

# Комплексная защита информационных ресурсов

# Safe'n'Sec + Teller Edition.

- Технологии
- Назначение и компоненты системы
- Принцип работы
- Возможности
- Техническая поддержка

# Технология проактивной защиты

D.I.C. - Dynamic Integrity Control - контроль запуска процессов позволяет предотвратить скрытую установку или выполнение приложений. (Защищает все исполняемые приложения системы благодаря обнаружению попыток несанкционированного запуска процессов и блокировки их запуска до того, как процесс может нанести вред системе).

D.S.E. - Dynamic Sandbox Execution - изолированная среда для запуска потенциально опасного ПО.

обеспечивает контроль системных привилегий для блокировки вредоносных действий.

D.R.C. - Dynamic Resource Control - контроль файловой активности процессов и попыток изменения системного реестра, доступа к внешним устройствам, сетевым ресурсам

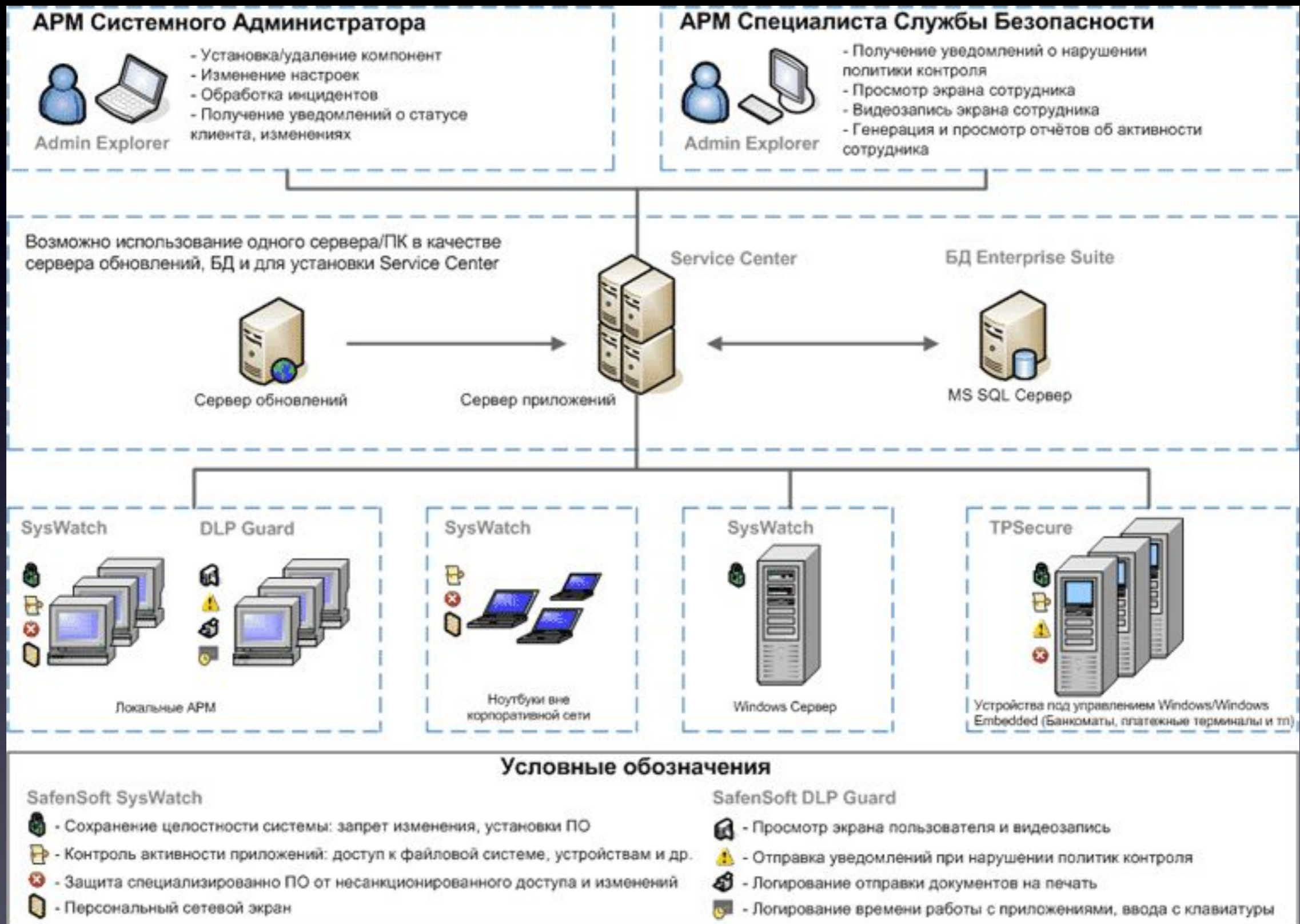
# Единая консоль администрирования Admin Explorer

уведомления и оперативное реагирование на инциденты ИБ, происходящие на удалённых клиентских рабочих станциях

## Service Center

сбор информации от клиентских рабочих станций и отправка им различных запросов

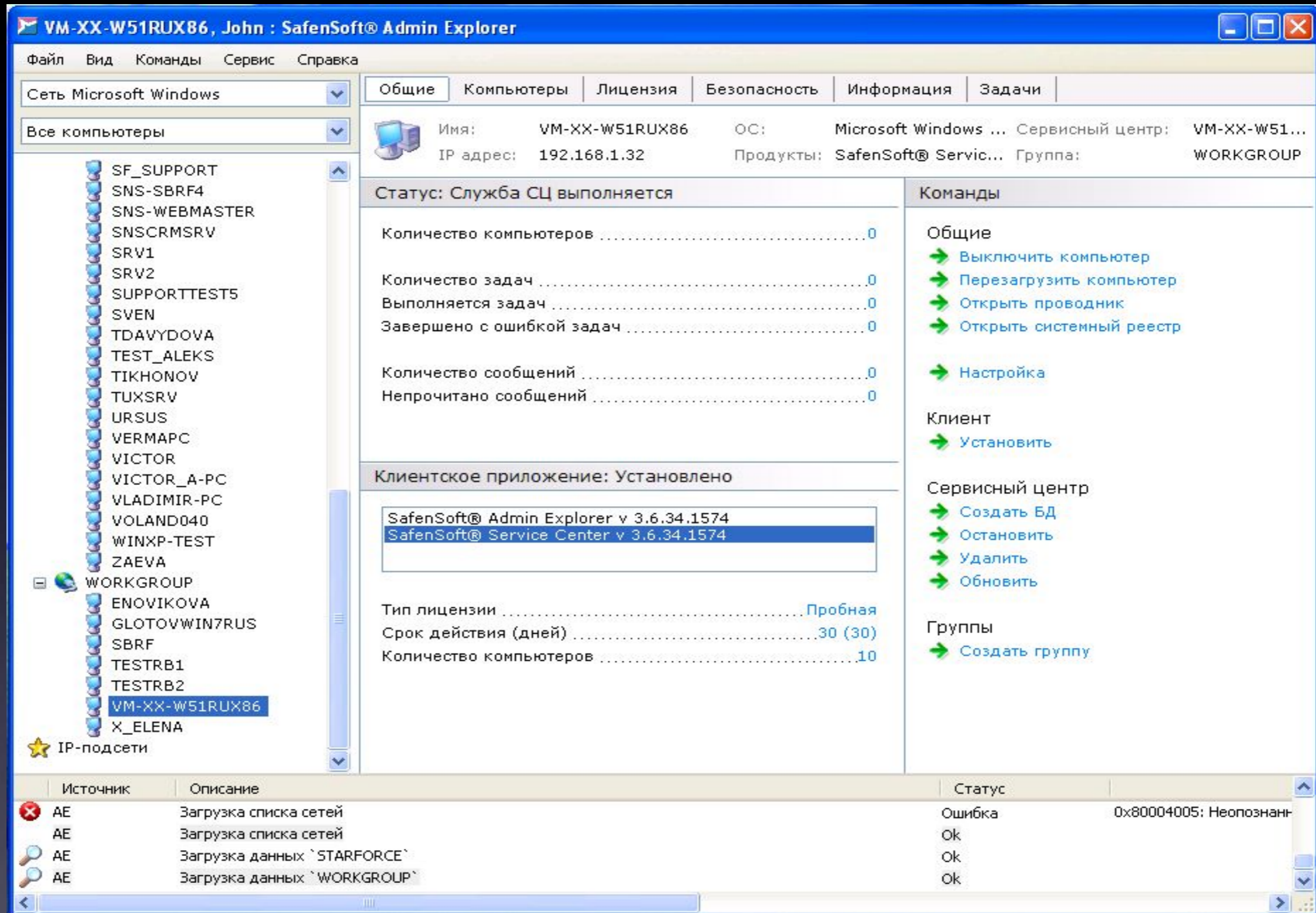
# Централизованное управление



# Возможности средств централизованного управления

- удаленная установка и удаление клиентских приложений SafenSoft;
- создание индивидуальных пакетов установки, включая продукты других производителей;
- синхронизация с Active Directory;
- централизованная настройка параметров работы клиентских приложений путем создания групповых политик;
- централизованное обновление клиентских приложений;
- проверка и назначение прав на выполнение административных задач;
- принятие решения по инцидентам на клиентских рабочих станциях;
- получение уведомлений о состоянии защиты рабочих станций
- получение уведомлений о нарушении политики безопасности на рабочих станциях сотрудников

# Доступный Интерфейс



**VM-XX-W51RUX86, John : SafenSoft® Admin Explorer**

Файл Вид Команды Сервис Справка

Сеть Microsoft Windows

Все компьютеры

- SF\_SUPPORT
- SNS-SBRF4
- SNS-WEBMASTER
- SNSCRMSRV
- SRV1
- SRV2
- SUPPORTTEST5
- SVEN
- TDAVDOVA
- TEST\_ALEKS
- TIKHONOV
- TUXSRV
- URSUS
- VERMAPC
- VICTOR
- VICTOR\_A-PC
- VLADIMIR-PC
- VOLAND040
- WINXP-TEST
- ZAEVA
- WORKGROUP
- ENOVIKOVA
- GLOTOVWIN7RUS
- SBRF
- TESTRB1
- TESTRB2
- VM-XX-W51RUX86**
- X\_ELENA

★ IP-подсети

**Общие** | Компьютеры | Лицензия | Безопасность | Информация | Задачи

Имя: VM-XX-W51RUX86    ОС: Microsoft Windows ...    Сервисный центр: VM-XX-W51...  
 IP адрес: 192.168.1.32    Продукты: SafenSoft® Servic...    Группа: WORKGROUP

**Статус: Служба СЦ выполняется**

Количество компьютеров	0
Количество задач	0
Выполняется задач	0
Завершено с ошибкой задач	0
Количество сообщений	0
Непрочитано сообщений	0

**Команды**

**Общие**

- ➔ Выключить компьютер
- ➔ Перезагрузить компьютер
- ➔ Открыть проводник
- ➔ Открыть системный реестр
- ➔ Настройка

**Клиент**

- ➔ Установить

**Сервисный центр**

- ➔ Создать БД
- ➔ Остановить
- ➔ Удалить
- ➔ Обновить

**Группы**

- ➔ Создать группу

**Клиентское приложение: Установлено**

SafenSoft® Admin Explorer v 3.6.34.1574
SafenSoft® Service Center v 3.6.34.1574

Тип лицензии ..... Пробная  
 Срок действия (дней) ..... 30 (30)  
 Количество компьютеров ..... 10

Источник	Описание	Статус	
AE	Загрузка списка сетей	Ошибка	0x80004005: Неопознанн
AE	Загрузка списка сетей	Ok	
AE	Загрузка данных `STARFORCE`	Ok	
AE	Загрузка данных `WORKGROUP`	Ok	

# Возможности Safe'n'Sec + Teller Edition.



- 1 Сохранение целостности системы
  - 1 Блокировка запуска неизвестных (или модифицированных) процессов, приложений и библиотек
  - 2 Правила доступа к объектам файловой системы и системного реестра для определенных приложений и групп приложений
- 2 Проверка контроля сетевой активности пользователей (персональный межсетевой экран)
- 3 Проверка защиты от несанкционированного использования USB накопителей и других устройств (CD/DVD и LPT и COM портов).
- 4 Проверка на вирусы (опционально)
- 5 Мониторинг и логирование действий сотрудников и работы приложений , просмотр экрана ПК выбранного сотрудника, контроль за набором на клавиатуре.....
- 6 Самозащита от удаления и защита от изменения настроек



# Комплексная защита информационных ресурсов

1. Защита систем управления от несанкционированного изменения данных и программного кода
  1. Защита АРМов операторов от
    1. Изменения ПО, несанкционированного копирования данных
  2. Защита контроллеров и узлов АСУ ТП от несанкционированного изменения настроек и программного кода

# Что дает использование SysWatch + Teller Edition.

## Директору информационной службы

- Оценка качества работы информационной системы

## Офицеру службы информационной безопасности

- Фиксация всех нарушений требований защиты информации
- Статистика работы пользователей с приложениями
- Предотвращение утечек и потерь информации

## Главный Системный Администратор

- Контроль за действиями системных администраторов локальных офисов и подразделений
- Контроль за внесением изменений в информационную систему разработчиками

## Разработчик приложений

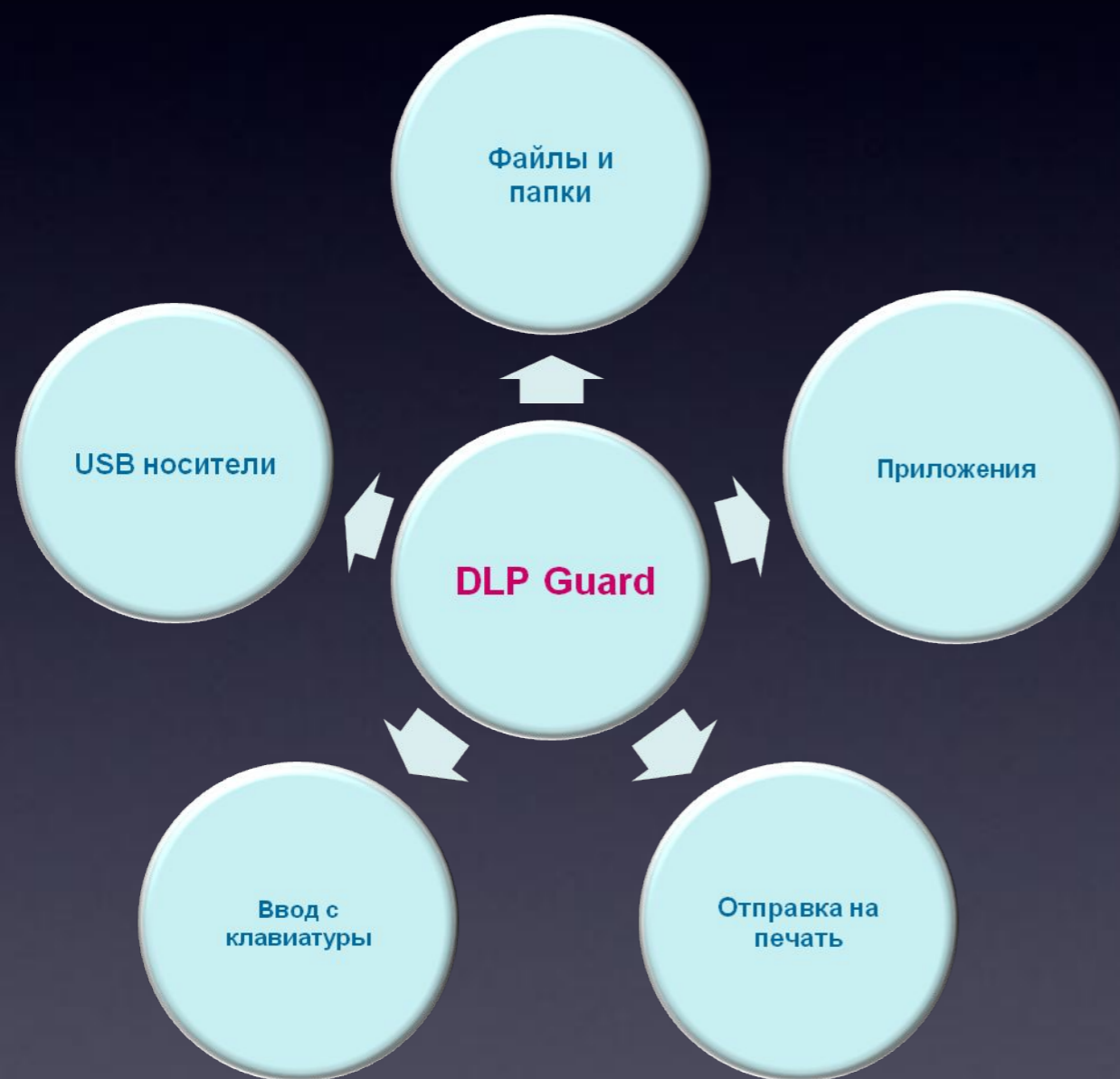
- Снижение трудоемкости разработки новых приложений, путем использования функционала SysWatch ES для выполнения требований по безопасности и защите данных

# SafenSoft DLP Guard

Контроль персонала и защита от утечек  
информации

# SafenSoft DLP Guard

SafenSoft DLP Guard осуществляет мониторинг и логирование деятельности персонала на рабочих станциях в корпоративной сети компании с возможностью отправки уведомлений об инциденте и создания отчётов.



- Централизованное администрирование и получение уведомлений об инцидентах
- Предотвращение утечек информации
- Контроль эффективности использования рабочего времени

# Возможности DLP Guard

- ✓ Мониторинг использования файловых ресурсов компании
- ✓ Мониторинг использования внешних USB-накопителей
- ✓ Просмотр экрана пользователя в режиме реального времени
- ✓ Видеозапись и воспроизведение записи экрана пользователя
- ✓ Запись текста, введенного с клавиатуры для любого приложения
- ✓ Ведение учета отправленных сотрудником e-mail
- ✓ Мониторинг файлов, отправленных для печати на принтер
- ✓ Мониторинг системного реестра
- ✓ Теневое копирование данных
- ✓ Учет рабочего времени сотрудника (общего и с каждым приложением)
- ✓ Учет используемых приложений
- ✓ Централизованное хранение данных мониторинга
- ✓ Незаметность клиентского модуля на компьютере сотрудника
- ✓ Получение уведомлений в консоль администрирования или на e-mail при нарушении политики безопасности

# Возможности DLP Guard

✓ Консоль администрирования Admin Explorer

The screenshot displays the Admin Explorer interface for a network named 'Safe'n'Sec Enterprise'. The left sidebar shows a tree view with computers SNSTESTXP1, SNSTESTXP55, and SNSTESTXP66. The main window is titled 'SNSTESTXP1, STARFORCE\sns\_stest : Safe'n'Sec@ Admin Explorer' and has a menu bar with 'Файл', 'Вид', 'Команды', 'Сервис', and 'Справка'. The main area is divided into several sections:

- Общие (General):** Displays system information for SNSTESTXP66, including the OS (Microsoft Windows), IP address (192.168.1.131), and the installed product (DLP Guard v 3.5.0.208).
- Статус: Ведется наблюдение (Status: Monitoring is in progress):** A list of monitored resources with green checkmarks:
  - Файловая система (File system)
  - Системный реестр (System registry)
  - Приложения (Applications)
  - Клавиатура (Keyboard)
  - Печать (Printing)
  - Почта (Mail)
- Зарегистрировано приложений (Registered applications):** Нет данных (No data).
- Наблюдается файловых ресурсов (Monitored file resources):** 1.
- Наблюдается ресурсов системного реестра (Monitored system registry resources):** 1.
- Клиентское приложение: Установлено (Client application: Installed):** DLP Guard v 3.5.0.208.
- Тип лицензии (License type):** Нет данных (No data).
- Срок действия (дней) (Validity period (days)):** Нет данных (No data).
- Компоненты (Components):** Нет данных (No data).
- Ограничения (Restrictions):** Нет данных (No data).
- Команды (Commands):** A list of actions available for the computer:
  - Общие (General): Выключить компьютер (Shut down computer), Включить компьютер (Turn on computer), Перезагрузить компьютер (Restart computer), Открыть проводник (Open Explorer), Открыть системный реестр (Open registry), Добавить компьютер (Add computer).
  - Настройка (Settings): Настройка (Settings).
  - Клиент (Client): Установить (Install), Удалить (Uninstall).
  - Сервисный центр (Service center): Установить (Install).
  - Группы (Groups): Переместить компьютеры (Move computers).

# Возможности DLP Guard

✓ Просмотр и запись экрана пользователя в режиме реального времени

The screenshot displays the 'Safe'n'Sec@ Admin Explorer' interface. The main window shows a remote session of a Windows XP desktop. The desktop contains a 'Solitaire' game window, a 'Calculator' window, and a 'My Computer' window. The taskbar at the bottom of the remote session shows the Start button, several icons, and the system tray with the time '2:31 PM'. The interface also features a navigation pane on the left with a tree view showing the network structure, including 'Сеть Safe'n'Sec Enterprise', 'AE-SC-SQL', and 'SYSWATCH-DLP12'. A right-hand pane displays system information for the remote session, including the name 'SYSWATCH-DLP12', IP address '192.168.0.197', and OS 'Microsoft Windows XP'. A calendar for February 2011 is visible in the top right corner. At the bottom of the interface, there is a control bar with playback buttons (stop, previous, play, next, refresh) and a timer showing 'Набл... 0:1:39'.

# Возможности DLP Guard

✓ Получение уведомлений в консоль администрирования

The screenshot displays the Admin Explorer interface for a network named 'Safe'n'Sec Enterprise'. The left pane shows a tree view with 'AE-SC-SQL' expanded to show the computer 'SYSWATCH-DLP12'. The main pane shows the 'Information (17)' tab for this computer, displaying system details like OS (Microsoft Windows XP) and IP address (192.168.0.197). Below this is a table of events, with the most recent one selected and expanded in the bottom pane.

Тип события	Дата и время	Компьютер	Источник
Предупреждение	03.02.2011 14:40:50	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:48	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:44	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:39	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:39	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:33	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:40:33	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:07	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:08	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:12	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:21	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:21	SYSWATCH-DLP12	DLP Guard
Предупреждение	03.02.2011 14:41:21	SYSWATCH-DLP12	DLP Guard

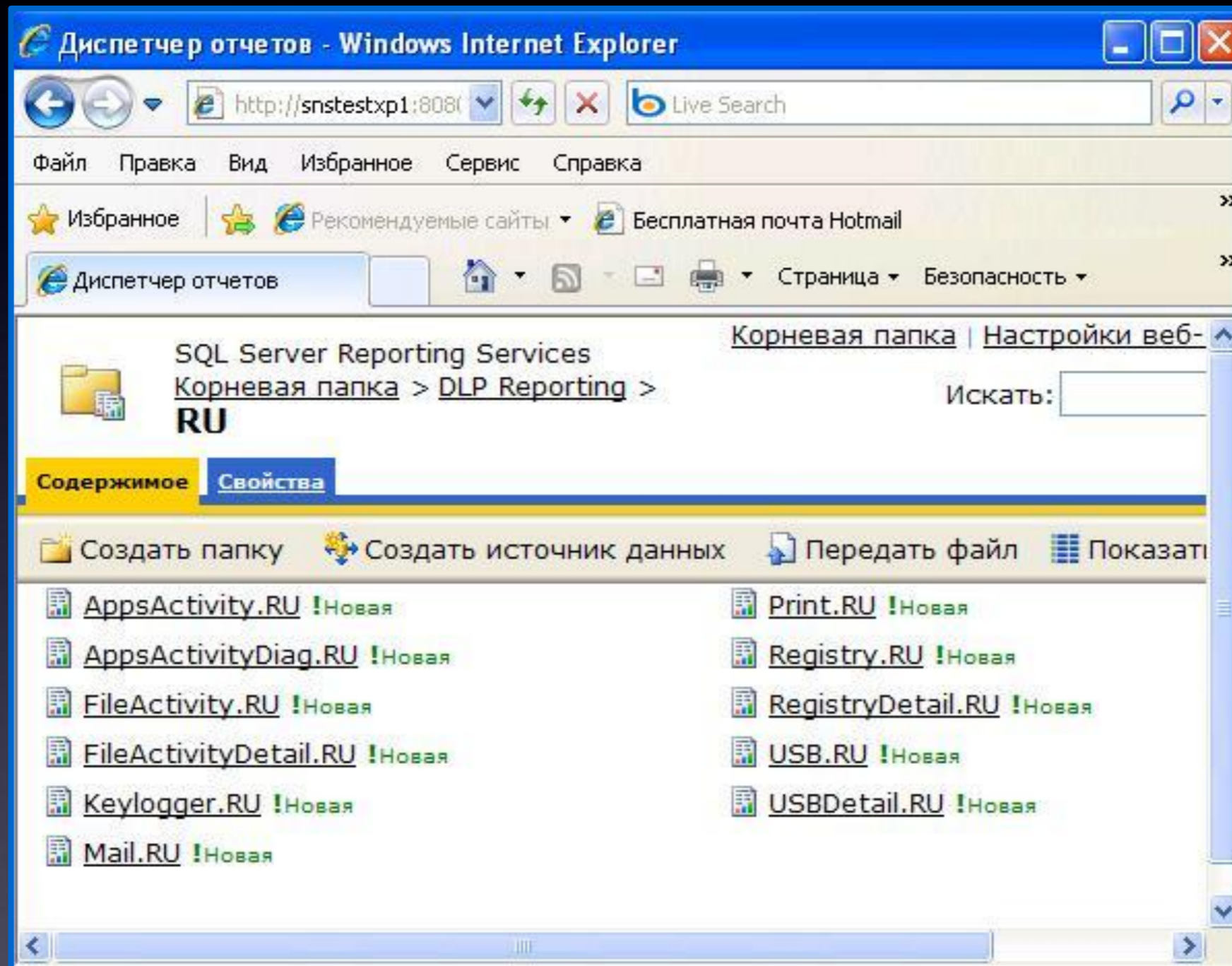
**Предупреждение**  
Компьютер: SYSWATCH-DLP12      Важность: Обычная  
Источник: DLP Guard                      Состояние: Не прочитано

User has changed controlled file C:\TEST\NEW SECRET.TXT



# Возможности DLP Guard

- ✓ Централизованное хранение данных мониторинга и создание отчётов



# Соблюдение требований

SafenSoft DLP Guard позволит дополнить защиту системы обработки персональных данных в соответствии с требованиями законодательства и регулирующих документов в части защиты конфиденциальной информации.

- ❑ Полностью соответствуют требованиям №152-ФЗ («О персональных данных»).
- ❑ Сертификация ФСТЭК России на соответствие 4-му уровню контроля на отсутствие НДВ\*.
- ❑ В соответствии с Приказом ФСТЭК №58 от 05.02.2011 может применяться для защиты информационных систем обработки персональных данных (ИСПДн) до класса К1 включительно.

\* Сертификация текущей версии на заключительном этапе.

# Техническая поддержка

- Выезд специалиста в случаи инцидента
- Консультации по внедрению
- Внедрение
- Тест на совместимость ПО
- Обучение сотрудников
- Центральный офис Москва

# Награды и сертификаты

2011



2010



2009





# SafenSoft

Спасибо за внимание.  
Вопросы?

Телефон: (495) 967-14-51  
E-mail: [sales@safensoft.ru](mailto:sales@safensoft.ru)  
Сайт компании: [www.safensoft.ru](http://www.safensoft.ru)

