UDC 355.4

M. Tkachenko

Yu. Tolstonosov

S. Sovinskii

PROPOSALS FOR ENSURING INFORMATION PROTECTION DURING THE USE OF ELECTRONIC COMPUTING TECHNIQUES AT CONTROL POINTS IN MILITARY FORMATIONS

Ways of solving the issue of determining and timely implementation of early and urgent rational organizational measures to protect electronic computing equipment (ECT) objects from unauthorized access to ensure information security at the control points of the military formation were considered.

Keywords: *control points, electronic computing equipment, automated systems, operational-tactical calculations.*

Statement of the problem. During hostilities, various automated control systems and personal electronic computers are used in the created control systems of military groups at control points, which are used to perform operational-tactical calculations, process information and reference data, and perform situational analysis for timely decision-making. This expanded the scope of information circulation, which is a state and military secret[1]. In this regard, the objects of electronic computing equipment (ECE) of control points of connections (groups) are considered by foreign intelligence as potential sources of receiving secret information. It has been established that the organization of reliable information protection is significantly complicated due to the wide variety of used computer equipment, the possibilities of its remote and collective use, a significant number of users, the number of service personnel, the presence of common banks and databases, and complex information processing modes. In addition, there is a danger of deliberate destruction or distortion of data sets and software, which in turn can lead to the failure of the object or failure to perform the combat mission.

Analysis of recent research and publications.

At the time of writing this article, open publications on the subject under consideration are unfortunately lacking in Ukraine. Similar publications contain information with restricted access, and therefore are not available in the public domain.

The purpose of the article. The algorithm of actions of the personnel of the connection control point (grouping) is proposed to ensure the security of information on ECE objects and personal computers.

Presenting main material. The constant improvement of computers, the variety of their technical implementation, microprogramming and the complexity of the programs used complicate unauthorized access to computer information, at the same time complicate the organization of its reliable protection. Organizational measures to protect ECE objects from unauthorized access are regulated by governing documents [2]. It should be borne in mind that all computer equipment that is put into operation has a prescription indicating the protection measures that should be taken when processing confidential information on this equipment.

Possible sources and reasons for leakage of protected information are shown in fig. 1.

In addition, there is a danger of deliberate destruction or distortion of data sets and software, which in turn can lead to the failure of the object or failure to perform the combat mission.

For example, if a deliberate error in the coordinates of the target is made in PC ACS, then when the target is destroyed, this will result in the failure of the combat mission [3]. That is why, at this stage of the development of automated systems, the task of ensuring information security at ECE facilities is considered by the Air Defense Forces as the most important factor in increasing combat readiness.

In general, information security at ECE facilities includes:
– exposure of possible information leakage channels;
– determination of the degree of vulnerability of information in the case of detected leakage channels;
– creation of means of information protection and development of methods of their use;
– verification of the effectiveness of the created means of protection.

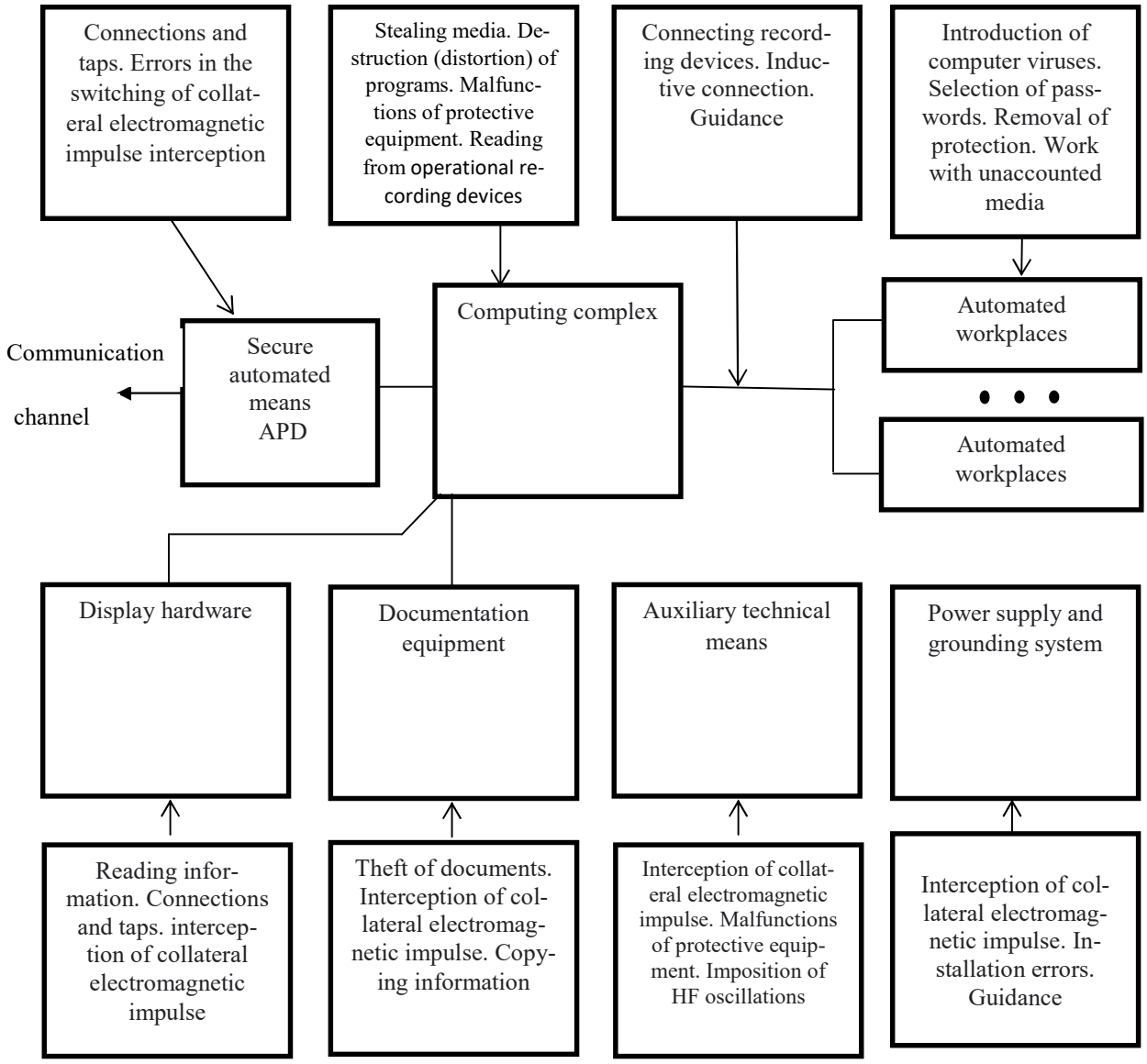

Fig. 1 – Possible sources and reasons for the leakage of information stored at the ECE facility

This security is based on the application of a complex of organizational, software (mathematical), technical and cryptographic methods [4]. Recently, personal computers (PCs) have become widely used in the practical activities of the military.

Thus, the need to ensure the preservation of information in a personal computer is determined by the following factors:
– lack of technical and software protection of information during its processing;
– the use of small removable media (magnetic disks, USB flash drives, etc.);
– the presence of non-removable magnetic media (hard disk) in certain types of machines;
– the possibility of uncontrolled reading of other people's information when working in networks;
– the propensity of computer viruses to affect information;
– lack of operating instructions for some types of personal computers (mainly foreign production).

The issue of ensuring the protection of information during the operation of personal computers in local computer networks is particularly acute, since due to the lack of reliable software and cryptographic protection means in them, additional channels of leakage of protected information arise:

– connection to the local network of third-party users;
– unaccounted copying and printing of data sets;
– creation of obstacles in the network;
– making distortions in the data set;
– destruction of a set of data and software;
– intentional or accidental introduction of viruses into the software.

The reasons for the spread of viruses in the first place are the uncontrolled copying of programs and the use of game files of foreign origin. Currently, more than 500 million "unique virus files" are known, performing various destructive functions.

Based on the analysis, actions to ensure the security of information in personal computers after their delivery can be presented in the form of an algorithm (Fig. 2). Let's explain some of its operations.

Categorization. Categorization of personal computer as an ECE object (the ECE object means electronic computing equipment together with the premises in which it is located) is carried out on the basis.

The criteria for categorization are: vulture of processed information; processing time of classified information; personal electronic computing machines placement.

For categorization, a commission is appointed, based on the results of which an act is drawn up with an attached List of ECE categorical means.

Laboratory check. Personal computers installed at ECE objects of categories 2–4 undergo laboratory checks for the presence of devices for interception (destruction) of information.

Checking the presence of a prescription. It is necessary to study the prescription for the operation of the corresponding personal computer and take all measures to ensure the security of information provided by this prescription.

Special inspection by electronic warfare authorities. The electronic warfare authorities carry out a special check of the effectiveness of the information protection measures taken, specified in the order.

Room equipment. The premises in which PCs are located must meet the requirements for premises for storing secret documents and carrying out secret work.

Compilation of forms. A form is established at each ECE facility, which includes:

– extracts from the commissioning orders and appointment of persons responsible for compliance with protective measures;
– characteristics of the ECE object;
– a scheme for placing computing equipment, auxiliary equipment, cable lines and power supply;
– data about the used programs;
– information on organizational and technical measures for the protection of information and other measures on the secrecy regime.

Development of instructions. Information security instructions are developed for each ECE facility.

This instruction sets out the duties of all officials involved in the operation of these facilities to ensure the security of information against unauthorized access, the procedure for accounting, storage of magnetic media (disks) and machine documents (printouts), as well as requirements for countering foreign technical intelligence (FTI) and other regime measures.

Organization of accounting and storage of magnetic data carriers and machine documents. All magnetic carriers of information and machine documents are subject to accounting and storage in accordance with the instructions for ensuring the preservation of state and military secrets.

Data records of flexible magnetic disks and cassettes are written on labels, which must be pasted on the cover of the disk (cassette case) and contain the following information: secrecy stamp, account number, copy number, code of the task, date of execution, signature of an employee of a secret body certified with a seal «for packages».

On magnetic tapes, credentials are printed on the ends of the tape.

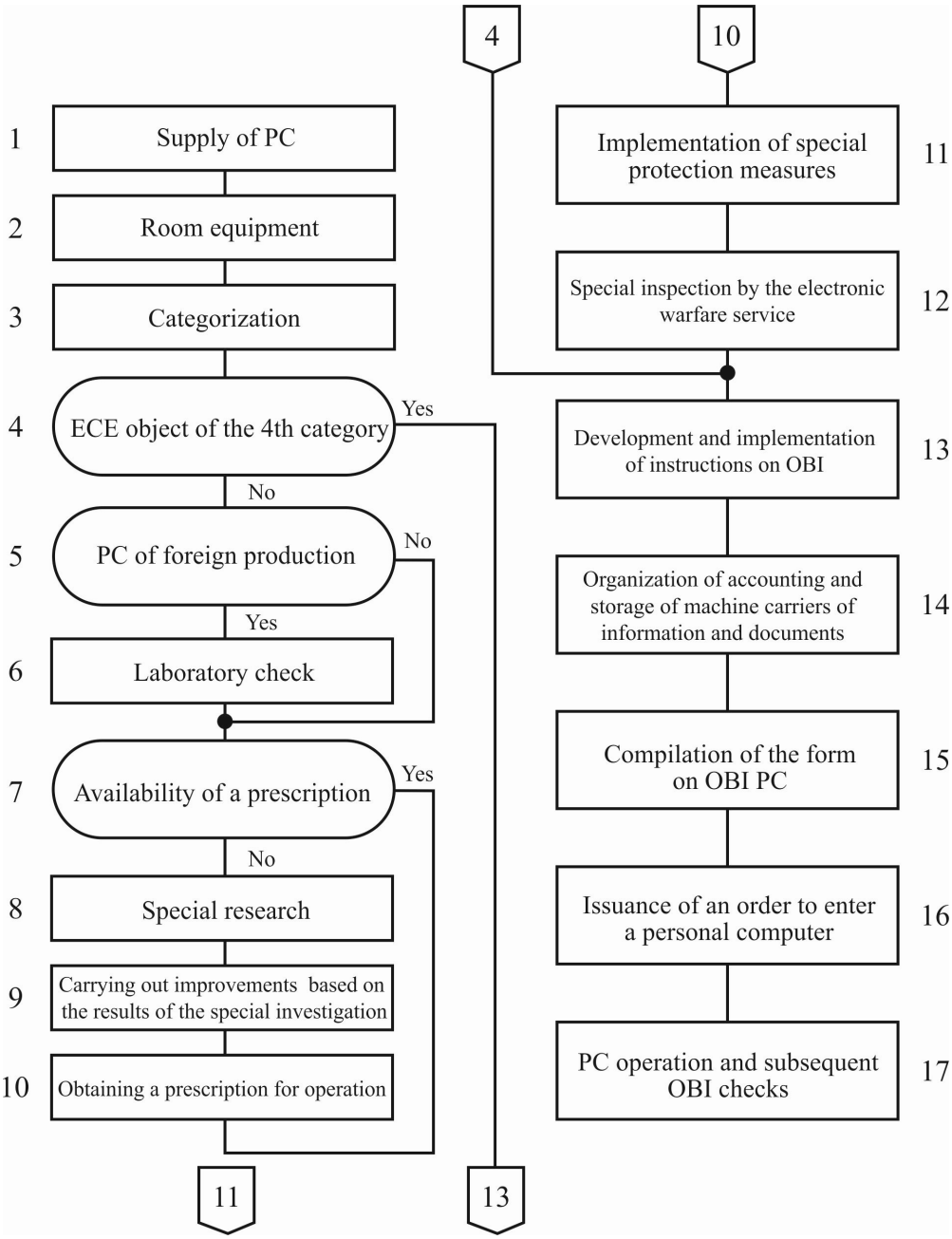

Fig. 2 – Algorithm of actions to ensure information security in personal computers

Compilation and proof of the order on putting the EOT object into operation. After the implementation of all the above protection measures related to the commissioning of the ECE object and the preparation of the relevant documentation, the head of the department (department, service) draws up an order, which determines the degree of confidentiality of the processed information, appoints the persons responsible for the operation of the personal computer and ensuring security information. By the same order, the instruction on protection of information from unauthorized access and the complex of countering foreign technical intelligence are put into effect.

The order is delivered to all personnel (employees).

It is known that the control over the presence of magnetic media and machine documents of personal computers in the process of operation is carried out according to the procedure established for all secret materials taken into account in the secret body.

In addition, every quarter and after each installation of ECE devices, the appropriate commission checks the functioning of protection devices, the quality of shielding and noise reduction, the absence of unauthorized connections and network taps. The results of the check are drawn up in an act and entered in the Information Security Form.

When PCs work in local networks, organizational and software measures must be taken to protect the network from unauthorized connections by third-party subscribers and limit the access of network subscribers to other people's information.

Thus, to ensure reliable ECE protection of air defense control points against unauthorized access by foreign intelligence agencies to processed secret information, it is necessary:

– to carry out early and immediate organizational measures to protect ECE objects;

– use methods of software encryption of information (before saving it on removable media);

– pay special attention to the application of software and cryptographic methods of information protection.

Conclusions

The question of priv from one side can be decided also, as well as for defence of traditional (paper) transmitters of information, and from the second side, the use of computer technologies of treatment of information carries new threats. In particular, it is the use of harmful and often destructive software (computer viruses). Therefore a task to the priv in the of informatively-communication systems is position of two directions:

– it is defence of important information, in particular, state, military secret, from purposeful interference;

– it is a priv from the influences, caused by the improper functioning of the computer system through the refuses of equipment, failures in-process software, error in realization of vehicle or programmatic facilities, or presence of programmatic facilities with hidden destructive.

Thus, it should be noted that only purposeful, complex application of the considered information protection methods in automated control system (ACS) and operational center (OC) allows to ensure the preservation of state and military secrets during the operation of computing equipment and automation on the control point.

References

1. Horbatyuk O.M. Current state and problems of information security of Ukraine at the turn of the century. *Bulletin of T. Shevchenko Kyiv University*. 2005. Pub. 14: International relations. P. 46–48.

2. Pylypenko O. Security Formula: Information Security. *CHIP*. 2005. No 12. P. 72–73.

3. Sidak V. S., Artemov V. Yu. Ensuring information security in NATO and EU countries: Training manual. Kyiv : KNT, 2007.

4. Ganzhelo D. About hackers, gadget protection and cyber security in Ukraine InDevLab. indevlab.com URL: http://surl.li/mcpou. Cited 2019-11-16.

Перелік джерел посилання

1. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Тараса Шевченка*. 2005. Вип. 14 : Міжнародні відносини. С. 46–48.

2. Пилипенко О. Формула безпеки: інформаційна безпека. *CHIP*. 2005. № 12. С. 72–73.

3. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: навч. посіб. Київ : КНТ, 2007.

4. Ганжело Д. Про хакерів, захист гаджетів та кібербезпеку в Украине InDevLab. indevlab.com URL: http://surl.li/mcpou (дата звернення: 16.09.2023).

The article has been sent to the editors 27.09.2023

УДК 355.4

М. Д. Ткаченко, Ю. М. Толстоносов, С. Є. Совінський

ПРОПОЗИЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ НА ПУНКТАХ УПРАВЛІННЯ У ВІЙСЬКОВИХ ФОРМУВАННЯХ

Постійне вдосконалення ЕОМ, різноманітність їх технічного виконання, мікропрограмування і складність використовуваних програм ускладнюють несанкціонований доступ до інформації ЕОМ і водночас ускладнюють організацію її надійного захисту. Організаційні заходи захисту об'єктів ЕОТ від несанкціонованого доступу регламентовані керівними документами.

Усі засоби обчислювальної техніки, які вводяться в експлуатацію, мають припис із зазначенням заходів захисту, які слід виконувати під час оброблення секретної інформації на цій техніці. Об'єкти електронно-обчислювальної техніки (ЕОТ) пунктів управління з'єднань (угруповань) розглядаються іноземними розвідками як потенційні джерела отримання таємних відомостей.

Установлено, що організація надійного захисту інформації значно ускладнюється через велику різноманітність застосовуваних засобів обчислювальної техніки, можливості її дистанційного і колективного використання, значну кількість користувачів, численний обслуговуючий персонал, наявність загальних банків і баз даних, складні режими оброблення інформації. Крім того, існує небезпека умисного знищення чи спотворення наборів даних і програмного забезпечення, що також може призвести до виходу об'єкта з ладу або до невиконання бойового завдання.

Авторами статті розглянуто проблеми і запропоновано шляхи вирішення питання стосовно визначення та своєчасного проведення запобіжних і безпосередніх раціональних організаційних заходів щодо захисту об'єктів електронно-обчислювальної техніки (ЕОТ) від несанкціонованого доступу для забезпечення безпеки інформації на пунктах управління військового формування.

Ключові слова: *пункти управління, електронно-обчислювальна техніка, автоматизовані системи, оперативно-тактичні розрахунки.*

Mykola Tkachenko – PhD (militarys ciences), associate professor, associate professor of operational art department, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0001-8478-8381

Yurii Tolstonosov – senior lecturer of operational art department, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0001-8677-5952

Serhii Sovinskii – senior lecturer of tactics and tactical special training department, Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0009-0004-4238-7589