УДК 621.391

С.Г. Самохвалова, Е.Ф. Новоселова

ИНФОРМАЦИОННАЯ СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА КОМПЬЮТЕРОВ ФБУ «ЗЕМЕЛЬНАЯ КАДАСТРОВАЯ ПАЛАТА»

В статье рассмотрены основные методы информационной безопасности на процедурном уровне и программы реализации этих методов.

The article presents the main methods of information security at the procedural level and a program implementing these methods.

Современный мир все больше зависит от систем, построенных на вычислительной технике. С каждым днем увеличивается объем информации, обрабатываемой компьютерными устройствами, информационные системы становятся более сложными, а вычислительные устройства – более мощными.

Поэтому немаловажную роль в информационных системах играет обеспечение информационной безопасности. Информационная безопасность – одна из важнейших составляющих работы любой организации. Безопасность должна обеспечиваться как на техническом и административном, так и на процедурном уровне [3].

Зачастую именно «человеческий фактор» – самый уязвимый элемент в информационной безопасности. Чтобы контролировать источник утечки информации и обеспечивать информационную безопасность учреждения, существуют различные методы, одним из которых является политика протоколирования и аудита.

Реализация политики протоколирования и аудита решает следующие задачи: обеспечение подотчетности пользователей и администраторов; обеспечение возможности реконструкции последовательности событий; обнаружение попыток нарушений информационной безопасности; предоставление информации для выявления и анализа проблем [1].

На сегодняшний день на основе политики протоколирования и аудита разработаны программы и комплексы программ сетевого мониторинга и контроля работы сотрудников в информационной системе. Данные программы в большей или меньшей степени решают следующие основные задачи: обеспечение информационной безопасности системы, организация более эффективного управления компьютерной техникой.

Главными объектами ежедневного мониторинга таких программ являются: имя текущего пользователя компьютера, время начала и окончания работы, список всех запущенных программ [2].

Мониторинг собранной информации позволяет анализировать накопленную информацию в режиме реального времени или периодически.

Немаловажную помощь системным администраторам оказывают также функции мониторинга основных характеристик компьютеров, находящихся в локальной сети. К характеристикам компьютера можно, например, отнести: имя компьютера/ ip-адрес, ОС, использованная оперативная память, процессор, свободное место на диске.

Следует отметить, что функции сбора характеристик компьютера («программы-сканеры») и функции контроля деятельности персонала («программы-шпионы») программисты часто выделяют в отдельные программы и не используют их совместно.

Анализ российского и зарубежного опыта в сфере разработки и использования программ мониторинга компьютеров позволил сделать вывод, что основными недостатками данных программ являются: цена; закрытый исходный код; отсутствие функций «программ - сканеров».

Исходя из этого было принято решение разработать свою собственную информационную систему удаленного мониторинга компьютеров.

Целью создания системы являются организация более эффективного управления компьютерной техникой, а также обеспечение информационной безопасности учреждения «Земельная кадастровая палата», путем постоянного мониторинга компьютеров-клиентов в локальной сети.

Практической значимостью программы является более рациональная организация работы сотрудников учреждения, исходя из собранных в результате мониторинга статистических данных.

Для создания централизованной системы мониторинга компьютеров на первом этапе была разработана архитектура системы. Следует отметить, что выбор был сделан в пользу двухуровневой архитектуры клиент-сервер.

Сервер приложения и баз данных занимается накоплением и обработкой данных, а приложение-клиент нацелено на сбор всех необходимых параметров с компьютеров-клиентов и создание максимально дружественного интерфейса для управления настройками и просмотра отчетов системным администратором.

На следующем этапе были выделены основные компоненты системы, представленные на рис. 1.

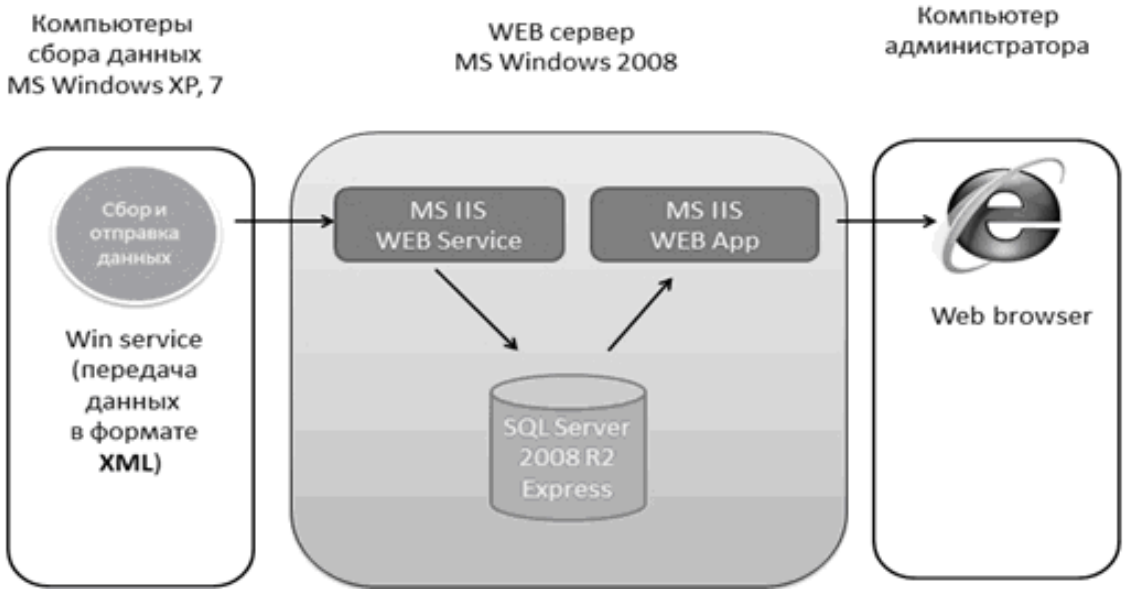

Рис. 1. Компоненты системы.

Принцип функционирования информационной системы мониторинга компьютеров следующий:

клиент-программа, установленная на рабочей машине пользователя, по заданному интервалу отправляет определённое число параметров в виде xml-сообщения на сервер;

сервер реализован как:

web-сервер – принимает информацию от клиента в виде xml-сообщения (инициатор – клиент);

база данных – накапливает информацию (инициатор – web-service);

WEB-app – отображает сохраненную в базе информацию по заданным критериям (например, по всем компьютерам, по одному компьютеру).

Для написания системы были использованы следующие технологии и язык программирования:

Microsoft Visual Studio Professional 2010 (+ sp1 for VS 2010), язык программирования c#;

MS SQL 2008 R2 Express – центральная база данных;

NET Framework 4.0;

ASP.NET 4.0 (веб-платформа);

ASP.NET MVC 3 Framework — фреймворк для создания веб-приложений;

MS IIS (Web service + xml);

ADO.NETEntityFramework (LINQforsql) – объектно-ориентированная технология доступа к данным;

JavaScript — прототипно-ориентированный скриптовый язык программирования;

HTML 5, CSS 3, JQuery, JSon;

Win services – клиентское приложение.

Заключительным этапом разработки явилась апробация программного средства – непосредственный сбор и накопление необходимой информации с компьютеров-клиентов, а также отображение сохраненной в базе информации по заданным критериям.

Для организации сбора необходимой информации на компьютере-клиенте устанавливается утилита «сервис мониторинга компьютеров», представленная на рис. 2.

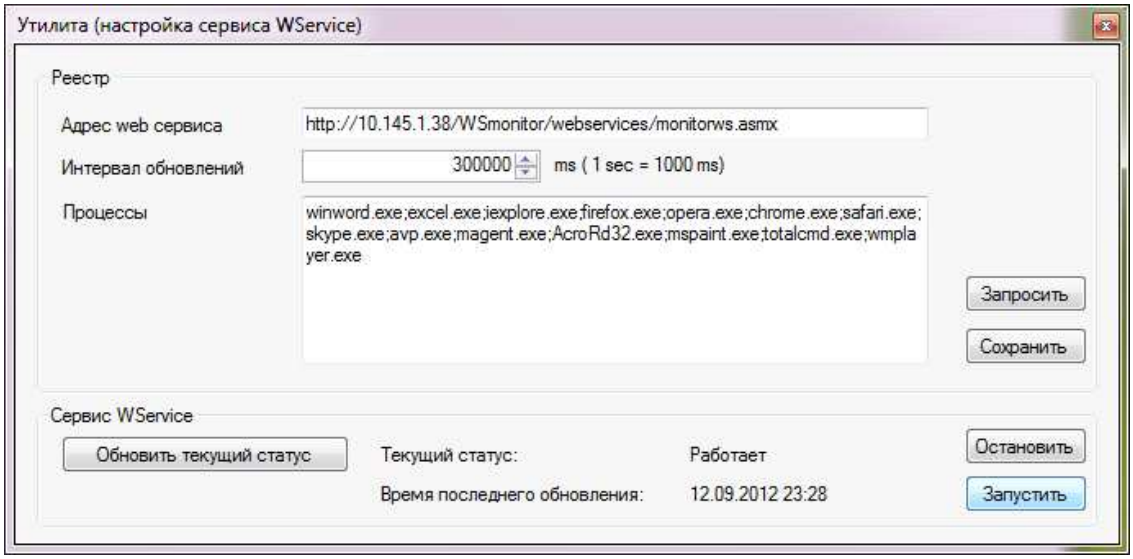

Рис. 2. Утилита «сервис мониторинга компьютеров».

После успешной инсталляции утилиты необходимо запустить ее и выполнить следующие настройки:

в первой строке указывается адрес веб-сервиса, на который будут отправляться xml-пакеты, собранные с компьютера-клиента;

во второй строке задается временной интервал сбора характеристик с компьютера;

в третьей строке выбираются процессы, которые будут постоянно отслеживаться на компьютере-клиенте.

Следует отметить, что настройку утилиты может произвести только пользователь, обладающий правами администратора в системе.

Таким образом, вся необходимая информация о рабочих станциях, собранная с помощью утилит, отправляется в виде xml-пакетов на сервер.

Для последующей работы и анализа собранных данных для администраторов системы разработано веб-приложение, после авторизации в котором администратор может проанализировать всю собранную информацию как в режиме онлайн, так и за определенный период времени.

Используя фильтры отбора, можно получить более детальные сведения о рабочей станции, запущенных на ней процессах, при этом обязательными полями для заполнения является временной интервал.

Проверка запущенных на удаленных компьютерах процессов необходима по многим причинам. Во-первых, она помогает в обнаружении на удаленных машинах вредоносного программного обеспечения – в этом случае нужно заранее знать имена процессов, запускаемых вирусами. Во-вторых, такая проверка позволяет администратору контролировать действия пользователей, запускающих определенные приложения в рабочее время, – игры, медиа-проигрыватели и т.п.

Основное окно администратора для работы с собранными параметрами с компьютеров-клиентов представлено на рис. 3.

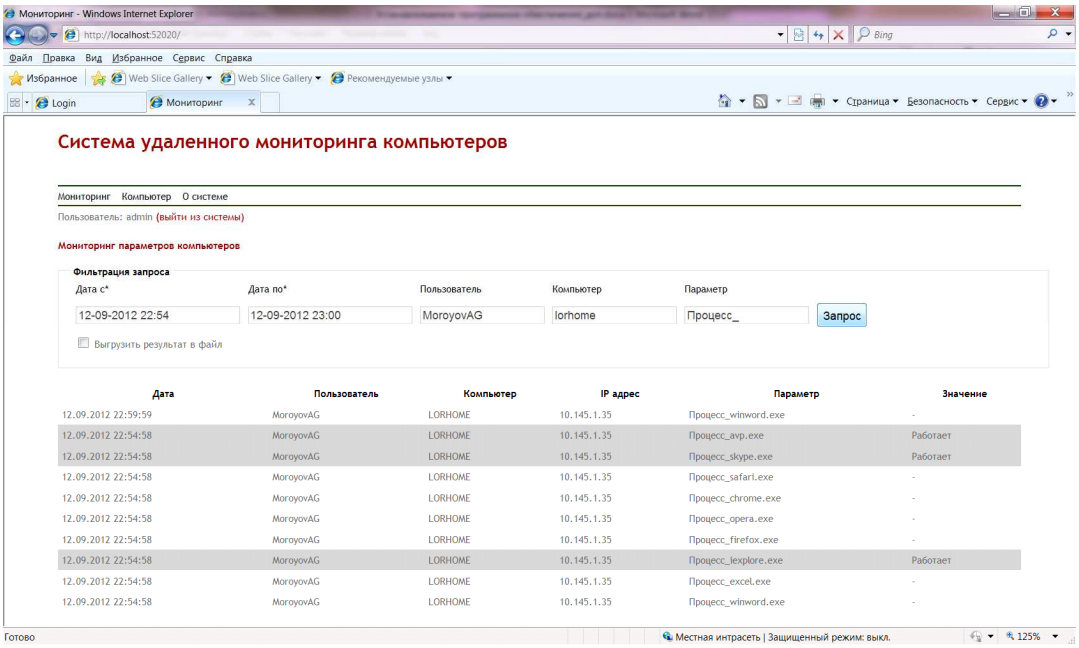

Рис. 3. Веб-интерфейс для анализа собранных параметров.

Следует отметить, что для удобства работы с данными мониторинга реализована функция выгрузки информации в файл.

Следующими немаловажными функциями информационной системы являются сбор и отображение основных характеристик компьютеров, позволяющими системному администратору более эффективно управлять вычислительной техникой.

Поскольку конфигурация компьютеров изменяется в современной организации почти каждый день и проведение «вручную» ежедневного мониторинга требует немыслимых временных затрат, в основе управления средствами вычислительной техники лежит автоматический сбор основных параметров.

Таким образом, на основании собранных данных формируется хранилище сведений о вычислительной технике, представленное на рис. 4.

При необходимости можно вывести на печать форму с характеристиками конкретного компьютера.

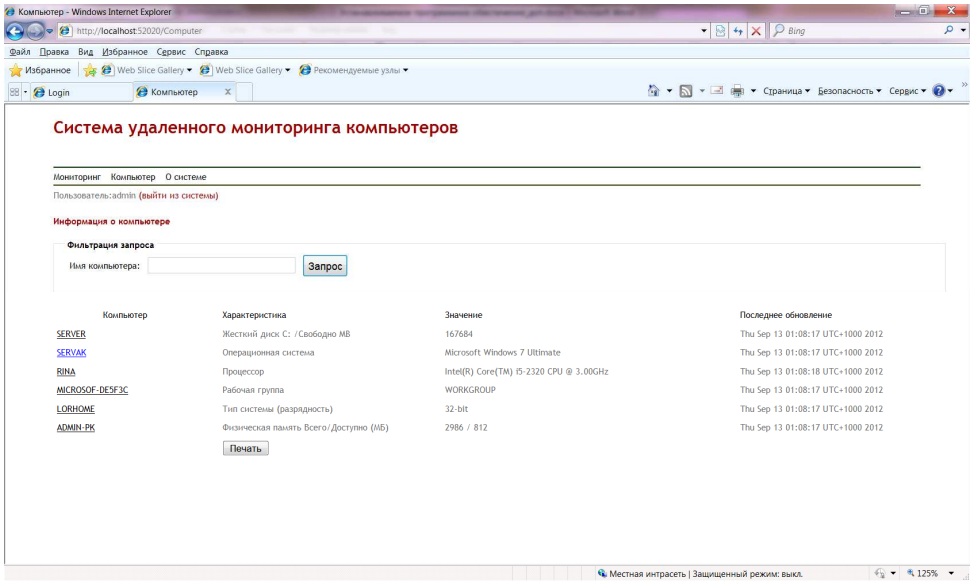

Рис. 4. Вкладка «информация о компьютерах».

Разработанная информационная система удаленного мониторинга для учреждения «Земельная кадастровая палата» позволяет автоматизировать процесс сбора необходимых параметров с компьютеров-клиентов, получать самые актуальные данные для формирования отчетности и последующего их анализа, помогает системному администратору вовремя выявить нарушения информационной безопасности, эффективнее управлять средствами вычислительной техники.

---

1. Безбогов, А.А. Безопасность операционных систем: Учеб. пособие/ А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартамьянов. – М.: Машиностроение-1, 2007. – С. 213-214.

2. Компьютерный шпионаж. Часть 1. Утилиты для слежки [Электрон. ресурс]. − Режим доступа: http://www.3dnews.ru/software/spy_tools_1 − 18.09.2012.

3. Протоколирование и аудит, шифрование, контроль целостности знаний [Электрон.ресурс]. − Режим доступа: http://www.intuit.ru/department/ security/secbasics/11/ − 18.09.2012.