АНОТАЦІЯ

Стецюк М. В. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2022.

Вирішення задачі підтримання постійної доступності та актуальності інформації в умовах впливів зловмисного програмного забезпечення (ЗПЗ), є однією із важливих наукових задач в сфері інформаційних технологій (ІТ), орієнтованих на побудову та подальшу експлуатацію спеціалізованих інформаційних систем (ІС).

У дисертації здійснено аналіз загроз від зловмисного програмного забезпечення та комп'ютерних атак для апаратно-програмних засобів та підтримки функціонування в них інформаційних систем в умовах впливів зловмисного програмного забезпечення. В роботі розроблено методи забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих інформаційних технологій, які покращують їх стійкість щодо впливів зловмисного програмного забезпечення та комп'ютерних атак, а також розроблено відповідні засоби і проведено з ними експериментальні дослідження.

Об'єктом дослідження є процес забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення та комп'ютерних атак.

Предметом дослідження є методи та алгоритми забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення та комп'ютерних атак.

Метою дисертаційного дослідження є покращення забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення та комп'ютерних атак.

Наукова новизна одержаних результатів полягає в наступному:

1) *вперше розроблено* метод забезпечення відмовостійкості ІТ згідно інтеграції компонентів надмірностей, який на відміну від відомих методів, надає змогу розширити можливості ІТ в частині їх адаптивності та відповідно автоматичної зміни апаратно-програмної конфігурації, що дозволяє створювати відмовостійкі ІТ щодо впливів ЗПЗ та комп'ютерних атак;

2) *вперше розроблено* метод забезпечення живучості спеціалізованих ІТ згідно аналізу маркерів та збереженої інформації для самодослідження, який на відміну від відомих методів, зберігає інформацію про ключові процеси та здійснює їх самоаналіз, що дає можливість покращити забезпечення живучості ІТ в умовах впливів ЗПЗ та комп'ютерних атак;

3) *вперше розроблено* метод забезпечення захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в поєднані із організаційними заходами інтеграцію в ІТ методів сегментування мережі, криптографічного захисту, двофакторної автентифікації програмного забезпечення, створення хибних об'єктів атаки, резервного копіювання з територіальним розмежуванням місць зберігання копій, що дозволяє створювати засоби з покращеним захистом інформації в умовах впливів ЗПЗ та комп'ютерних атак;

4) *вперше розроблено* метод забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в інтеграції в ІТ методів забезпечення відмовостійкості, живучості та захисту інформації згідно їх збігів в станах при реагуванні на впливи ЗПЗ та комп'ютерних атак, що надало змогу створювати спеціалізовані ІС з покращеними характеристиками відмовостійкості, живучості та захисту інформації до цих впливів.

Практичне значення отриманих результатів. За результатами виконаних досліджень здобувачем розроблено методи, алгоритми та засоби забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, в яких здійснено інтеграцію засобів забезпечення відмовостійкості, живучості та захисту інформації згідно їх збігів в станах при реагуванні на впливи ЗПЗ та комп'ютерних атак. Це дало змогу створювати спеціалізовані ІС з покращеними характеристиками відмовостійкості, живучості та захисту інформації до цих впливів. Дослідження методу забезпечення відмовостійкості спеціалізованих ІТ щодо показників надмірності та автоматичної зміни апаратно-програмного конфігурування дало змогу отримати покращення ефективності на 87% порівняно з спеціалізованою ІТ, в яку не було імплементовано цей метод. Крім того, в результаті проведених експериментальних досліджень з засобами, в які імплементовано розроблені методи, отримано покращені характеристики відмовостійкі, живучості та захисту інформації до впливів ЗПЗ та комп'ютерних атак, оціночні значення яких становлять окремо для спеціалізованої ІТ з імплементованим методом забезпечення відмовостійкості 76%, з імплементованим методом забезпечення живучості 72% та при інтеграції в спеціалізовану ІТ методу забезпечення відмовостійкості, живучості та захисту інформації 67%.

Теоретичні та практичні результати дослідження впроваджені при розробці компонентів ІС в бухгалтерії Хмельницького національного університету, при створенні ІТ в ТОВ «ІТТ» та ТОВ «Деймос», а також, в освітньому процесі Хмельницького національного університету на кафедрі комп'ютерної інженерії та інформаційних систем при викладанні дисциплін «Безпека та захист комп'ютерних систем», «Комп'ютерні мережі, адміністрування та кібербезпека», «Безпека та якість інформаційних систем та технологій».

У вступі представлено обгрунтування актуальності наукової задачі із забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ в умовах впливів ЗПЗ та комп'ютерних атак. Також, представлено зв'язок тематики дослідження з напрямками наукових досліджень

відомих дослідників цієї проблеми в світі та відображено основні наукові результати роботи та її практичне значення.

У першому розділі здійснено аналіз предметної області дослідження, відомих методів забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, а також здійснено постановку задачі дослідження.

У другому розділі представлено розробку методу забезпечення відмовостійкості ІТ згідно інтегрованого залучення компонентів резервування та надмірностей, який на відміну від відомих методів, надає змогу розширити можливості ІТ в частині її адаптивності та відповідно автоматичної зміни апаратно-програмної конфігурації, що дозволяє створювати відмовостійкі ІТ щодо впливів ЗПЗ та комп'ютерних атак. А також обгрунтовано його ефективність.

У третьому розділі представлено розроблений метод забезпечення живучості спеціалізованих ІТ згідно аналізу маркерів та збереженої інформації для самодослідження, який на відміну від відомих методів, зберігає інформацію про ключові процеси та здійснює їх самоаналіз, що дає можливість покращити забезпечення живучості ІТ в умовах впливів ЗПЗ та комп'ютерних атак та обгрунтовано його ефективність. Також, представлено розроблений метод забезпечення захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в поєднані із організаційними заходами інтегроване в ІТ залучення механізмів сегментування мережі, криптографічного захисту, двофакторної автентифікації програмного забезпечення, хибних об'єктів атаки, резервного копіювання з територіальним розмежуванням місць зберігання копій, що дозволяє створювати засоби з покращеним рівнем захищеності інформації в умовах впливів ЗПЗ та комп'ютерних атак.

У четвертому розділі представлено розроблений метод забезпечення відмовостійкості, живучості та захисту інформації спеціалізованих ІТ, який на відміну від відомих, полягає в поєднані та інтегруванні в ІТ механізмів забезпечення відмовостійкості, живучості та захисту інформації згідно їх збігів в станах при реагуванні на впливи ЗПЗ та комп'ютерних атак, що надало змогу

створювати спеціалізовані ІС стійкі до цих впливів та представлено архітектуру засобів, в які він імплементований та його ефективність.

У висновках представлено отримані наукові та практичні результати дослідження.

У Додатках представлено наукові публікації, в яких відображено основні наукові результати роботи, акти впровадження результатів роботи, лістинг програмного забезпечення, таблиці взаємозв'язків та блок-схеми алгоритмів.

Ключові слова: комп'ютерна система, інформаційна технологія, інформаційна система, відмовостійкість, живучість, захист інформації, зловмисне програмне забезпечення, комп'ютерні атаки, апаратно-програмні засоби.

ANNOTATION

Stetsiuk M. V. Methods and means of ensuring fault tolerance and survivability of specialized information technologies under the influence of malicious software. - Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 123 - Computer Engineering. - Khmelnytsky National University, Khmelnytsky, 2022.

Solving the problem of maintaining constant availability and relevance of information in the face of malicious software (SPR) is one of the important scientific tasks in the field of information technology (IT), focused on the construction and further operation of specialized information systems (IS).

The dissertation analyzes the threats from malicious software and computer attacks for hardware and software and supports the functioning of information systems in them under the influence of malicious software. The paper develops methods to ensure fault tolerance, survivability and information protection of specialized information technologies that improve their resilience to malware and computer attacks, as well as developed appropriate tools and conducted experimental studies with them.

The object of research is the process of ensuring the resilience, survivability and protection of information of specialized information technologies in the face of malicious software and computer attacks.

The subject of research is methods and algorithms to ensure fault tolerance, survivability and protection of information of specialized information technologies in the face of malicious software and computer attacks.

The aim of the dissertation research is to improve the resilience, survivability and protection of information of specialized information technologies in the face of malicious software and computer attacks.

The scientific novelty of the obtained results is as follows:

1) for the first time, a method was developed to ensure IT resiliency according to the integration of redundancy components, which, unlike known methods, allows to expand the capabilities of IT in terms of their adaptability attacks;

2) for the first time, a method was developed to ensure the viability of specialized IT according to the analysis of markers and stored information for self-examination, which, unlike known methods, stores information about key processes and self-analyzes, which allows to improve IT viability;

3) for the first time a method of providing information protection of specialized IT was developed, which, unlike known ones, consists in integration with organizational measures of integration of IT network segmentation methods, cryptographic protection, two-factor software authentication, creation of false attack objects, backup with territorial delimitation of storage locations. copies, which allows you to create tools with improved protection of information in the face of malicious software and computer attacks;

4) for the first time, a method of ensuring the resilience, survivability and protection of information of specialized IT, which, unlike the known ones, consists in integrating into IT methods of ensuring resilience, survivability and protection of information according to their coincidences in response to malicious software and computer attacks. the ability to create specialized IP with improved fault tolerance, survivability and protection of information to these effects.

The practical significance of the results obtained. Based on the results of the research, the applicant has developed methods, algorithms and means of ensuring resilience, survivability and protection of information of specialized IT, which integrates means of ensuring resilience, survivability and protection of information according to their coincidences in response to malicious software and computer attacks. This has made it possible to create specialized IS with improved fault tolerance, survivability and information protection against these impacts. The study of the method of ensuring the resilience of specialized IT in terms of redundancy and automatic change of hardware and software configuration allowed to obtain an efficiency improvement of 87% compared to specialized IT, which did not implement this method. In addition, experimental studies with tools that have implemented the developed methods have improved the characteristics of fault tolerance, survivability and protection of information against the effects of malicious software and computer attacks, the estimated values of which are separately for specialized IT with implemented method of ensuring resilience 76%, with the implemented method of ensuring the survivability of 72% and the integration into the specialized IT method of ensuring resilience, survivability and protection of information 67%.

Theoretical and practical results of the study were implemented in the development of IS components in the accounting department of Khmelnytsky National University, in the creation of IT in ITT and "Deimos", as well as in the educational process of Khmelnytsky National University at the Department of Computer Engineering and Information Systems "The protection of computer systems", "Computer networks, administration and cybersecurity", "Security and quality of information systems and technologies".

The introduction presents the rationale for the relevance of the scientific problem of ensuring resilience, survivability and protection of information of specialized IT in the face of malicious software and computer attacks. Also, the connection of the research topic with the directions of scientific research of famous researchers of this problem in the world is presented and the main scientific results of the work and its practical significance are reflected.

In the first section the analysis of the subject area of research, known methods of ensuring fault tolerance, survivability and protection of information of specialized IT, and also the statement of the research task is carried out.

The second section presents the development of a method to ensure IT resiliency according to the integrated involvement of redundancy and redundancy, which, unlike known methods, allows to expand the capabilities of IT in terms of its adaptability and automatic change of hardware and software configuration to create fault-tolerant IT and computer attacks. And also its efficiency is proved.

The third section presents the developed method of ensuring the viability of specialized IT according to the analysis of markers and stored information for self-examination, which, unlike known methods, stores information about key processes and self-analysis, which improves the viability of IT user attacks and substantiated its effectiveness. Also, the developed method of providing information protection of specialized IT, which, in contrast to the known, is combined with organizational measures integrated into IT involvement of network segmentation mechanisms, cryptographic protection, two-factor software authentication, false attack objects, backup with territorial delimitation copy storage sites, which allows you to create tools with an improved level of information security in the face of malicious software and computer attacks.

The fourth section presents the developed method of ensuring resilience, survivability and protection of information of specialized IT, which, unlike the known ones, is to combine and integrate into IT mechanisms to ensure resilience, survivability and protection of information according to their coincidences in response to malicious software and computer This allowed the architect to create resistant IS to these influences and presented to the architect the means in which it is implemented and its effectiveness.

The conclusions present the obtained scientific and practical results of the study.

The Appendices present scientific publications, which reflect the main scientific results of the work, acts of implementation of work results, software listing, tables of relationships and flowcharts of algorithms.

Keywords: computer system, information technology, information system, fault tolerance, survivability, information protection, malware, computer attacks, hardware and software.