Известия Гомельского государственного университета
имени Ф. Скорины, №5 (44), 2007

УДК 681.3

Удаленный контроль и управление процессами в локальных сетях

А. В. Воруев, О. М. Демиденко, А. И. Кучеров

Эксплуатация локальной вычислительной сети (ЛВС) в современном производственном процессе недостаточно эффективна. Причиной данного факта являются:

- низкая потребность производственных процессов в информационном обмене между узлами сети;
- низкий уровень обеспеченности программными системами, использующими сетевой обмен при управлении производственными и информационными процессами;
- недостаточная квалификация пользователей и обслуживающего персонала.

Современные сетевые технологии поддерживают скорость сетевого обмена до 10 Гбит в секунду в пределах ЛВС, что позволяет разместить в ней серьезное информационное наполнение (например, несколько медиапотоков в режиме on-line).

Стоимость сетевого оборудования неуклонно снижается. Таким образом, при организации новой или модернизации существующей сети у обслуживающего ЛВС персонала появляется запас сетевого трафика, который возможно использовать для автоматизации некоторых технических процедур обслуживания сети, а также сбора многочисленных статистик, позволяющих принимать эффективные решения по изменению состава оборудования и структуры ЛВС.

К числу подобных задач можно отнести:

– сбор статистик по структуре информационных потоков в ЛВС;

– ведение учета состояния материальной базы узлов ЛВС и ее изменения;

– учет занятости рабочих мест сети (по времени использования и по составу рабочей нагрузки);

– учет рабочего времени пользователей, затраченного на работу в ЛВС предприятия.

Существует два подхода к организации удаленного контроля и управления сложными сетями: централизованный и децентрализованный.

Основными достоинствами централизованного управления являются:

– концентрация всей информации о состоянии сети в одном узле управления;

– минимальная длина цикла управления;

– непротиворечивость принимаемых решений.

К недостаткам такого подхода следует отнести:

– уязвимость системы управления;

– значительный объем обрабатываемой информации требует запаса системных ресурсов.

Децентрализованное управление сетью характеризуется отсутствием единого центра управления сетью. Его функции перераспределяются между множеством систем управления сетью.

Децентрализованное управление также обладает рядом достоинств и недостатков, поэтому в реальной практике используются сложные модели сочетания этих двух подходов для решения практических задач.

К примеру, для решения задачи контроля эксплуатации пользователями компьютеров под управлением операционных систем MicroSoft и являющихся узлами ЛВС достаточно воспользоваться накопленной системной информацией. Операционной системой каждого узла ЛВС ведется журнал безопасности (security log), куда записываются события открытия и закрытия сеанса работы пользователей. Ограничением этих журналов могут быть сроки актуальности записей, тогда новые регистрируемые события вытесняют из журнала предыдущие события.

Для формирования статистической выборки необходимо организовать процедуру перио-

дического опроса журналов безопасности отдельных узлов, объединения их информации в единую базу данных и фильтрации вновь собираемых данных от ранее зарегистрированных событий. Также в журналах операционных систем MicroSoft фиксируется множество событий, незначимых при решении данной задачи, для удобства работы их приходится отфильтровывать.

Схема работы программной системы показана на рисунке 1.

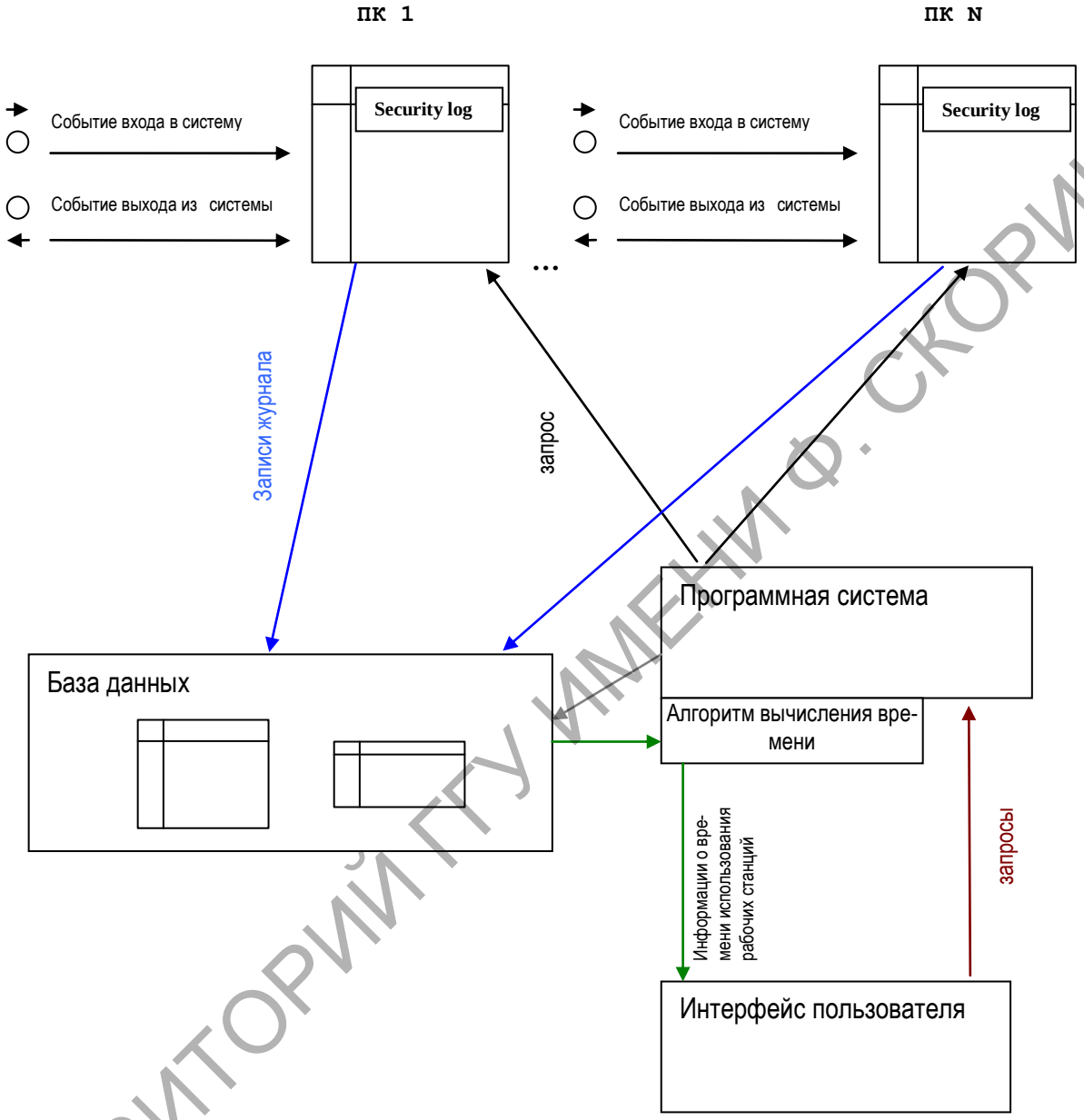

Рисунок 1 – Функциональная схема первичного сбора данных

Для снижения нагрузки на систему программа назначается политикой как logoff-скрипт. Во время выхода пользователя в единую базу SQL будут записаны следующие значения: имя пользователя (в формате Имя Фамилия), дата и время выхода, uptime компьютера пользователя в секундах, дата и время входа, имя компьютера, на котором работал пользователь.

Для организации удаленного доступа к информации, хранящейся на узлах ЛВС используется технология WMI.

Инфраструктура WMI связывает приложения управления и провайдеров, а также играет роль хранилища классов-объектов и, во многих случаях, менеджера памяти для устойчивых объектных свойств. WMI осуществляет хранение (работает как репозитарий), подобно базе данных на жестком диске. WMI, как часть своей инфраструктуры, поддерживает несколько API, с помощью которых приложения управления обращаются к объектным данным, а провайдеры поставляют данные и определения класса.

WMI разработан специалистами Microsoft на базе технологии управления предприятием через Web – Web-Based Enterprise Management (WBEM). WBEM – это стандарт, определенный консорциумом Distributed Management Task Force (DMTF). WBEM определяет структуру расширяемого набора данных о предприятии и возможности администрирования, необходимые для управления локальными и удаленными системами, включающими произвольные компоненты.

Использованием программ данного направления можно сократить простои оборудования, более эффективно планировать приобретение и обновление вычислительной техники, а также переподготовку персонала, обслуживающего вычислительную технику.

При сборе такой распределенной статистики для установления однозначной последовательности событий необходимо предусмотреть синхронизацию системных часов узлов сети. Системы, реализующие данную функцию, были предложены и неоднократно опробованы. К их числу можно отнести: алгоритм синхронизации логических часов, централизованное управление системными часами узлов сети и периодическая корректировка системного времени узлов. Для нашей задачи более эффективным механизмом являются два последних, тем более что они поддерживаются на уровне серверных компонент семейства операционных систем Microsoft.

Ограничения, которые следует учитывать при организации работы нашей программной системы, заключаются в следующем:

– необходимо интегрировать в состав центрального узла сбора статистики пакет системных функций framework.net второй версии или выше;

– клиенты сети, которые будут доступны для удаленного сбора статистики, должны управляться операционной системой MS Windows 2000 или более новых версий;

– утилита сбора статистики должна иметь удаленный доступ к данным на уровне системной службы, что может рассматриваться некоторыми брандмауэрами как нарушение системы безопасности.

Abstract. The developed program system on gathering statistical data on operation of computer facilities and work of users in a network is offered in the paper.

Литература

1. Попов, А. Администрирование Windows с помощью WMI и WMIC (+ CD-ROM) / А. Попов, Е. Шикин // Серия: Мастер систем, Санкт-Петербург, БХВ-Петербург, 2004. – 752 с.

2. Шиндер, Д. Л. Основы компьютерных сетей / Д. Л. Шиндер // Пер. с англ., Москва: Издательский дом «Вильямс», 2002. – 656 с.

3. Спортак М. Компьютерные сети и сетевые технологии. Platinum Edition / М. Спортак, Ф. Паппас // Пер. с англ., Санкт-Петербург: ООО «ДиаСофтЮП», 2005. – 720 с.

Гомельский государственный
университет имени Ф. Скорины

Поступило 17.04.07