

АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена удосконаленню процесів боротьби зі шкідливими програмами шляхом створення комплексного підходу до забезпечення інформаційної безпеки. В результаті аналізу визначено недосконалість існуючих систем захисту кіберпростору та ідентифіковано потребу в поєднанні кількох засобів, які спільно значно збільшують можливості користувачів (особливо превентивні) в мінімізації ризиків. В процесі виконання проєкту розроблено технологію створення системи протидії зловмисного коду та шпигунського програмного забезпечення, яка складається з чотирьох етапів та базується на кількарівневій структурі. В ході дослідження визначено також принципи правильної роботи системи: комплексність, цілісність, інтеграція, відповідальність, конфіденційність. Додатково запропоновано способи проведення оцінки її впливу на інформаційну безпеку.

ABSTRACT

According to the purpose of the research, the paperwork is devoted to improving the processes of combating malicious programs by creating a comprehensive approach to ensuring information security. As a result of the analysis, the imperfections of the existing cyberspace protection systems were determined and the need for a combination of several tools was identified, which together significantly increase the capabilities of users (especially preventive ones) in minimizing risks. During the implementation of the project, the technology of creating a system for combating malicious code and spyware was developed, which consists of four stages and is based on a multi-level structure. In the course of the study, the principles of proper operation of the system were also defined: comprehensiveness, integrity, integration, responsibility, confidentiality. Methods of assessing its impact on information security are additionally proposed.