1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 3**

1. «Планировщик задач Windows»
2. по дисциплине «Безопасность современных информационных технологий»
3. Выполнил
4. студент гр. 4851003/00802 Вологдин М.В.

<*подпись*>

1. Преподаватель Соловей Р.С.

<*подпись*>

1. Санкт-Петербург
2. 2023
3. **Цель работы**

Изучить возможности встроенного в ОС Windows планировщика задач.

1. **Задача**

Реализовать программу для управления планировщиком задач в ОС Windows, использующую возможности Windows API.

* язык программирования: C/C++;
* разрабатываемая программа не должна использовать готовые обертки над Windows API;
* программа должна уметь выводить список активных задач и их статус;
* создайте правило, уведомляющее пользователя о внесении изменений в механизмы безопасности Windows: в работу встроенного антивируса Windows Defender, изменении любых настроек брандмауэра;
* создайте правило, уведомляющее пользователя, когда брандмауэр Windows блокирует ping-запрос с определенного IP-адреса;

поддержка ОС Windows 7–10.

1. **Ход работы**

В данной лабораторной работе было реализовано приложение, использующее WinAPI, выводящее информацию о списке задач. Также была реализована программа, выполняющая следующие задачи: выводить уведомление при изменении механизмов безопасности Windows(windows defender, firewall), выводить уведомление о заблокированных ping-запросах и адресе отправителя.

Меню основной программы можно увидеть на рисунке 1.

Основной функционал состоит в выводе всех текущих задач и их статуса, а также создании задачи для вывода соответствующих уведомлений.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1 - Главное меню программы

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2 - Вывод всех задач

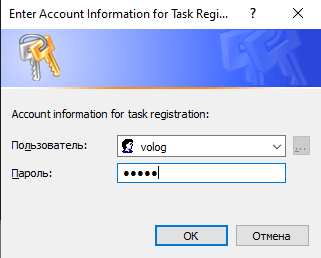


Рисунок 3 - Запись задачи в планировщик

На рисунке 2 изображен вывод списка текущих задач, на рисунке 3 меню, всплювающее при попытке записи задачи в планировщик, после чего эти задачи можно увидеть через стандартное меню планировщика taskschd.msc (рисунок 4).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 - Запись задачи в планировщик

Далее при выключении брандмауэра всплывает уведомление (рисунок 5), при попытке ping’a также выводится уведомление (рисунок 6).

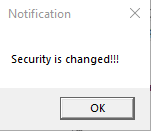


Рисунок 5 - Главное меню программы

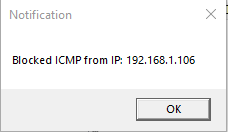


Рисунок 6 - Главное меню программы

Для тестирования вывода уведомления при блокировании входящих пакетов сначала был запрещены входящие запросы следующими командами:

auditpol /set /subcategory:"Отбрасывание пакета платформой фильтрации" /success:enable /failure:enable

auditpol /set /subcategory:"Подключение платформы фильтрации" /success:enable /failure:enable

Структура задачи записывается в формате XML.

Фильтр на изменение в параметрах безопасности Windows Defender:

<QueryList>

<Query Id='0'>

<Select Path='Microsoft-Windows-Windows Defender/WHC'>\*[System[Provider[@Name='Microsoft-Windows-Windows Defender'] and EventID=5007]]</Select>

</Query>

</QueryList>

<QueryList>

<Query Id='0'>

<Select Path='Microsoft-Windows-Windows Defender/Operational'>\*[System[Provider[@Name='Microsoft-Windows-Windows Defender'] and EventID=5007]]</Select>

</Query>

</QueryList>

Фильтр на изменение в параметрах Windows Firewall:

<QueryList>

<Query Id = '0' Path = 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall'>

<Select Path = 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall'>\*

[System[Provider[@Name = 'Microsoft-Windows-Windows Firewall With Advanced Security'] and EventID=2003]]

</Select>

</Query>

</QueryList>

Фильтр на блокирование запросов с определенного IP:

<QueryList>

<Query Id='0' Path='Security'>

<Select Path='Security'>

\*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and EventID=5152]]

</Select>

</Query>

</QueryList>

1. **Контрольные вопросы**

**1. Опишите, зачем нужен планировщик задач ОС Windows и какие есть альтернативы данному инструменту.**

Task Scheduler – сервис в ОС Windows, который, начиная с Windows 95, помогает исполнять рутинные задачи на выбранном компьютере (локальном или удаленном). Задачи выполняются с помощью различных триггеров, которые запускают задачи, когда срабатывает условие.

Случаи применения:

* Автоматическое создание резервной копии реестра
* Отправка отчетов о неполадках
* Оптимизация и дефрагментация дисков
* Обновление поискового индекса
* Оптимизация загрузки системы
* Создание точки восстановления системы
* Очистка временных файлов

Альтернативы: xStarter, nnCron, System Scheduler, Macro Scheduler, JIT Scheduler

**2. Какие триггеры существуют во встроенном планировщике задач ОС Windows?**

* Триггер регистрации (триггер на основе событий). Он запускает задачу при регистрации или обновлении задачи;
* Триггер события (инициированный событиями). Он запускает задачу при возникновении определенного системного события;
* Триггер времени (триггер, основанный на времени). Он запускает задачу в определенную дату и время;
* Ежедневный/еженедельный/ежемесячный/ежемесячный недельный (DOW) триггер (таймер календаря по времени). Он запускает задачу в определенное время по ежедневному/еженедельному/ежемесячному/ежемесячном расписании дня недели графику;
* Триггер бездействия (инициируемый событиями триггер). Он запускает задачу, когда компьютер переходит в состояние ожидания;
* Триггер загрузки (инициируемый событиями). Он запускает задачу при загрузке системы;
* Триггер входа (триггер на основе событий). Он запускает задачу при входе пользователя в систему;
* Сбой изменения состояния сеанса (триггер на основе событий). Он запускает задачу, когда сеанс сервера терминалов изменяется.

**3.** **Какие ограничения накладываются на задачи?**

Нельзя использовать задачи для повышения привилегий. Также действия, связанные с доступом к объектам, зависят от параметра безопасности пользователя.

**4.** **Перечислите типы задач, которые могут быть запущены с помощью планировщика.**

* TASK\_ACTION\_EXEC – это действие выполняет операцию командной строки. Например, действие может запускать скрипт, запускать исполняемый файл или, если указано имя документа, найти связанное приложение и запустить приложение с документом.
* TASK\_ACTION\_COM\_HANDLER – это действие вызывает обработчик. Его можно использовать, только если для свойства совместимости задачи установлено значение TASK\_COMPATIBILITY\_V2.
* TASK\_ACTION\_SEND\_EMAIL – это действие отправляет сообщение электронной почты. Его можно использовать, только если для свойства совместимости задачи установлено значение TASK\_COMPATIBILITY\_V2.
* TASK\_ACTION\_SHOW\_MESSAGE – это действие показывает окно сообщения. Его можно использовать, только если для свойства совместимости задачи установлено значение TASK\_COMPATIBILITY\_V2.

**5. Опишите механизмы безопасности Windows, которые задействованы**

**при регистрации новых задач.**

Каждая задача регистрируется и исполняется в отдельном контексте. Также задачи для разных пользователей стартуют в разных сессиях Windows. Также для регистрации задачи нельзя обойти UAC, то есть обязательно нужен пользователь с правами администратора

1. **Выводы**

В данной лабораторной работе была создана программа для управления планировщиком задач в ОС Windows, для чего были изучены возможности встроенного в ОС Windows планировщика задач. Данная программа может выводить список активных задач и их статус, создавать правила, которые уведомляют пользователя о внесении изменений в механизмы безопасности Windows и о блокировке брандмауэром ping-запросов.