УДК 811.111:004.05

ADVANTAGES AND DISADVANTAGES OF OPEN-SOURCE SOFTWARE

Pilipenko D.A., student
Scientific supervisor – Vanik I.Y., senior lecturer
English language department №1
Belarusian National University of Technology
Minsk, Republic of Belarus

Open-source software refers to a type of software that is available for viewing, studying, and modification. In recent years, there has been a growing popularity of this type of software, with evidence from many sources. For example, according to the 2023 Synopsys report, the overall volume of open-source code in each codebase has also increased; it has grown by 35% since 2018, with 89% of the total code being open source [1].

This paper reveals the advantages that have led many developers to adopt open-source software, as well as its disadvantages, to clarify why sometimes it might be better to avoid using it.

The first and most significant advantage is that by using open-source software, you get a ready-made product right away, eliminating the need to 'reinvent the wheel,' which saves considerable time and resources. All you need to do is to adapt the project to your needs.

However, this also leads to the main drawback of such software. Many people assume that open-source software can be freely taken and used, even if they are grateful, but this is not the case. Open-source software, as a rule, comes with usage restrictions, which are specified in special licenses that must be included with the software [2]. Depending on the license, some open-source software may only be used for educational purposes, while others can also be used commercially – provided that the new project includes the original license and credits the authors. Unfortunately, not everyone follows these rules [2].

For example, Patrick Wardle, a former hacker and ex-employee of the U.S. National Security Agency (NSA) and NASA – now known as a macOS malware expert – has written a significant amount of open-source software. His license requires commercial users to obtain his permission first. However, some companies have used his software

without consulting him, offering no compensation or even crediting him as a co-author [3].

Wardle believes he is far from the only open-source developer whose code is being used in paid software. He was only able to detect his own code because the software he writes is highly specialized and not widely distributed. In other words, most open-source developers may never even discover that their code is being used without permission. And even if they do, they would have to go to court to prove that their code was actually incorporated into a particular project [3].

Another significant advantage of open-source software is its enhanced security. Since numerous programmers contribute to open-source projects, they can fix each other's mistakes and implement additional security measures. A prime example of this is Linux, which is considered to be the most secure operating system. Professional developers and computer enthusiasts contribute to the Linux kernel by adding new features or fixing bugs or security flaws.

However, this very aspect also leads to another drawback: malicious actors may introduce harmful functionality into open-source software. For instance, in 2024, IT professionals encountered such malicious packages in the Python Package Index (PyPI) repository [4].

Thus, when choosing open-source solutions, it's crucial to carefully analyze their licenses, verify the developers' reputation, and comply with legal requirements. This approach allows you to maximize the benefits of open-source software while minimizing potential negative consequences.

References

1. Open-source security and risk analysis report – URL: https://balwurk.com/wp-content/uploads/2023/06/rep-ossra-2023.pdf (date of access: 15.03.2025).

2. The legal side of open source – URL: https://opensource.guide/legal/ (date of access:17.03.2025).

3. This Mac hacker’s code is so good; corporations keep stealing it – URL: https://www.theverge.com/2022/8/11/23301130/patrick-wardle-mac-code-corporations-stealing-black-hat (date of access: 25.03.2025).

4. Six Malicious Python Packages in the PyPI Targeting Windows Users – URL: https://unit42.paloaltonetworks.com/malicious-packages-in-pypi/ (date of access: 25.03.2025).