УДК 004.49

А. Ю. Монастирська
Л. В. Ібрагімова

EVOLUTION OF VIRUS AND ANTIVIRUS PROGRAMS AND THEIR DEVELOPMENT

Вінницький національний технічний університет

Анотація *У наш час серед людей можна зустріти тих, хто впевнений, що комп'ютерний вірус здатен зруйнувати не лише програмний мозок комп'ютера, а й його залізне тіло. Чи існуватимуть у майбутньому способи захиститися від такого явища, як комп'ютерна загроза? Дана стаття відповідає на ці питання, а також прогнозує, як віруси можуть продовжити свою еволюцію та як зміняться захисні програми.*

Ключові слова: комп'ютерний вірус, антивірус, еволюція вірусів, розвиток антивірусів.

Abstract *Nowadays, there are people who believe that a computer virus can destroy not only the computer software brain, but also its iron body. Will there be ways to protect against a computer threat in the future?*

This paper answers these questions as well as predicts how viruses can continue their evolution and how protection programs will change.

Key words: computer virus, antivirus, evolution of viruses, evolution of antivirus.

Computer viruses appeared much later than the first computers but users were completely unprepared for them. Even if the first ones did not harm the machine and personal data, and their developers were guided only by curiosity and desire to obtain statistics (for example, the use of certain media, rewriting or plagiarism), or prove their own strength and knowledge, they were viruses.

A virus that coexists with living things can cause their mutations, chronic disease, or, what we are interested in - evolution. It is viruses that force the immunity of a living being to adapt, change genetics and move to another level of life [1].

By projecting this onto a computer, we get a tedious experiment with only one end: a virus that infects a machine. Because both computers and their “diseases” were created by humans and are not living beings, they are not able to generate or protect themselves from diseases. That is why immunity for the helper must also be created by man. That's what happened, but the first pests to enter the computer required certain programs, and one of the programs could stop only one virus. So, a machine had a weak narrow-minded immunity, and any other virus could penetrate unnoticed.

With the advent of the Internet, the risk of receiving an unexpected “gift” on your own device has increased. It was realized that in this way money can made: decoding data, threatening to destroy or spread data, shocking reports of heavy fines for visiting a site and the account number to which the funds should be sent [2]. The variety of virus programs quickly became too large to install a single program on a single virus. This has led to the emergence of virus databases with samples of criminal programs that warn of the threat, but the weakest point of these programs – a person who can still allow the pest to get on the device. The more people used cloud services, the more they tried to protect their data, and this encouraged thieves to develop new technologies, write more complex code that could bypass the immunity program. Worms, trojans, blockers and cryptographers, ad-viruses, zombies, just superfluous programs and others [3] – all of them are not only viruses but also catalysts for the development of anti-virus programs. It is the “pests” that motivate developers to complicate the operating system and create algorithms to identify or eliminate the threat.

But what will happen next? If people were not interested in artificial intelligence, the answer would be very simple: new viruses and new programs would appear. Artificial intelligence is already able to diagnose human health [4]. A lot of people use electronic assistants to make their lives easier or to increase security (face recognition, text recognition) [5]. Artificial intelligence has great potential for development not only in such fields as medicine, marketing and art, but also in cyber security, although its training will be much more complex and will require power hardware. However, there are many ways to teach artificial intelligence and not all of them use the same amount of data. There are also a variety of ways to detect the virus, such as to compare the algorithm of actions, direct review of actions performed, review expert judgment or reputation, and compare the code of an unknown program with an existing database. It is possible to combine all this in one usual program, but only in theory. This software will require too much hard disk space and total machine power, which not everyone can afford. That's why the idea of teaching artificial intelligence to protect a computer from threats by yourself seems more realistic than creating a universal program.

However, this problem should be viewed from a different angle: the better the protection, the more complex the viruses become, and if the antivirus evolves to the level of intelligence, hackers will try to create a more complex program or teach their own artificial intelligence. Thus, the phrases "cyber threat" and "cyber war" may receive completely different interpretations.

СПИСОК ВИКОРИСТАНОЇ ЛІЕРАТУРИ

1) Вплив вірусу на еволюцію – [Електронний ресурс] – https://postnauka.ru/questions/155208
2) Еволюція антивірусів – [Електронний ресурс] – https://www.cezurity.com/ru/teaser/local2cloud
3) Основні види вірусних програм – [Електронний ресурс] – https://zillya.ua/osnovni-vidi-virusnikh-program
4) Як штучний інтелект змінe життя – [Електронний ресурс] – https://www.radiosvoboda.org/a/29015231.html
5) Досягнення ШІ – [Електронний ресурс] – https://umn.ua/news/4716

Монастирська Анастасія Юріївна – студентка групи 2ІСТ-20б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: monanastya.2004@gmail.com

Науковий керівник: ***Ібрагімова Людмила Володимирівна*** – старший викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: milatvin@ukr.net

Monastyrska Anastasia **–**Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: monanastya.2004@gmail.com

Ibrahimova Liudmyla V. — Senior Lecture, Chair of Foreign Languages, Vinnytsia National Technical University, Vinnytsia, e-mail: milatvin@ukr.net