УДК 004

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ АНАЛИЗА ЛОГ ФАЙЛОВ

А.О. Юдин
Научный руководитель: Д.М. Сонькин, доцент каф. ИПС ИК ТПУ
Национальный исследовательский Томский политехнический университет

Nowadays many people use personal computers. Not every one of them can deal with problems appears during working with computers. We are developing software that can show reasons of errors and illegal data transmission. This software will use multiple log files form different sources such as Windows logs and antivirus software. It will be a middle point between users and technical support.

Keywords: log file, software, technical support.
Ключевые слова: лог-файл, программное обеспечение, техническая поддержка.

В последнее десятилетие более семидесяти процентов населения Земли являются пользователями персональных компьютеров. Не все из этих пользователей способны самостоятельно разобраться с проблемами, возникающими при работе с компьютерами. В ходе разработки данного программного обеспечения мы стараемся создать прикладное приложение, которое обеспечит пользователей должной поддержкой при возникновении данных проблем, а людей, занимающихся технической поддержкой, инструментом выявления причин возникновения ошибок и упрощения работы с пользователями.

Если говорить о таком классе программ, как анализаторы лог-файлов, то они получили активное развитие, как инструмент работы с сетевыми логами. На данный момент большая часть данных программ до сих пор ориентирована на работу с сетями, сетевым трафиком, серверными технологиями и веб-сервисами. Однако, в ходе подготовительной работы к разработке данного программного обеспечения было выявлено, что есть ниша в которой данные приложения развиты мало или не затрагивают ее вовсе.

При работе операционная система Windows ведет тщательный учет действий запущенных программ и действий пользователя. Аналогичный учет ведут программы-антивирусы, программы класса firewall и пакеты программ комплексной защиты. При совмещении логфайлов данных программ мы получим почти полную информацию о том, что система делала в выбранный период времени. Таким образом мы решаем две важные задачи. Первая – совместить сетевые логи и информацию о работе программ в системе. Вторая – в случае потери одного источника информации по причине работы вредоносного программного обеспечения мы можем частично воспользоваться информацией из другого. В результате работы нашей программы, мы сможем однозначно отследить, какая программа вызвала ошибку в работе или передала данные вне ведома пользователя.

В общем виде работа программы может быть представлена следующим образом:

- Сбор данных из лог файлов различных служб.
- Выборка данных по различным критериям.
- Формирование логических массивов.
- Обработка полученных массивов.
- Вывод результата и рекомендаций.

На этапе сбора данных мы считываем данные различных лог файлов для последующей работы с ними. При выборке мы отсеиваем различные данные по признакам, задаваемым оператором. На этапе формирования массивов мы объединяем оставшиеся данные по логическим признакам в один многомерный массив. В процессе обработки данных мы применяем различные алгоритмы нахождения зависимостей внутри массива. На основании работы алгоритмов поиска программа делает выводы о причинах возникновения ошибок или нежелательных передач данных в сеть.

Таким образом, данная программа будет полезна как для продвинутого пользователя, так и для служб технической поддержки. Продвинутые пользователи получат инструмент для нахождения неисправностей в системе и в дальнейшем смогут самостоятельно ее устранить. Службы технической поддержки получат мощный инструмент поддержки тех пользователей, удаленное администрирование которых невозможно по причинам слишком большого количества пользователей или отсутствия подключения к сети. Следует учесть, что наше программное обеспечение не рассчитано на самостоятельное решение проблем пользователей, однако будет являться полезным инструментом в поиске ошибок.