Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Системное программное обеспечение вычислительных машин (СПОВМ)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

на тему:

«Сниффер клавиатуры»

Студент: гр.350501 Шешко В.Р.

Руководитель: Яночкин А.Л.

Минск 2015

Содержание

[Введение 3](#_Toc414805627)

[1.Обзор литературы 4](#_Toc414805628)

[2. Техническое задание 6](#_Toc414805629)

[Заключение 7](#_Toc414805630)

[Список литературы 8](#_Toc414805631)

# Введение

Общество, в котором живет современный человек, характеризуют как информационное. Компьютеры получают все более широкое применение – даже там, где, как казалось совсем недавно, их применить невозможно. Информационные технологии и их знание становится неотъемлемой частью жизни любого человека, и в основу применения этих технологий также легло применение компьютера.

Сегодня большая часть работы выполняется с использованием компьютера: электронных документов, файлов, программ и сайтов. Неудивительно, что хронометраж рабочего времени за компьютером так популярен сейчас. С его помощью можно проанализировать рабочий процесс и выявить резервы времени.

**Учет деятельности за компьютером** — дешевый и полностью объективный способ. Он идеально подходит для офисного персонала, который большую часть времени проводит на рабочем месте за компьютером.

Снифферы клавиатуры принадлежат к той группе программных продуктов, которые осуществляют контроль над деятельностью пользователя персонального компьютера. Программные продукты этого типа предназначаются исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (лог-файл), который впоследствии изучается человеком, установившим эту программу.

# 1.Обзор литературы

* 1. Спецификация клавиатурных снифферов

Клавиатурный сниффер — это программное обеспечение или аппаратное устройство, регистрирующее нажатия клавиш на клавиатуре компьютера.

Клавиатурные снифферы подразделяются на аппаратные и программные. Первые представляют собой небольшие устройства, которые могут быть закреплены на клавиатуре, проводе или в системном блоке компьютера. Вторые — это специально написанные программы, предназначенные для отслеживания нажатий клавиш на клавиатуре и ведения журнала нажатых клавиш. Принципиальная идея сниффера состоит в том, чтобы внедриться между любыми двумя звеньями в цепи прохождения сигнала от нажатия пользователем клавиш на клавиатуре до появления символов на экране.

 Наиболее популярные технические подходы к построению программных клавиатурных снифферов:

* системная ловушка на сообщения о нажатии клавиш клавиатуры (устанавливается с помощью функции WinAPI SetWindowsHook, для того чтобы перехватить сообщения, посылаемые оконной процедуре.
* циклический опрос клавиатуры (с помощью функции WinAPI Get(Async)KeyState, GetKeyboardState).
* драйвер-фильтр стека клавиатурных драйверов ОС Windows.

Кейлоггеры могут внедряться в любом месте последовательности обработки, перехватывая данные о нажатых клавишах, передаваемые одной подсистемой обработки следующей подсистеме в цепочке обработчиков.

Установка ловушки для клавиатурных сообщений

Пожалуй, это самый распространенный метод реализации клавиатурных снифферов. Посредством вызова функции SetWindowsHookEx сниффер устанавливает глобальную ловушку на клавиатурные события для всех потоков в системе. Фильтрующая функция ловушки в этом случае располагается в отдельной динамической библиотеке, которая внедряется во все процессы системы, занимающиеся обработкой сообщений. При выборке из очереди сообщений любого потока клавиатурного сообщения система вызовет установленную фильтрующую функцию.

К достоинствам этого метода перехвата относится простота и гарантированный перехват всех нажатий клавиатуры, из недостатков можно отметить необходимость наличия отдельного файла динамической библиотеки и относительную простоту обнаружения по причине внедрения во все системные процессы.

Использование циклического опроса состояния клавиатуры

Состояние всех клавиш с небольшим интервалом опрашивается с помощью функций GetAsynсKeyState или GetKeyState. Данные функции возвращают массивы асинхронного или синхронного состояния клавиш; анализируя их, можно понять, какие клавиши были нажаты или отпущены после последнего опроса.

Достоинства данного метода — предельная простота реализации, отсутствие дополнительного модуля недостатки — отсутствие гарантии обнаружения всех нажатий, могут быть пропуски; легко обнаруживается мониторингом процессов, опрашивающих клавиатуру с высокой частотой.

Использование драйвер-фильтра драйвера класса клавиатуры Kbdclass

Документированный в DDK способ перехвата. Снифферы, построенные на основе этого метода, перехватывают запросы к клавиатуре посредством установки фильтра поверх устройства «\Device\KeyboardClass0», созданного драйвером Kbdclass. Фильтруются только запросы типа IRP\_MJ\_READ, поскольку именно они позволяют получить коды нажатых и отпущенных клавиш.

Достоинства — гарантированный перехват всех нажатий, невозможность обнаружения без использования драйвера. Недостатки — необходимость установки собственного драйвера.

При выборе средств для разработки приложения необходимо учесть множество различных аспектов, наиболее важным из которых является язык программирования, так как он в значительной степени определяет другие доступные средства. Для реализации клавиатурного сниффера наиболее эффективным будет использование языков программирования C и C++. Они предоставляют все средства для создания приложения для операционных систем семейства Windows X.

2. Техническое задание

Требуется разработать программу, ведущую мониторинг нажатий клавиш на клавиатуре.

Необходимо предусмотреть возможности:

- отслеживание нажатий клавиш

-  запись вводимой информации в файл

- дистанционно получать информацию о работе программы

-  возможность незаметной работы для пользователя

- возможность незаметной установки

Используемые языки программирования – С, С++.

**Заключение**

# Список литературы