

2. Home | TIOBE - The Software Quality Company [Електронний ресурс]. – Режим доступу : <https://tiobe.com/tiobe-index/> (дата звернення: 2021-11-01). – Назва з екрана.

3. Python | TIOBE - The Software Quality Company [Електронний ресурс]. – Режим доступу : <https://www.tiobe.com/tiobe-index/python/> (дата звернення: 2021-11-01). – Назва з екрана.

4. Вакансії DOU.UA [Електронний ресурс]. – Режим доступу : <https://jobs.dou.ua/vacancies> (дата звернення: 2021-11-01). – Назва з екрана.

5. Stack Overflow Developer Survey 2021 [Електронний ресурс]. – Режим доступу : <https://insights.stackoverflow.com/survey/2021#technology-most-popular-technologies> (дата звернення: 2021-11-01). – Назва з екрана.

Ключові слова: відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики, освіта.

Keywords: open software, open data formats, open communication protocols, threats and risks, education.

Ключевые слова: открытое программное обеспечение, открытые форматы данных, открытые протоколы взаимодействия, угрозы и риски, образование.

Задерейко Александр Владиславович

*Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий, кандидат технических наук,
доцент*

Кухаренко Сергей Викторович

*Национальный университет «Одесская юридическая академия»,
доцент кафедры кибербезопасности, кандидат технических наук*

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ УТЕЧЕК В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

Большинство пользователей операционной системы (ОС) Windows, встречали в списке диспетчера задач, множество процессов с именем *svchost.exe*.

В зависимости от версии ОС Windows и от ее конфигурации, количество таких процессов может составлять от нескольких единиц до нескольких десятков.

Это объясняется тем, что *svchost.exe* является главным процессом для системных служб ОС Windows, загружаемых из динамических библиотек (*.dll). Исполняемый файл *svchost.exe* размещен в системном каталоге \Windows\system32\. Запуск системных служб организован так, что позволяет существенно уменьшить затраты оперативной памяти и ресурсов процессора. Все копии процессов *svchost.exe* запускаются системным процессом *services.exe* в ходе начальной загрузки ОС Windows, а также в ходе выполнения системных процессов, а также процессов связанных с запуском прикладного программного обеспечения (ППО) пользователя [1].

Системные процессы ОС Windows, особенно те, за запуск которых отвечает процесс *svchost.exe*, являются необходимыми компонентами для ее полноценной работы [2]. В процессе загрузки ОС Windows осуществляется запуск служб:

- диспетчера сетевых подключений;
- планировщика заданий;
- Plug and Play и HID;
- центра обновления;
- защитника ОС Windows;
- фоновой интеллектуальной службы передачи BITS и других.

При запуске ОС Windows служба *svchost.exe* проверяет разделы реестра со службами и создает список служб, которые загружаются в оперативную память. Каждый сеанс службы *svchost.exe* может выполняться в виде группирования служб. Такая организация необходима для уменьшения количества различных запущенных служб и улучшает их возможную отладку, если будет в этом необходимость. К примеру, один процесс *svchost.exe* запускает несколько служб связанным с встроенным сетевым экраном ОС Windows [3], который по умолчанию беспрепятственно пропускает все его исходящие соединения при наличии подключения к цифровому пространству Интернет (рис. 1).

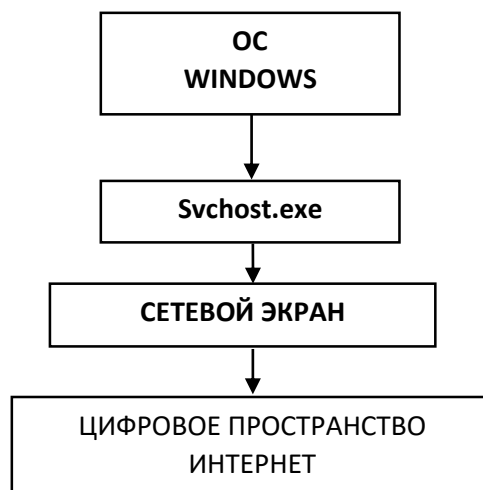


Рис. 1. Схема организации соединений службы *svchost.exe* с цифровым пространством Интернет.

Такие настройки встроенного сетевого экрана являются предустановленными при установке ОС Windows на компьютер пользователя. Это обстоятельство в свою очередь приводит к полному или частичному дублированию всех исходящих/входящих соединений, осуществляемых прикладным программным обеспечением (ППО) пользователя, что само по себе представляет потенциальную угрозу для утечек персонализированных данных пользователя (рис. 2).

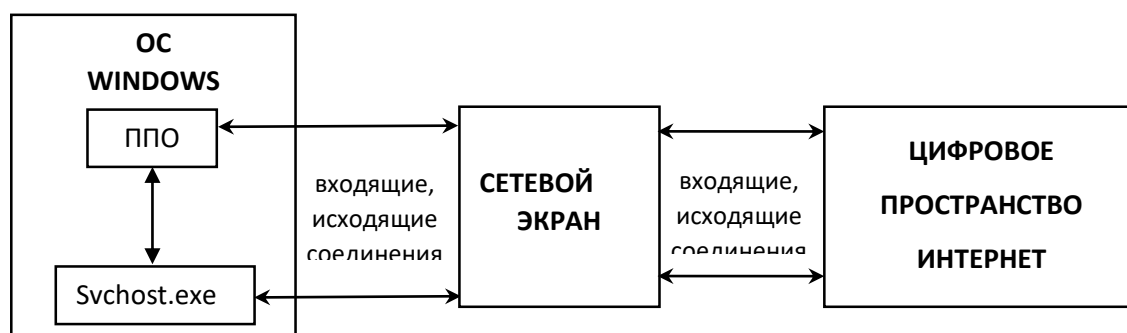


Рис. 2. Организация обмена данными между ОС Windows, ППО и цифровым пространством Интернет.

Для осуществления регламентированного доступа к цифровому пространству Интернет в семействе ОС Windows предусмотрено наличие встроенного брандмауэра (сетевого экрана) – системного программного обеспечения, которое выполняет контроль за обменом данными между ОС Windows и цифровым пространством Интернет [4].

Однако, как показывает долговременная практика углубленного исследования сетевого трафика ОС Windows, ППО и сетевого процесса *svchost.exe* с цифровым пространством Интернет с применением снифферов [5] – встроенный сетевой экран беспрепятственно пропускает большинство исходящих/входящих соединений системного ПО ОС Windows и ППО, которые неизбежно приводят к утечкам персональных данных пользователя [6, 7].

Анализ трафика исходящих/входящих соединений позволил разделить их на рабочие и сторонние. Также в процессе углубленного анализа было установлено наличие исходящих соединений сетевого процесса *svchost.exe*, которые можно классифицировать, как сторонние, так как они инициируются ППО и в большинстве случаев не соответствуют исходящим соединениям самого ППО (рис. 3).

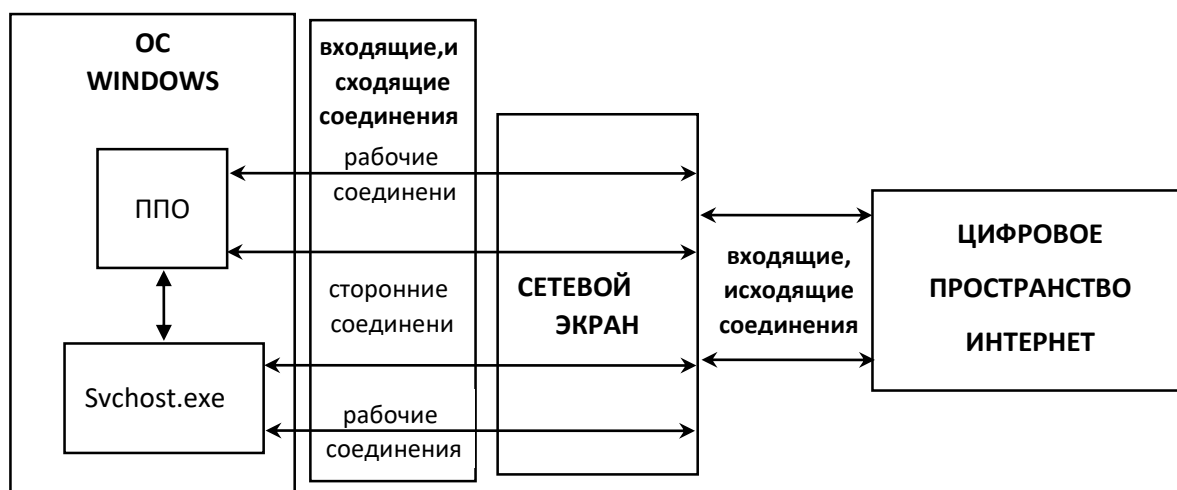


Рис. 3. Взаимосвязь сторонних и рабочих соединений ОС Windows, ППО и цифровым пространством Интернет.

Такая организация исходящих/входящих соединений в ОС Windows может с высокой долей вероятности привести к утечкам персональных данных пользователей. Для устранения этой проблемы, необходимо выполнить принудительную блокировку сторонних соединений ППО и сетевого процесса *svchost.exe* (рис. 4).

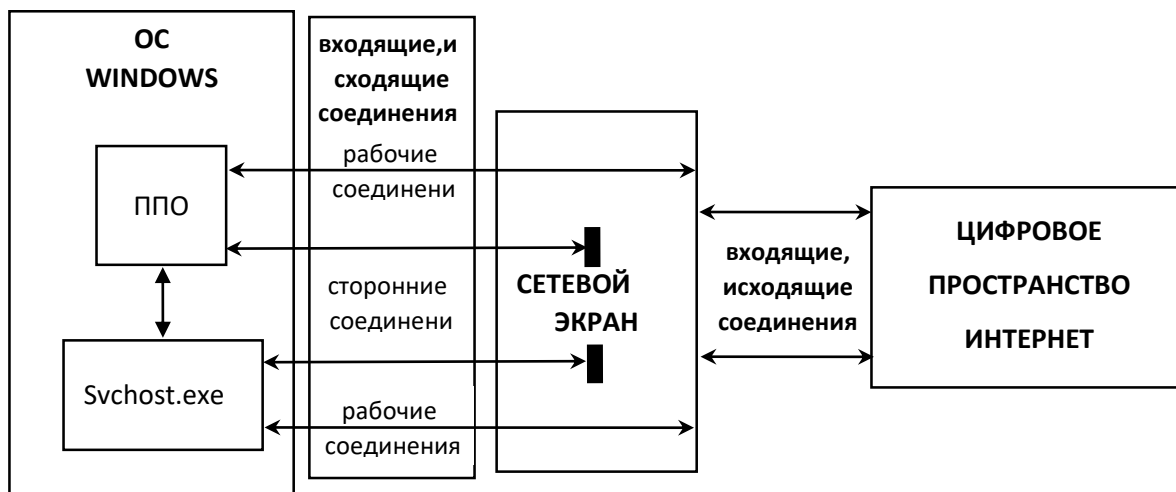


Рис. 4. Организация блокировки сторонних соединений ОС Windows и ППО с цифровым пространством Интернет.

В процессе длительного мониторинга и последующего анализа исходящих/входящих соединений, при организации блокировки сторонних соединений ОС Windows и ППО (см. рис. 4), была экспериментально подтверждена эффективность предлагаемого подхода для организации защиты персональных данных от потенциально возможных утечек.

Список использованных источников:

1. Процесс svchost.exe и системные службы, связанные с ним. : Веб сайт. URL: <https://ab57.ru/svchost.html> (Дата звернения: 1.11.2021).
2. Назначение процесса svchost.exe в ОС Windows. : Веб сайт. URL: <https://www.statusrecovery.ru/articles/assigning-the-svchost-exe-process-windows.html> (Дата звернения: 1.11.2021).
3. svchost.exe: Что это за хост-процесс? Почему грузит систему? [Электронный документ] - URL: <https://mywebpc.ru/windows/sluzhba-uzla-svchost-exe/> (Дата звернения: 1.11.2021).
4. Брандмауэр и защита сети в системе безопасности Windows. : Веб сайт. URL: <https://support.microsoft.com/ru-ru/topic-брандмауэр-и-защита-сети-в-системе-безопасности-windows-2385b621-9c5c-4834-9914-c7393f75fa84> (Дата звернения: 1.11.2021).
5. Снифферы (Sniffers). : Веб сайт. URL: <https://www.anti-malware.ru/threats/sniffers> (Дата звернения: 1.11.2021).

6. Algorithm of user's personal data protection against data leaks in Windows 10 OS / Olexander V. Zadereyko, Olena G. Trofymenko, Nataliia I. Loginova // Informatyka, Automatyka, Pomiarы w Gospodarce i Ochronie Środowiska, vol.9, - p. 41 – 44. URL: <https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-b9e2407a-7fc7-41bf-a947-c285ad6b6d70>.

7. Zadereyko A. Development of algorithm to protect user communication devices against data leaks / A. Zadereyko, Y. Prokop, O. Trofymenko, N. Loginova, O. Plachinda // Eastern-European Journal of Enterprise Technologies. – V. 1/2 (109) – Technology Center, 2021. – P. 24-34. URL: <http://dspace.onua.edu.ua/handle/11300/14489>.

Ключевые слова: утечки персональных данных, утечки данных в ОС Windows, блокировка утечек персональных данных.

Keywords: personal data leaks, data leaks in Windows OS, blocking of personal data leaks.

Ключові слова: витоки персональних даних, витоки даних в ОС Windows, блокування витоків персональних даних.

Лобода Юлія Геннадіївна

Національний університет «Одеська юридична академія»,

доцент кафедри інформаційних технологій,

кандидат педагогічних наук, доцент

ПРОГРАМНІ АНАЛІТИЧНІ ІНСТРУМЕНТИ BIG DATA ANALYTICS

Програмне забезпечення Big Data Analytics широко застосовується для ефективної обробки даних та досягнення конкурентної переваги на ринку. Програмні аналітичні інструменти Big Data допомагають відстежувати поточні ринкові зміни, потреби клієнтів, а також отримувати різну цінну інформацію. Розглянемо найпопулярніші інструменти аналітики.