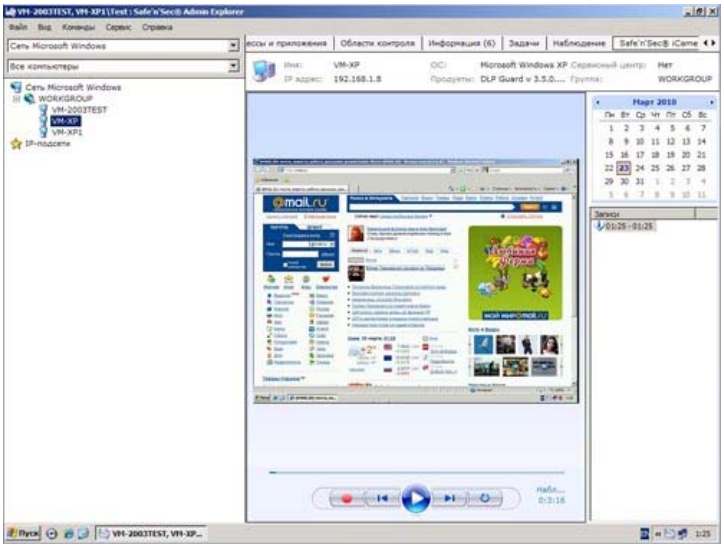
Рисунок 39: Правила наблюдения сработали



И в заключение рассмотрим очень интересную вкладку **Safe'n'Sec iCamera**. В ней мы можем вести удалённое видеонаблюдение за рабочей станцией или какой-либо другой точкой сети с возможностью записи видео-роликов. Как правило, в организациях часто уже применяются системы удалённого управления и видеонаблюдения типа Radmin или семейство VNC. Не стоит отказываться от них, если они уже развёрнуты. Они прекрасно дополнят друг друга.

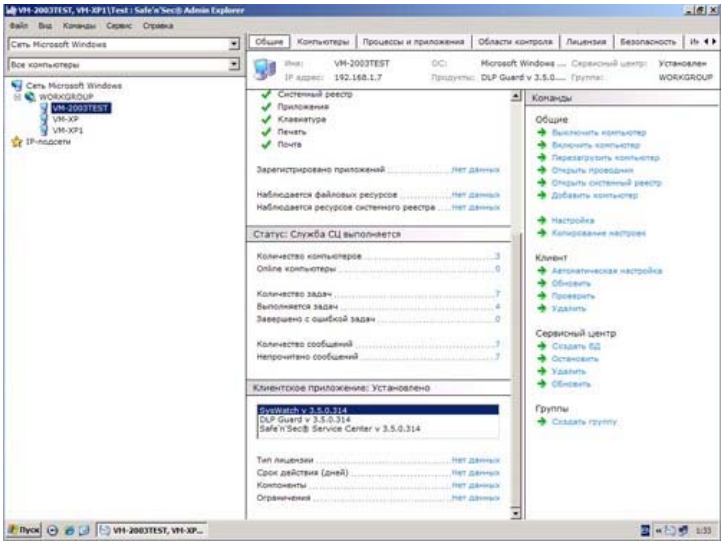
Записанные видео-фрагменты систематизируются по времени, что очень удобно для их последующего поиска и анализа, см. рисунок 40.

Рисунок 40: Записанный видео-фрагмент действий пользователя при помощи Safe'n'Sec iCamera



На сервере с установленным сервисным центром доступны дополнительные возможности в Safe'n'Sec Admin Explorer, а именно просмотр списка конечных точек сети обслуживаемых этим сервисным центром и управление лицензиями. В окнах **Информация** и **Задачи** отображаются все сообщения и задачи со всех конечных точек сети обслуживаемых этим сервисным центром.

Рисунок 41: Главной окно Safe'n'Sec Admin Explorer



Видим, что кроме установленных SysWatch и DLPGuard на данном узле есть ещё и Safe'n'Sec Service Center.

Рисунок 42: Список конечных точек сети, обслуживаемых данным сервисным центром

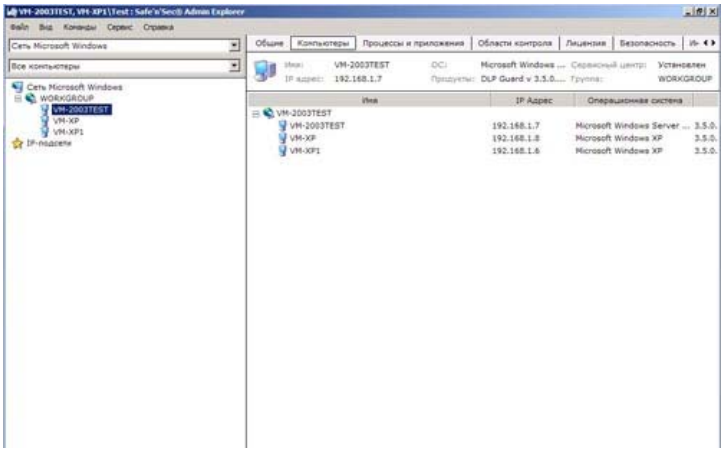


Рисунок 43: Установленные лицензии

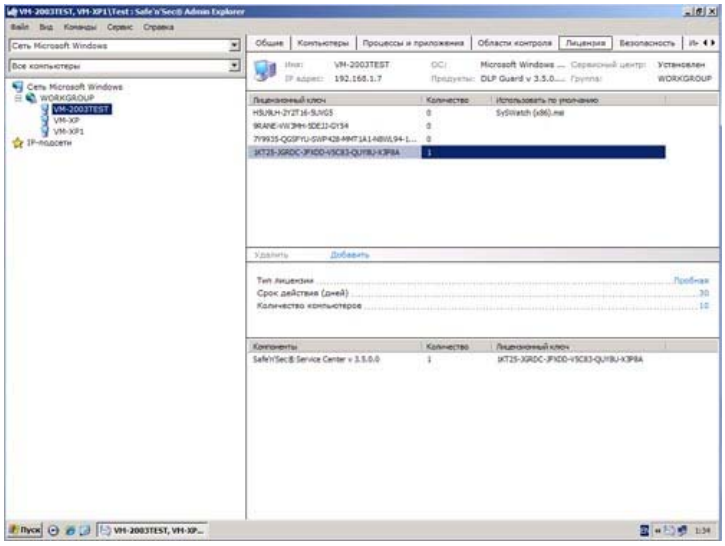
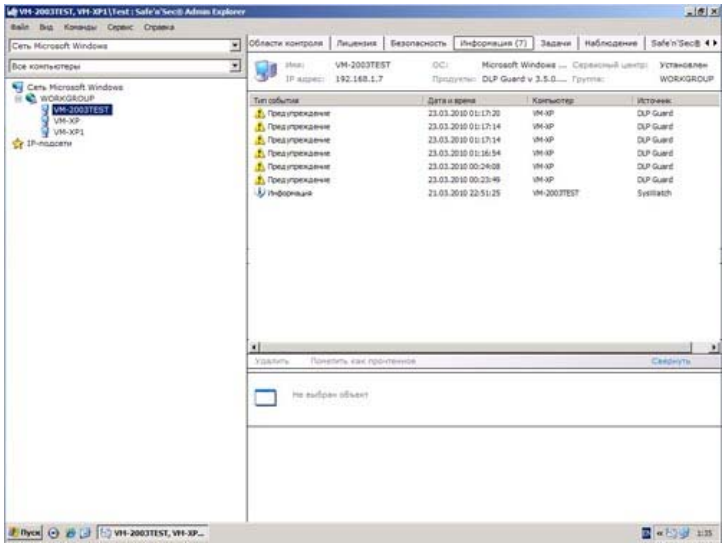
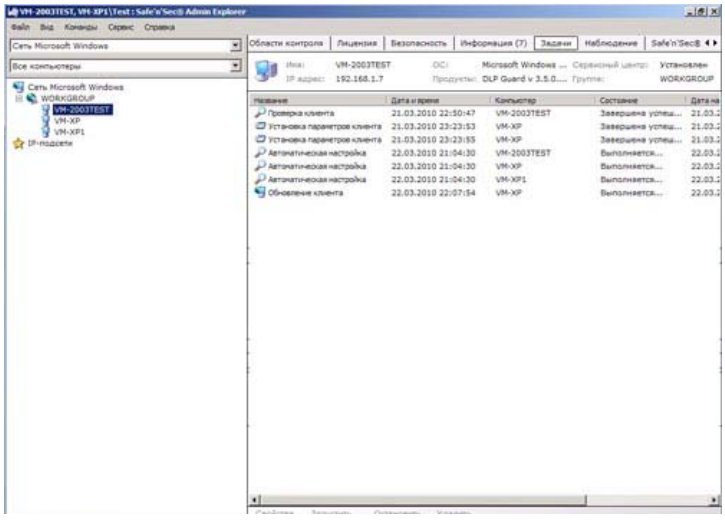


Рисунок 44: Список сообщений всех конечных точек сети, обслуживаемых данным сервисным центром



Централизованный сбор и отображение всех событий со всех конечных точек сети избавляет офицера безопасности от необходимости просмотра каждой конечной точки сети в отдельности.

Рисунок 45: Список задач всех конечных точек сети обслуживаемых данным сервисным центром



На этом мы заканчиваем обзор основных возможностей Safe'n'Sec Enterprise Suite

Выводы

Safe'n'Sec Enterprise Suite является мощным продуктом для обеспечения комплексной безопасности корпоративных сетей, контроля и разграничения доступа к конфиденциальной информации, основанным на самых современных технологиях.

К плюсам Safe'n'Sec Enterprise Suite стоит отнести обширный функционал по контролю и защите информации от внешних и внутренних угроз, достаточную простоту установки и лёгкость в работе, применение передовых инновационных технологий в работе продукта, хорошая совместимость с антивирусным программным обеспечением, а также низкие системные требования для клиентской части продукта.

Использование технологии "белых списков" прекрасно подходит для защиты типовых рабочих станций, платёжных терминалов и банкоматов. Так как программное обеспечение и оборудования там изменяется крайне редко, то блокирование всех недоверенных приложений и действий является наиболее логичным и эффективным подходом с точки зрения безопасности.

Стоит отметить встроенный клиент видеонаблюдения **Safe'n'Sec iCamera**, который предоставляет возможность записи видео-фрагментов с рабочего стола удаленной конечной точки сети. Это дает дополнительные возможности по сбору доказательной базы для службы безопасности.

К минусам продукта, как было уже сказано в начале обзора, можно отнести отсутствие возможности мониторинга сообщений интернет-мессенджеров (очень нужная функция, с учётом того, что они вошли прочно даже в рабочую жизнь), работы с беспроводными сетями и контроль над посещением интернет-ресурсов сотрудниками предприятия. Но это скорее не минусы, а пожелания для дальнейшего развития функционала продукта с нашей стороны, так как в большинстве случаев на фирмах уже используются системы контроля доступа сотрудников к сети Интернет.

Также в Safe'n'Sec Enterprise Suite явно не хватает возможности отслеживания изменений содержимого конфиденциальных документов, на наш взгляд, для продуктов такого класса она просто необходима. Также разработчикам стоит ввести в продукт возможность отправки уведомлений и отчётов не только по e-mail, но и по другим каналам, например, по ICQ, Jabber или по SMS.

Отдельно стоит отметить проблемы технического характера: были замечены сбои в работе сервисных компонентов продукта, проведённые изменения настроек не всегда сохранялись.

Тем не менее, наша **субъективная оценка решения Safe'n'Sec Enterprise Suite - 8 из 10 баллов**.

Продукт получает награду Approved by Anti-Malware.ru

Список рекомендуемых нами продуктов »

Автор обзора:
Алексей Баранов

Средняя оценка: 4.2 (голосов: 15)