UDC 335.02

Pampukha I.V., candidate of technical sciences, associate professor,
Grishin S.P., candidate of technical sciences,
Miroshnichenko O.V.,
candidate of technical sciences

MODERN PROBLEMS OF THE TECHNOLOGICAL SAFETY OF THE PROGRAMMING MEANS OF THE SYSTEM OF THE CONTROL OF THE ARMAMENT AND DEFENSE TECHNOLOGY

Software security of the complex systems for military purposes is related to the potential possibility for bringing in the software purposeful defects or special software tools that are used to focus the hidden impact on the technical or informational system, which uses computers. Therefore, an information on the possible effects of their introduction and methods of the protection from them is very important.

Key words: *technological security, information system, harmful software, resistance of the systems of modern weapons.*

Statement of the problem. According to experts, to the present situation, when the combat capability and stability of systems of modern weapons are determined by the quality and reliability of software tools (to a greater extent compared with the hardware). Software is becoming a source of vulnerability of modern defensive systems, and use of software tools in the weapons systems, battle management and communications, as well as other critical systems gives rise to a new problem-ensuring technological security software for military purposes. Even a rough analysis shows stable a significant increase in the relative fortunes of tasks and functions that are performed by using the software, compared to the hardware. Thus, to the present situation, when the combat capability and stability of systems of modern weapons to a large extent determined by the quality and reliability of software. In this regard, some Western reputable scientists have expressed opinions about what failure of software that is part of a strategic management system for combat forces and means, could potentially become a detonatorami nuclear conflict.

The purpose of the article is to highlight the main problems of technological security software for military purposes and the possible ways of solving them. Analysis of recent studies and publications said the continuous increase of requirements to the quality of the software components of modern and promising means of armed struggle, explaining this tumultuous inter-related processes computerization and intellectualization of respective systems engage. The inevitable consequence is the sudden increase in volume and complexity of software tools that are used in computers, weapons systems, automated systems, combat control and communication, support and security systems for military purposes.

For the first time such a problem has arisen in the mid 60s. While experts have created systems of information processing and management, faced with a new phenomenon. It turned out that the reliability of their functioning depends on the programs that are running at the moment on the computer. Revision or replacement of programs allowed to address some denial, though, could cause failures of another species. Now security software complex systems (primarily military) is associated with an opportunity make wilful to software defects, or special software (computer viruses, logic bombs, Trojan horses, software and etc.), which are used for covert action on the targeted technical or informational system, which uses computers. Especially a lot of inconvenience in the last time deliver computer viruses which today reaches 3 million. Therefore, information about the possible consequences of their implementation and the methods of protection from them remains very relevant. Fortunately, a large group of real viruses are harmless, that does not disturb the work of the PC. Their authors typically are high school students, college students and those who seek to improve their qualification in the field of programming. Among viruses, functioning of the computer is safe (which does not damage the file system structure), dangerous (which clog this structure) and very dangerous (which derive from the failure of the equipment). These viruses are constructed mostly by professionals. The largest damage in terms of information leakage cause kriptovìrusi, capable of penetrating a dent even in such a powerful tool, as kriptozahist. At the time of the introduction of electronic signature kriptovìrusi intercept secret keys and copy them into a specified location. Moreover, when checking the electronic signature they can cause a team to confirm the authenticity of knowingly incorrect signature. And even when you enter into the system only once, at the time of the generation of keys, the kriptovìrus leads to the creation of weak keys. For example, in the formation of key sensor-based random number using the built-in timer kriptovìrus can cause a change in testimony of the timer with the subsequent return to the initial state. As a result the keys easily uncover. Today virtually the only protection against such kriptovìrusìv-downloading information from a "clean" the media and the use of "clean" (corporate) software product. But on the other hand, even pure software product may contain software bookmarks and other software designed for output of order (failures) or to leak sensitive information.

Summary of the basic material. Malware can be very effectively applied in military use as an active element of information-cybernetic countermeasures. Thus, the higher the degree of computerization and intellectualization systems for military purposes, the greater the likelihood of the appearance of malware. So one of the modern features of the design and development of software for military purposes is the need to ensure its technological security. However, when implementing complex and multi-staged process of creating software tools in their composition may be intentionally made special malware. The developer of this software (algoritmìst, programmer, or systemotechnìk) may perform the following actions either accidentally or intentionally. The latter causes particular concern relevant intelligence. Malware can be realized in the form of several teams and have a rather complex and delicate "mechanism of activation" tuned "on conditions of real combat weapon system or on strictly certain combination of input data. These programs can be included in both general software computing systems, and special (application) software tools that implement conversion algorithm information.

In foreign technical literature is a kind of malicious software and software bookmarks are subdivided into automatic and controlled. First, as a rule, have a mechanism actuated in advance set (directly or indirectly) in terms of real combat weapons systems or military control, and the latter have the mechanism of activation which is controlled externally (for example, through electronic bookmarks). Detect the presence of program software bookmarks in the large volume and complexity is very difficult, because it can be disguised as actually existing algorithm or part of it. This is compounded by the complete uncertainty about the conditions and the time of actuation software bookmarks, as well as the lack of direct and indirect signs of its presence in the software.

Unlike common electronic objects are perfect nature that it is difficult to identified. Both of these types represent a special danger for the prospective of strategic defensive systems. The consequence of activation of malware can be full or partial violation of disability designation system, unauthorized access to the information of the automated system (passing complex remedies and differentiation of access), loss or distortion of information in special data banks and t.i. is the greatest danger they represent for the weapons systems of single combat, such as strategic missile complexes, as well as for combat management that have logical distribution channels of combat and the regular modes.

Experts from a number of countries, analyzing the likely impacts of the use of malware, have discovered that one of them may be blocking the possibility of combat weapon system of a certain class or informational system for military purposes. In other words, this means that, possessing a powerful weapon for deterrence potential enemy, can actually be an unarmed. As an illustration of this situation can lead to military conflict in the Gulf, when the multinational force operation "Desert Storm" of Iraq's air defense system was blocked for an unknown reason. As a result, the Iraq side was forced to leave unanswered bombing on its territory. Despite the lack of comprehensive information, many foreign experts have expressed belief that the computers that are part of a complex of technical means of air defense systems, who bought France contained special managed electronic bookmark that blocked the work of computing systems. If they were right, it means that since then began the phase of practical application of the new electronic and information warfare.

The problems associated with the development of software tools, begin to seriously bother the majority of countries in the world. In order to increase production and improve the quality of software in the United States from mid-1983 was initiated several programs resulting from the implementation of which was created by the UK automated programming environment that covers the entire life cycle of the software. The base served as the target program for the creation of a universal high-level programming language ADA. Thanks to its use, it became possible to have compatible development tools and support software, control its reliability and safety. According to Stephan Cejger of Rational Software Corporation, a software development on the ADA generally costs 60% cheaper, and developed the program has 9 times less defects than when using a

SI. Recent changes in the ADA standards were published in March 2007. They addressed mostly features of object-oriented programming: input interfaces passed normal for most hybrid language syntax to call the method, made a number of additions.

The Ministry of Defense of the United States in 1994 demonstrated the system software for high distributed and parallel computing systems. The technology of software with a high guarantee of reliability is required in designing the systems critical to the safety of personnel and the majority of weapons systems, and secure systems, which should be guaranteed the confidentiality and integrity of information. All this testifies to the fact that industrialized nations is extremely cautious, unlike us, relating to the use of imported information technology, suspecting the presence in them of intentional defects, that activates when a particular combination of input data (azimuth launching rockets, aircraft, specific management team) with the aim of breaking the system for military purposes. Very interesting is the fact that the American legislation had restricted the use of technical and programming tools of foreign production in favour of ensuring national security.

In the whole United States policy in the area of technology programming should be regarded as a full-blown strategy of confrontation in the information sphere, pereslìduûču global political and economic goals. It also involves the creation of one of the types of "non-lethal weapon" special means of action on the software and means of protection from similar action on his part. The complexity of modern software, military lies in the fact that in principle there is no technology to create software products without a single defect. Because no single institution-the developer does not guarantee the absolute reliability of the produced software, removing themselves of any responsibility for the consequences, which can cause defects in the programs.

The position is and what may occur situations when you cannot answer the question: are there discovered software design of intentional software, bookmark or accidental software defect even when found that activation of the software design is blocking features combat weapon system under certain conditions-from a given point in time or on a specific target (objects). This means that the author of the malware is able to avoid the full legal liability using the intricacies of developing software tools that implement features algorithms and models. In addition, a progressive tendency to import foreign software and information technologies leads to increasing reliability of import software defects of this kind.

Modern methods of anti-malware software. Currently for the detection software and random software defects by antivirus programs, signaling the presence of suspicious code in the boot sector of the disk. With the initiative static errors on discs copes disk doctor, which is included in the common set of utilities with Norton Utilities. Data integrity and validation tools on the disk type ADinf, AVZ and etc. can be successfully detect changes that are made to files software bookmarks. In addition, also effective search fragments of program code bookmarks characteristic for these sequences of zeros and ones (signatures), as well as permission only programs with known signatures. Detection of program code incarnate bookmarks is to identify signs of its presence in the computer system. These signs can be divided into the following two classes: high-the visuals and the ones that are the means testing and diagnostics.

The high-quality visual signs include feeling and observation of the user's computer system, which notes some deviations in her work (changing the composition and length of files, old files somewhere to go missing, and instead of them there are new programs begin to run slower or finish the job very quickly, or even cease to run). Despite the fact, that the idea of the presence of signs of this class seems to be very subjective, however, they often indicate problems in the computer system and, in particular, about the need to conduct additional checks the presence of software tools bookmarks testing and diagnostics. The problem of protection from software bookmarks can be considered in three fundamentally different ways: – do not allow the implementation of program bookmarks in the computer system; – reveal inherent programming bookmark; – remove the inherent programming bookmark.

When considering these options protect against software-bookmarks similar to the protection of computer systems from viruses. As in the case of fighting computer viruses, the problem is solved by means of monitoring the integrity of system and application programs that are run, as well as the integrity of the information stored in the computer system and for events that are critical for the functioning of the system. However, these funds effective only when they themselves are not affected by software bookmarks that can: to impose the final audit results; to influence the process of reading information and run programs, which are controlled; to modify the algorithms of functioning of controls. It is very important to the inclusion of controls was carried out before the commencement of the program bookmarks or when control was carried out only with the use of control programs that are of the computer system.

Interesting method of dealing with an embodiment of the software of bookmarks can be used in the information the banking system, which circulate only files-documents. To prevent the penetration of software bookmarks via the communication channels, in this system there is no admission no executable code. For recognition of the event type of the received executable code and the rece apply control over the availability of the file is forbidden characters: the file is that contains the executable code if it contains characters that are never found in the files-documents.

A specific method of removing software embodied bookmarks depends on the method of its implementation in a computer system. If it is hardware tab, then reprogram of the computer. If it's bootable, driver, application, disguised bookmark or bookmark simulator, you can replace them with the appropriate boot record, driver, utility, application or utility obtained from a source that is credible. Finally, if it is an executable software module, you can try to get the original text, remove existing bookmarks or suspicious fragments, and then re-decompensate. Universal protection against the introduction of software bookmarks is the creation of a stand-alone computer. The computer is called isolated, if the following conditions are met: it has its own type system BIOS that does not contain software bookmarks; operating system tested for the presence of bookmarks; reliably established the constancy of the BIOS and operating system for this session; the computer does not run and do not run any other programs besides those already tested for the presence of bookmarks; excluded start-tested programs in any other conditions other than those listed above, i.e., outside an isolated computer. To determine the degree of isolation of the computer model may be used speed control. Its essence consists in the following. So first we check that there are no changes in the BIOS. Then, if everything is in order, read the boot sector and operating system drivers, which in turn also analyzed make unauthorized changes. Finally, using the operating system starts the driver control call programs, which ensures that the computer starts only proven program.

Conclusions

Despite the considerable list of ways and means of dealing with malicious software that exists at this stage, the problem of providing technological security software military forces to draw attention to themselves almost daily. It should be noted that in the development of advanced models of "smart weapons" (that is when the future of computing, and intelligent systems for military use) there is an inevitable paradox of modern software, which is that the fundamental source of technological progress is simultaneously growing source of technological vulnerability. The probability of this threat in a modern setting increases dramatically due to the following factors: unification of weapon-control system, which leads, in particular, to the possibility of defeat just grouping the same type of weapons one intentional diversinet software defect or influence; mass import of computing resources, networks, information technologies and software; the imperfection of the system of procurement of military equipment; the lack of legal norms regulating features of the development of computerized and intellectualized high-precision weapons systems, fighting and supporting military systems; degradation of system development of arms and military equipment due to the difficult economic stop; changes in the cooperation of the developers of strategic defense systems and the exclusion of a certain part of the developers in the composition of the neighboring independent States; the increase in the number of individuals and organizations that may possess information weapons (including terrorist groups); the weak development of the scientific and theoretical basis on the problem of software security systems for critical applications; the creation of a global network structures or connect to them weapons systems. Disruption of the normal functioning of information systems can cause a kind of chain reaction of negative consequences, thus exacerbating the problem of security of information technologies.

LIST OF USED SOURCES

1. *Ленков С.В., Перегудов Д.О., Хорошко В.А.* Методы и средства защиты информации.-К.: Арий, 2008. – С.163-180.

2. *Ярочкин В.И.* Информационная безопасность.-М.:Международные отношения, 2000.-400 с.

3. *Азаров С.С., Хорошко В.А.* Современные модели провайдинга.-К.: ПолиграфКонсалтинг, 2006. – 98с.

4. Введение в криптографию/Под общей ред. *В.В. Ященко.* – С-Пб.: Питер, 2001.-288с.

5. *Онучин С.В.* Устройства защиты информации. Критерии выбора.-Connect!Мир связи.-1998-N 11.- С.104

6. http://it2b.ru/

7. http://kiev-security.org.ua