Захист інформації

UDC 681.324

I.V. Ruban

Kharkiv National University of Radioelectronics, Kharkiv

AN APPROACH TO CYBER SECURITY SUPPORT

The article deals with the basic concepts of cyber security and cyber system and gives the basic classification of cyber system vulnerabilities. The mechanism of cyber attack is analyzed and the system model of cyber security is suggested in the article as well.

Keywords: *cyber system, cyber security, vulnerability, threat detecting, threat blocking.*

Introduction

The development of information technology has become the basis for a new area that is called "cyber security". At present, in scientific literature the term "information security" is used, but it is interpreted differently in various sources, for example as a state, process, activity, ability, guarantee system, etc., but the conception of information remains the object of security anyway.

To understand the phenomenon of cyber security it is reasonable to consider the main concepts of cybernetics and a cyber system.

The term *cybernetics* is derived from the Greek word *Κυβερνητική* that means "the art of control" [1]. In terms of [2, 3] cybernetics was developed as the science about general laws of control processes and information transfer in machines, living organisms and society and is an interdisciplinary science that covers a great number of areas such as system theory, information theory, decision making, pattern recognition, system analysis, optimal control methods. Due to its interdisciplinary content, cybernetics considers all controlled systems as the objects of control, and automated systems take the main place among them. This fact defines the task of control as the most important one for researching and developing.

The article is intended to consider the fundamental concepts of cyber security and the approach to its evaluation.

1. Cyber system

Generally, a control process comprises the following stages:

1) data collecting and processing (systematization, analysis, etc.);

2) compiling the set of goals, selecting and implementing specific method of control;

3) checking and assessing the efficiency of control.

The realization of these three stages enables converting the controlled system from one state to another by means of control action to achieve the stated goal effectively in the process of system operation.

Up-to-date means of information security are aimed at ensuring privacy, integrity and availability of data. If, in general terms, the threat to information security is interpreted as a possible hazard to information resources that harms an owner or user, then for cyber systems the main task of security is to ensure the continuity and accuracy of control and operation process.

Grounding on the facts mentioned above, it is possible to state that cyber security as a separate science is aimed at researching problems of opposing unauthorized impact upon the process of system operation and control.

Such systems can be subdivided into three main groups – engineering, social and social and engineering. This subdivision in the terms of cyber security is conditional, and all controlled systems can be considered as social and engineering or cyber systems. It is true not only due to a human being who participates in the process of control, but also because a cyber attack is the realization of a threat by means of the system subject with the use of vulnerability of computer subsystem for updating control actions to violate the operation process.

Cyber security considers automated systems of engineering process control as the most important as these systems include systems of power generation control and transportation control. The attacks aimed at these systems can cause serious consequences up to anthropogenic disaster. The use of *Stuxnet* computer virus can be referred to as an example. This first known worm was developed to attack automated control systems of engineering process control; it intercepted and modified the control flow among *Simatic S7* programmable logic controllers and *Simatic-WinCC* work stations of *Siemens* SCADA-system [4].

2. Cyber attack mechanism

The mechanism of this virus action consists of the following stages:

1) infecting system through USB-flash-memory;

2) searching goal software and equipment produced by Siemens;

3) taking control;

4) disabling equipment.

The virus uniqueness lies in the fact that it was the first one that physically affected engineering control process and destroyed the infrastructure (Fig. 1).

Thus, the worm can be used as a subversive tool to destroy equipment in cyber system.

3. Cyber system vulnerability

To understand the tasks of cyber security support integrally, it is reasonable to consider general vulnerabilities of a cyber system (Fig. 2).

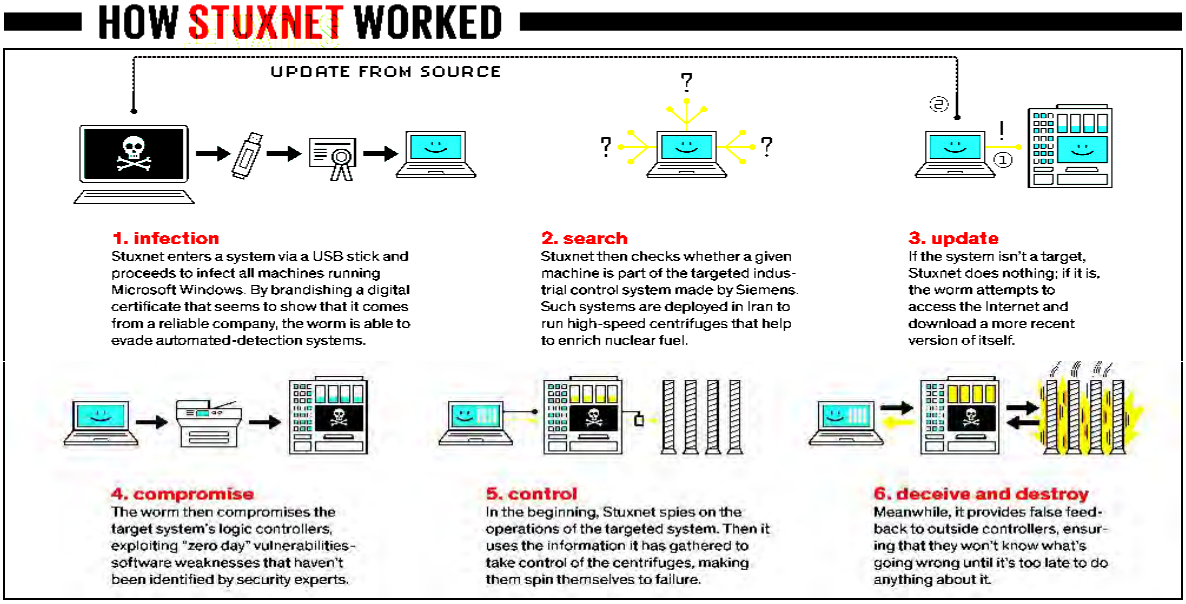

Fig 1. *Stuxnet* action mechanism [5]

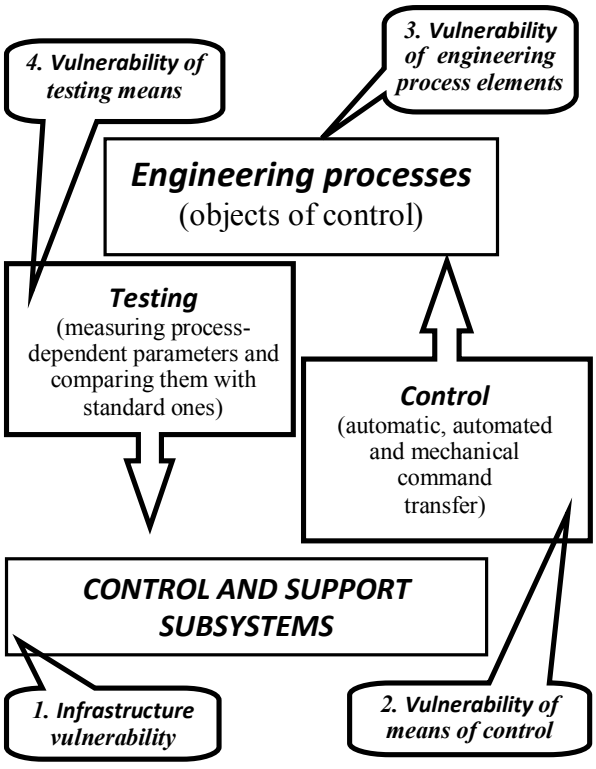

Fig. 2. Vulnerability of cyber system

Infrastructure vulnerability is caused due to the strong environmental impact (for example remote operation, availability of the Internet) or because of deep mutual integration of subsystems (the use of cross-platform developments) as well as due to the high level of confidence among the subsystems of the infrastructure.

Vulnerability of means of control, elements of engineering process and testing means are determined by the openness of technologies of cyber system firmware (means of programmed logic control, execution units, and protocols of engineering networks).

This conception does not enable structuring vulnerabilities and threats, and it is not possible to develop the general classification of vulnerabilities on the basis of heterogeneous, multitasking and structurally complex cyber systems.

4. The model of cyber security level control

One of the tools for developing the model of cyber security for complex system is the decomposition of complex systems on the basis of "process approach" [6]. This approach enables describing all main processes, excluding duplicating functions, unifying technology and developing the levels of cyber system monitoring, which include:

– the level of environmental interaction;

– the level of processes (the interaction of subsystems);

– the level of subsystem;

– the level of object.

As a result of such decomposition the model of cyber security level control is suggested (Fig. 3).

On the basis of this model the tasks of cyber security support on each level are determined.

Cyber security support of the environmental interaction level consist in detecting and blocking threats

directed to the change of input and output parameters and interfaces of interaction with the environment. Therefore, the state of cyber security on the environmental interaction level is determined by the ability to check and find the violations in data communications, remote access authorization, and input and output parameters of the system.

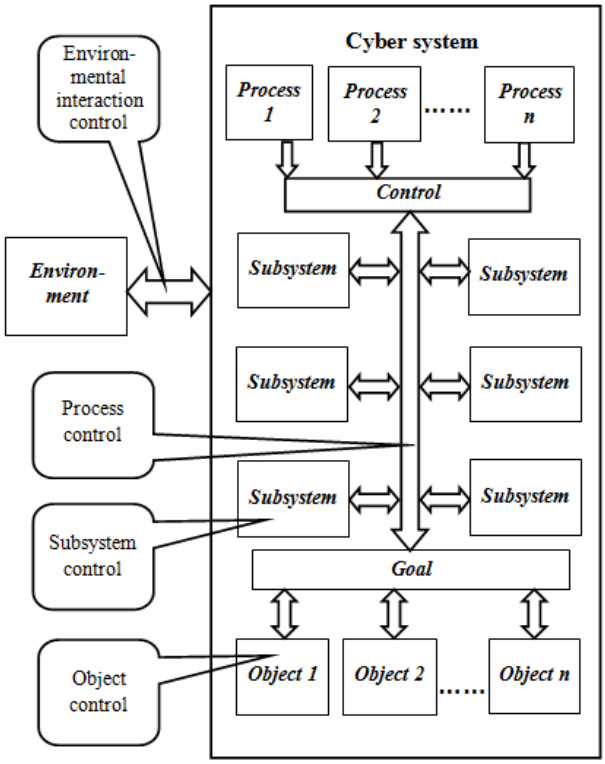

Fig. 3. The model of cyber security level control

Cyber security support on the engineering processes level consists in detecting and blocking threats directed to the change of time and engineering parameters of the operating process. Therefore, the state of cyber security is determined by the ability to control the set of operating features and the character of interrelations among the processes and subsystems at the moment, and to detect and block the anomaly as early as possible.

Cyber security support on the subsystem level consists in detecting and blocking threats directed to the change of time and engineering parameters of the process of subsystem operation. Therefore, the state of cyber secu-ity on the subsystem level is determined by the ability to control the set of operating features, subsystem parameters, and to detect and block the anomaly as early as possible.

Cyber security support on the object level consists in detecting and blocking threats directed to the change of the state of a controlled object. Therefore, the state of cyber security on the object level is determined by the ability to control the set of controlled object states.

Developing the system of factors, criteria and methods based on the generalization enables creating the systems of cyber security which can oppose attacks within the whole control cycle.

Conclusion

In the terms of suggested decomposition, the general task of cyber security support consists in minimizing the possibilities of arising anomaly which disturbs the processes of operation and control on the basis of constant monitoring the states of four levels (environmental interaction, subsystem interaction, subsystem operation, and object operation) to find vulnerabilities and block threats.

Lisi of references

1. Словарь по кибернетике / Под ред. В.С. Михалевича. – К.: УСЭ, 1989. – 751 с.

2. Энциклопедия кибернетики / Под ред. В.М. Глушкова. – К., 1974. – Т. 1. – 440 с.

3. Wiener N.. Cybernetics or Control and Communication in the Animal and the Machine / N. Wiener. – Paris, The Technology Press, Cambridge, Mass, 1948).

4. Rootkit.win32.stuxnet.a [Electr. resource]. – Accessed to: https://w.securelist.com/ru/descriptions/rootkit.win32.stuxnet.a.

5. The Real Story of Stuxnet [Electr. resource]. – Accessed to: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

6. Информационные технологии организационного управления сложными социотехническими системами / О.Е. Федорович, Н.В. Нечипорук, Е.А. Дружинин, А.В. Прохоров. – Х.: НАУ "ХАИ", 2004. – 295 с.

Надійшла до редколегії 19.05.2015

Рецензент: д-р фіз.-мат. наук, проф. С.В. Смеляков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

І.В. Рубан

Розглянуто базові поняття кібернетичної безпеки, кібернетичної системи. Наведено базова класифікація вразливостей кібернетичної системи, проаналізовано механізм кібернетичної атаки і запропонована системна модель кібернетичної безпеки.

Ключові слова: *кібернетична система, кібернетична безпека, вразливість, виявлення загроз, блокування загроз.*

ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

И.В. Рубан

Рассмотрены базовые понятия кибернетической безопасности, кибернетической системы. Приведена базовая классификация уязвимостей кибернетической системы, проанализирован механизм кибернетической атаки и предложена системная модель кибернетической безопасности.

Ключевые слова: *кибернетическая система, кибернетическая безопасность, уязвимость, выявление угроз, блокирование угроз.*