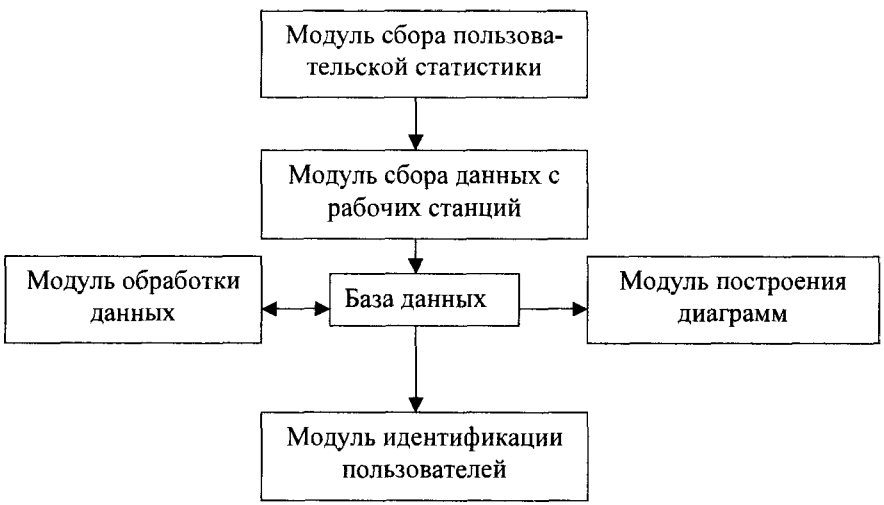
УДК 007

ПРОГРАММНЫЙ КОМПЛЕКС СБОРА И АНАЛИЗА ДАННЫХ ОПЕРАЦИОННОЙ СРЕДЫ ОБ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ

С.В. Дробышевский, студент;
Г.Ю. Наумова, преподаватель-стажер;
А.И. Кучеров, ассистент кафедры АСОИ
ГГУ им. Ф. Скорины, kucherov@gsu.by

Цель проекта создание системы анализа работы пользователей в сетевой среде и формирование отчетов с сохранением их в необходимый формат. При разработке клиент-серверного приложения использовалась среда разработки Delphi 7 для языка программирования pascal.

На рисунке 1 показана упрощенная схема программного комплекса.



Имеется модуль сбора пользовательской статистики, который функционирует на пользовательских станциях, которая собирает информацию о деятельности пользователей в операционной среде.

Клиент-серверное приложение является идеальным вариантом для работы в сетевой среде и взаимодействия с удаленными базами данных, т.к. позволяет обрабатывать собираемые программой-клиентом данные, на сервере не загружая тем самым терминалы.

Разработка приложения в клиент-серверной архитектуре обладает рядом преимуществ: небольшая нагрузка на сеть (в сравнении с файл-серверной архитектурой), высокая степень защиты данных из-за того, что управление базой данных осуществляется через сервер, а не напрямую приложением и простотой самого приложения.

Приложение на серверной стороне собирает файлы статистики созданные клиентской частью приложения, сортирует их и заносит данные статистики в базу данных. В файле, получаемом от программы-клиента, содержится информация о времени включения и выключения терминала, пользователях использовавших этот терминал, времени их входа и выхода из системы, загружаемые приложения и сайты, статистика по нажатию клавиш клавиатуры и мыши, время простоя терминала.

Данные файла статистики обрабатываются серверной частью приложения и заносятся в базу данных, сортируя их по именам машины и дате создания, строятся различные графики и диаграммы, которые позволяют судить о частоте использования тех или иных приложений, помогая тем самым гибко настраивать политику доступа данным.

Программа после сбора статистики с рабочих станций и последующей их обработке на сервере позволяет определять время простоя и пиковую загрузку компьютерных систем с построением графиков. При дальнейшей доработке программа позволит делать и другие выводы на основе имеющейся информации.

В дальнейшем, данные, полученные в результате обработки пользовательской статистики, могут использоваться для дополнительной идентификации пользователей на основе их поведения в операционной среде.

Результатом проекта стало создание системы мониторинга пользователей на рабочей станции, для автоматизации поиска информации в современных компьютерных сетях, обладающей следующими функциями и особенностями:

программа загружается как процесс;

клиентская часть загружается при загрузке компьютера и отслеживает изменения состояния среды, поведения пользователей (загруженные файлы, процессы, приложения, периодичность нажатия кнопок клавиатуры и мышки и др.) и формирует на и основе файлы статистики;

при входе в систему серверная часть опрашиваст удаленные машины клиентов на наличие новых файлов статистики;

копирует их на сервер, обрабатывает и заносит результаты в базу данных;

по желанию администратора строит различные графики и диаграммы по данным статистики;

на основе имеющейся информации, которая хранится в база данных, позволяет с некоторой погрешностью идентифицировать пользователя.

Применение созданного программного комплекса позволит существенно улучшить идентификацию пользователей как по известным схемам так и с применением новы алгоритмов. В свою очередь, это позволит поднять на новый уровень информационную безопасность организации.