International Journal of Engineering & Technology, 7 (3.14) (2018) 276-282

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Management of Rectification of the Consequences of an Emergency Situation

Andrey Klimentevich Chernykh[1], Sergey Arkadyevich Nefedyev[1], Evgenij Nikolaevich Bardulin[1], Vladislav Pavlovich Andreev[2,] Olga Vladimirovna Stashevskaya[3]

[1]Saint Petersburg University of State Fire Service of EMERCOM of Russia, 149 Moskovskiy Ave., Saint Petersburg, 196105, Russia
[2]Saint Petersburg University of Ministry of Internal Affairs of Russia, 1 Pilotov St., Saint Petersburg, 198206, Russia
[3]Saint Petersburg State Technological Institute (Technical University), 26 Moskovskiy Ave., Saint Petersburg, 190013, Russia

Abstract

The purpose of the paper is to develop an information technology used to implement operational and quality management of rectification of the consequences of an emergency situation. Typical examples are given of malicious programs and the ways of their impact on the work of computers used to develop solutions for the elimination of the consequences of an emergency situation. To prevent unauthorized access to computers and their infection with malicious programs, preventive measures are recommended. The novelty of the paper is the development of an information technology to recover the encrypted or blocked by malicious programs data necessary to develop solutions for the elimination of the consequences of an emergency situation and the concept of building a fragment of an information system within which this information technology should be implemented. The authors consider an approach to the improvement of the information system for officials of the management bodies of the Ministry of Emergency Situations of Russia, developing a solution for the relief of the consequences of an emergency situation, which provides the protection of their personal computers from malicious programs.

Keywords*: emergency situation, decision for emergency response, information systems, information threats, unauthorized access, information protection, malicious programs.*

1. Introduction

In accordance with the information security doctrine of the Russian Federation [1], it is especially important to protect data received from the regional computer networks by officials of the Russian Emergency Situations Ministry management bodies, in a region where it is necessary, in real time, to make decisions concerning rectification of the consequences of an emergency situation. Also, a rather topical problem is the problem of operational application of information systems used in making a decision for the rectification of consequences of an emergency situation in the conditions of reliable data acquisition for these information systems.

A significant number of publications are devoted to the problem of information security, for example [2-7]. In this connection, it is necessary to characterize the main information threats for personal computers (local computer networks) of the officials of the management bodies of the Ministry of Emergency Situations of Russia which develop a solution for the relief of the consequences of an emergency situation and the measures to eliminate these threats.

Harmful actions directed at the personal computers of these officials, carried out by unauthorized persons, making it difficult to use data from the regional computer networks necessary to develop a solution for the relief of the consequences of an emergency situation, may lead to a lack of promptness in the management of these processes [8-10].

In this connection, it is important to develop ways to combat malicious programs that block the operation of the computers of the officials of the Russian Emergency Situations Ministry management bodies or encrypt data on them necessary to develop a solution for curing the effects of an emergency situation.

The most typical example of such programs is the Trojan program GPCode. This program, when a computer is infected, establishes a connection to the server and downloads a public RCA key to the computer, by which it encrypts some data on it. For a subsequent computer that will be infected, a new unique key is created. Accordingly, the private keys for decrypting the files will only be possessed by the initiators of the infection of the computer. According to the estimates by Kaspersky Lab, the number of unique IP addresses of victim computers from which requests for domains with sinkhole servers were received was 2,764 in more than 30 countries [11]. In recent times, such malicious programs began to occur less frequently, as they ceased to be an unexpected "surprise" for the officials of the Russian Emergency Situations Ministry management bodies, who are already familiar with the appropriate measures that must be taken to solve the arising problems; so new malicious programs and their modifications appear: only in 2016 there appeared 62 new families of such programs and about 40 thousand of their modifications [11].

It should be noted that the saboteurs (hackers) began to use more and more sophisticated methods of infection, for example, a malicious code in the form of analytical scripts on the sites of scientific organizations to infect the devices of the site visitors or quite legal software: administration tools, utilities for automating the solution of various problems.

For example, in 2016, some new malicious software of the PowerWare series was identified [12], which used the Microsoft Office application and the PowerShell utility included in the Windows operating system. PowerWare is loaded by a Word docu-

ment with macros. Macros are used to create and run the cmd.exe file, which activates the PowerShell utility with options that load the malicious PowerWare code.
Especially dangerous are the services that appeared in 2015, working according to the Raas model ("extortion as a service"), which allow any user who does not even have proper education to register for such services and begin distributing Trojan malware. The danger lies in the fact that the "services" of these servers can be used by technically unprepared saboteurs whose actions can lead to the inability to recover information in the event of infection. An example of such a service is the Satan service, located in the anonymous network The Onion Router, known by the abbreviation "Tor".

2. Methods

To prevent unauthorized access to a personal computer and the risk of losing confidential information or infecting computers with malicious programs, the following preventive measures should be observed first.
1. Use the services of a reliable Internet service. Protection of the data of officials of the Russian Emergency Situations Ministry management bodies is impossible without taking appropriate measures from the Internet services used to develop a solution for the emergency response. Current protection methods are not always sufficient, although some services have started taking additional measures to protect their users, for example, encryption of data transferred among their own servers.
2. Do not use cloud storage as a backup storage of private data. First, the information placed in the "cloud" is in practically free access to the developers of the service. Secondly, after a hacker attack on a "cloud" service that does not have enough reliable protection against hacking, the data can be stolen or destroyed.
3. Use the basic method of protecting a personal computer: installing a reliable anti-virus program that can prevent infection. Modern antivirus products have an intrusion prevention system that blocks even unknown versions of Trojans, preventing them from entering the system. For example, when GPCode attacks during receiving a spam letter with an attached malicious DOC file, Trojan-Dropper.MSWord.Tored.a is detected. The component that loads GPCode on the computer is identified as Trojan-Downloader.Win32.Small.crb. The GPCode itself is detected by an antivirus. Work without anti-virus protection, especially with files from questionable sources, may result in irretrievable loss of information. The main function of the anti-virus program, Monitoring of activity, should always be turned on.
4. Regularly create backup copies of data, preferably on other devices.
5. Timely update the software on the computer. First of all, this applies to updates for the installed operating system, for application security systems in the operating system and the tools for removing malware. Updates enhance the compatibility of software installed on the computer, fix bugs and vulnerable fragments of the operating system.
6. Keep confidential information separate from other data.
7. Do not use open Wi-Fi networks in public places. If necessary, one can use only those network names and passwords that are provided by administrators of these locations. When visiting sites where one is not sure about proper protection, in the settings, it is recommended to select the "Always use a secure connection" (HTTPS) option.
Note that if an official of the Russian Emergency Situations Ministry management bodies nevertheless became a victim of a malicious program and the data on his/her computer turned out to be encrypted, one needs to access the No More Ransom site from an uninfected computer. In July 2016, the National Police of the Netherlands, Europol, Intel Security and Kaspersky Lab created a noncommercial "No More Ransom" project to help restore the data blocked by malicious software.
Besides, Kaspersky Lab specialists have created their own utilities XoristDecryptor (Fig.1) and RectorDecryptor to combat these programs.

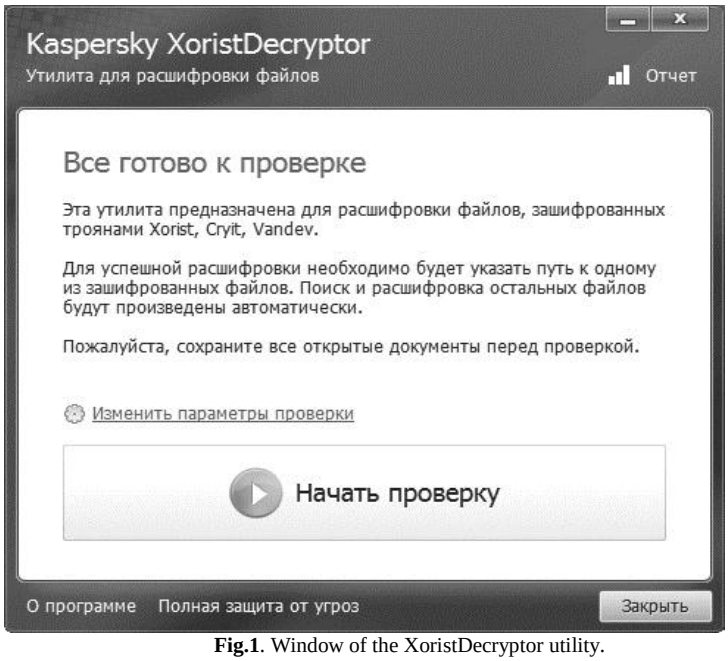


Fig.1. Window of the XoristDecryptor utility.

If launching of the utilities does not yield a result, the malicious file will be sent to the Kaspersky Lab's mail, where it will be examined by specialists and after the solution is found for its neutralization it will be included in the database. Restarting utilities should eliminate infection.
The cases of computer blocking by banners with the requirement to send SMS for obtaining the unlock code are less dangerous; and, as a rule, experienced officials of the Russian Emergency Situations Ministry management bodies can independently unlock their computer. It should be noted that in such cases there is no universal solution. Since the saboteurs constantly modify the malicious code, the solutions for its neutralization depend on each specific case of infection.

In all cases of infection, virtually the entire computer is blocked, including the Start button and the Task Manager program.

3. Results

The authors propose the following information technology, which should be implemented in the framework of the information system used by officials of the Russian Emergency Situations Ministry management bodies in making a decision to cure the effects of an emergency situation, to restore the blocked data on the computer of one of the officials.

1. Reboot the computer in safe mode and try to roll back the system. It rarely helps. Try to activate the task manager (when loading, quickly press ctrl + alt + delete) before the banner starts. If it works, select the Processes tab in the Task Manager program and terminate new unfamiliar processes. Try to determine the name of the banner process (activate some processes and see what it leads to, if there is no banner – reboot, etc.). After determining the name of the process, perform a search on it throughout the computer. In this case, one should activate the displaying of hidden files. Delete the found banner files. Next, activate the Run command (Windows + R) and enter the msconfig command in the dialog window that appears. Select the Startup tab (Fig.2). Check the properties of the activated programs: name, publisher and the degree of influence of activity. Disable suspicious unfamiliar programs. Remember the name and location of their files. After they are uninstalled, restart the computer.

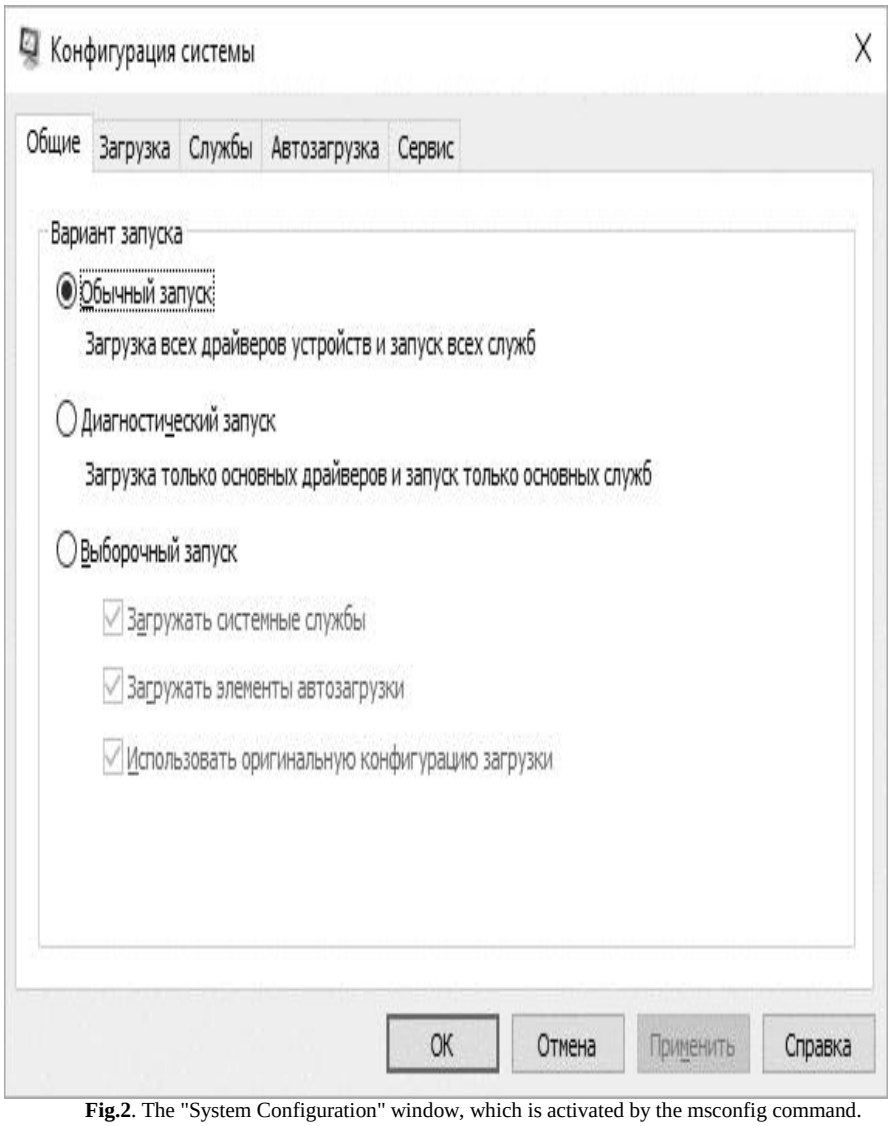


Fig.2. The "System Configuration" window, which is activated by the msconfig command.

2. To unlock the Task Manager and the system registry editor, one can use special unlocker programs, for example, a portable version of Winhelper. The program runs on top of various banners (the "Over all windows" mode). The "Restore" tab will help to restore the registry editor, the shell explorer.exe. In addition, in the "Startup" tab one can view all running programs.

3. An efficient way to unlock a personal computer is to use boot programs, for example, WinDoza Live CD & USB, containing tools to restore the operating system after it is blocked by the banner.

4. In the framework of one of the easiest ways to get rid of the Trojan-blocker, it is necessary to contact, from an uninfected computer, the database of unlock codes "Doctor Web" at https://www.drweb.com/xperf/unlocker/?lng=ru and, using a special form, find the unlock code of the computer by the purse number, phone number or banner image (Fig.3).

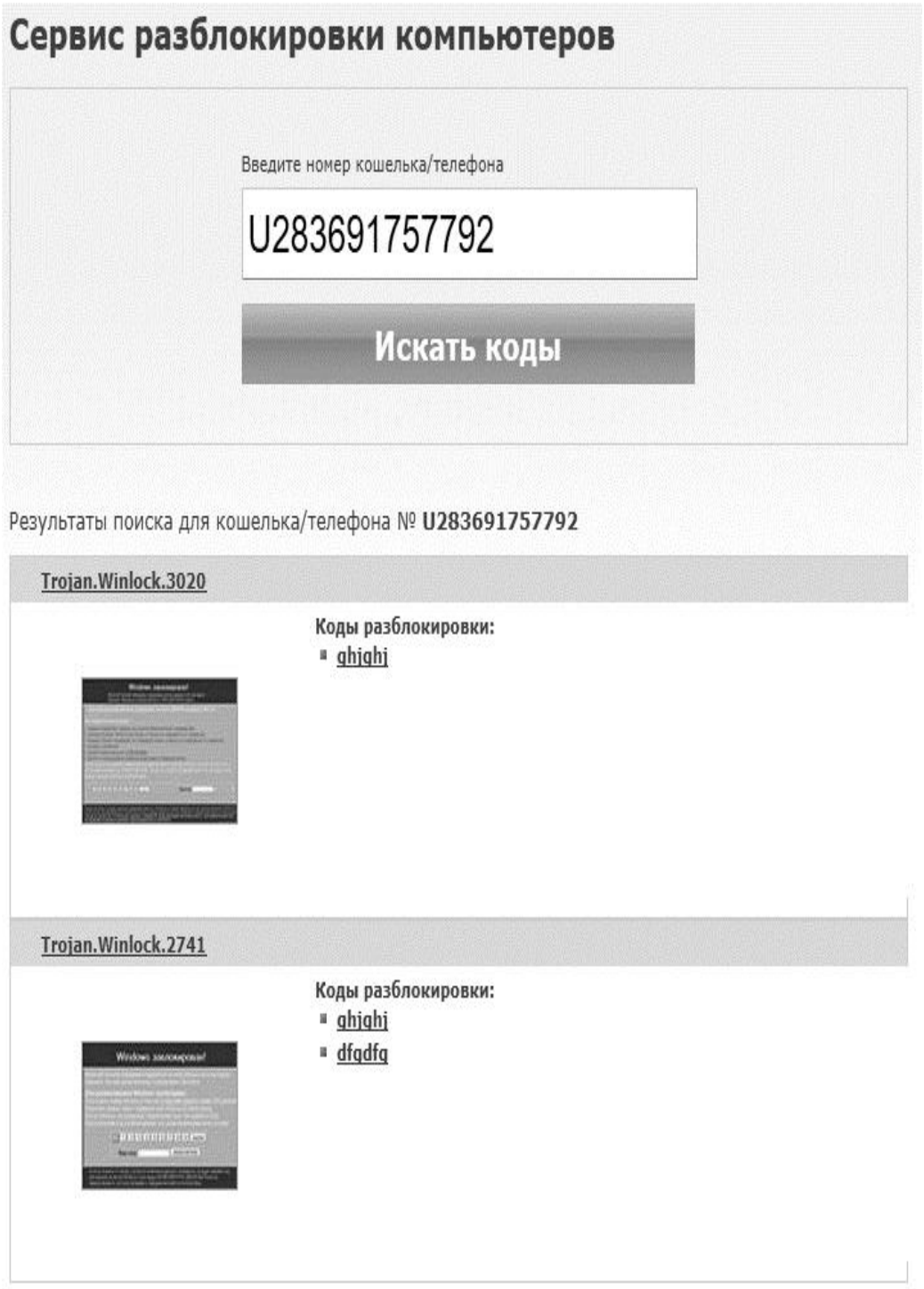


Fig.3. "Doctor Web" Unblocking Service Window.

Note. It is important to note that one should not limit oneself to unblocking the computer, it is also necessary to remove traces of the Trojan found.

4. Discussion

Based on the analysis of numerous publications devoted to the problem of information security [13-17], in addition to the proposed information technology, let us formulate the conceptual principle of constructing such a fragment of the information system, the use of which, in the condition of harmful impact on the computer of the officials of the Russian Emergency Situations Ministry management bodies, minimizes the probability of blocking information necessary for the implementation of the current accounting module of the information system that prepares the initial data for making decision on the rectification of consequences of an emergency situation and the obtaining the results of calculations of the system. It should be noted that the efficiency of the constructed information system, calculated according to the approaches indicated in [18-19], practically does not decrease.

The idea here is that the information for the specified information system is converted to a form that can be used for a different sequence of the modules inclusion in the calculation scheme. The diagram of the automated formation of the configuration of the structure of the calculation modules in order to sequentially connect the information necessary to solve each of the calculation modules of the information system is shown in Fig.4.

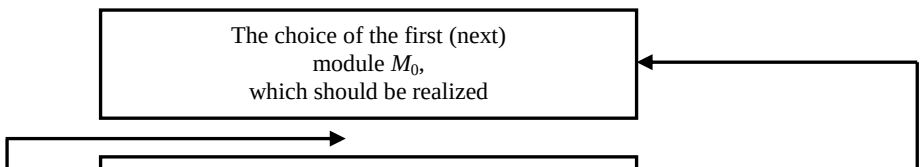


Fig.4. The scheme of automated formation of the configuration of structures of the calculation modules.

As an explanation to Fig.4, let us note that the link between the module M_{ij} and the module M_0 (Block 3, Fig.4) is defined as a group of equations of the form:

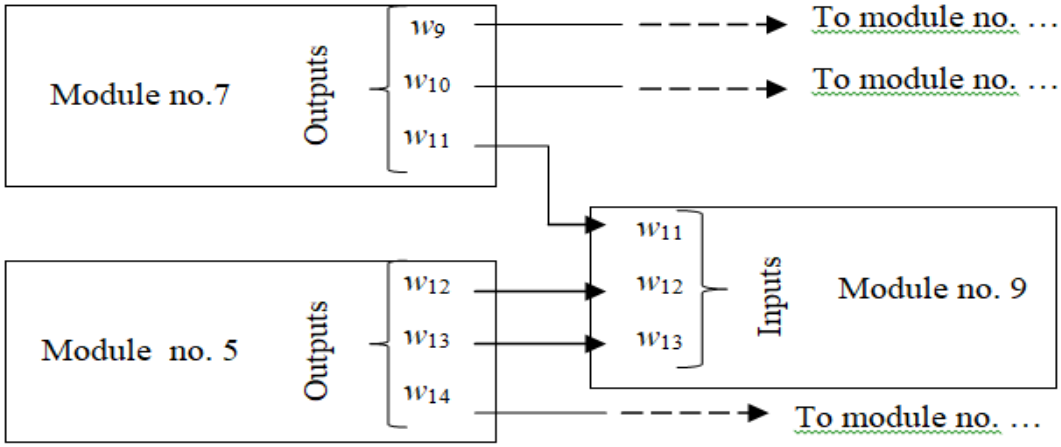
$v_k = w_k \quad k = \overline{k_o, k_n}$ (Fig.5),

where v_k is the identifier of the *k*-th input parameter of the module M_0; w_k is the identifier of the *k*-th output parameter of the module M_{ij}; $[\kappa_o, \kappa_n]$ is the interval of changing of identifiers.

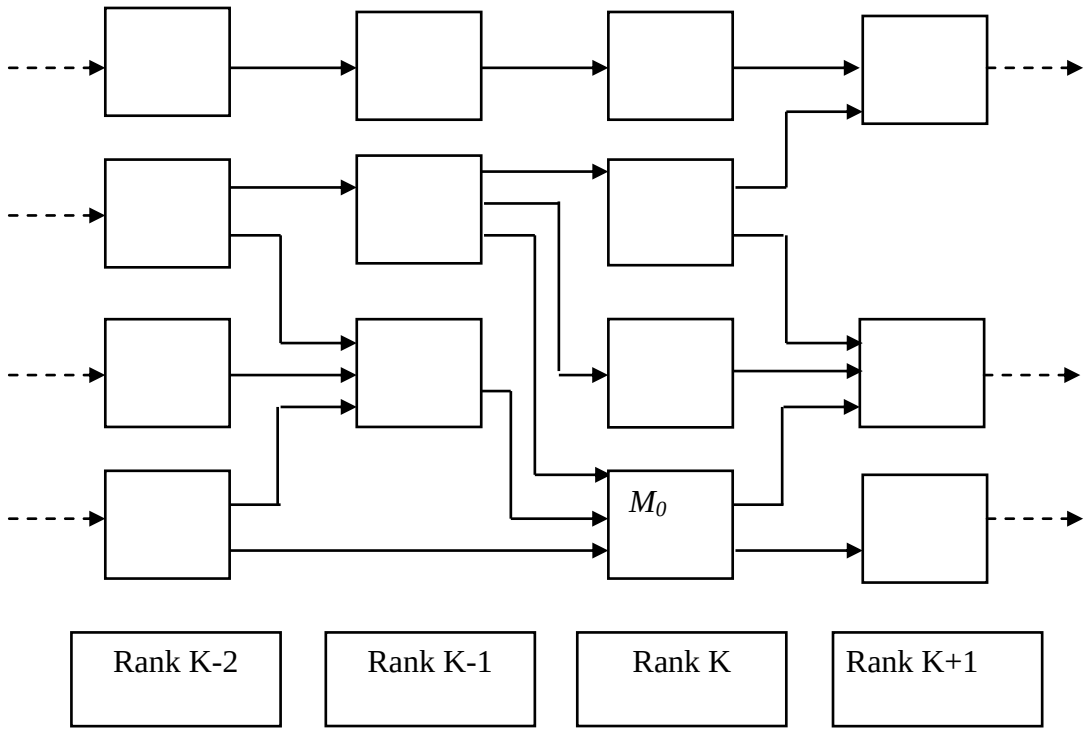
The choice of a new module $M_{ij} \in \{MN\}$ for the role of the module M_0 (Block 11, Fig.4) is carried out according to the rule:

$$M_0 = \max_i \{M_{ij} \in \{MN\}\}$$,where

$\{\{MN\}: M_{ij}, i = \overline{k-1,1},\ j = \overline{1,n}\}$, *n* is the number of modules.



a) Isomorphism relation between the input and output information of modules



b) Ranking of modules

Fig.5. Fragment of the structure of the model.

5. Conclusion

Thus, in the article, analyzing the examples of the impact on the computers, used to develop solutions for the rectification of consequences of an emergency situation, by malicious programs, the authors propose:
- an information technology for recovering the necessary data encrypted or blocked by the malicious program;
- a conceptual approach to the construction of an information system, the use of which, in the condition of harmful impact on the computer of an official of the Russian Emergency Situations Ministry management bodies, allows minimizing the probability of blocking the information necessary for the implementation of the calculation modules of the information system;
- the procedure for the automated construction of the structure of calculation modules, based on the above principle, in the framework of implementation of the decision-making and management processes of relieving the consequences of an emergency situation.

In terms of the prospect of further research on this subject, it should be noted that this approach to the construction of fragments of information systems, similar to the one proposed in the article, should be implemented on the basis of distributed computing in the management of rectification of the consequences of an emergency situation on the network of transport communications in a region affected from an emergency situation, for example, when controlling the movement of road transport [20-22].

References

[1] Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [The Doctrine of Information Security of the Russian Federation]. Approved by the Decree of the President of the Russian Federation No. 646.

[2] Kod bezopasnosti. SZI ot NSD Secret Net [Security Code. Means of Protecting Information from Unauthorized Access by Secret Net]. http://www.securitycode.ru/products/secret_net/. Accessed June 27, 2018.

[3] SZI ot NSD Dallas Lock. Dallas Lock 8.0-K [Dallas Lock − Means of Protecting Information from Unauthorized Access. Dallas Lock 8.0-K]. https://www.dallaslock.ru/products/szi-nsd-dallas-lock/. Accessed June 27, 2018.

[4] A.V. Barabanov, A.S. Markov, V.L. Tsirlov, Metodicheskii apparat otsenki sootvetstviya avtomatizirovannykh sistem trebovaniyam bezopasnosti informatsii [Methodological Apparatus for Assessing the Compliance of Automated Systems with Information Security Requirement], Spetstekhnika i svyaz 3 (2011).

[5] M.P. Chaplygina, Metodika kontrolya zashchishchennosti avtomatizirovannoi sistemy obrabotki konfidentsialnoi informatsii ot nesanktsionirovannogo dostupa k informatsii [The Methods for Controlling Security of an Automated System for Processing Confidential Information from Unauthorized Access to Information], Molodoi uchenyi 4 (2016) 166-169. https://moluch.ru/archive/108/26137/. Accessed June 27,2018.

[6] K.E. Klimentyev, Kompyuternye virusy i antivirusy. Vzglyad programmista [Computer Viruses and Antiviruses. The View of the Programmer], DMK Press, St. Petersburg, 2013.

[7] V.F. Shangin, Informatsionnaya bezopasnost i zashchita informatsii [Information Security and Information Protection]. DMK, Moscow, 2014.

[8] V.G. Anisimov, A.A. Selivanov, E.G. Anisimov, Metodika otsenki effektivnosti zashchity informatsii v sisteme mezhvedomstvennogo informatsionnogo vzaimodeistviya pri upravlenii oboronoi gosudarstva [Method of Assessing the Effectiveness of Information Protection in the System of Inter-Agency Information Interaction in the Management of the State Defense], Informatsiya i kosmos 4 (2016) 76-80.

[9] V.V. Balyasnikov, Yu.V. Vedernikov, Model prichinnogo analiza na osnove ispolzovaniya dannykh ob osobykh situatsiyakh [Model of Causal Analysis Based on the Use of Data on Special Situations], Voprosy oboronnoi tekhniki, Seriya 16: Tekhnicheskie sredstva protivodeistviya terrorizmu 1-2 (2015) 31-38.

[10] V.G. Anisimov, E.G. Anisimov, Risk-orientirovannyi podkhod k organizatsii kontrolya v podsistemakh obespecheniya bezopasnosti informatsionnykh sistem [Risk-Oriented Approach to the Organization of Control in the Subsystems to Ensure the Security of Information Systems], Problemy informatsionnoi bezopasnosti, Kompyuternye sistemy 3 (2016) 61-67.

[11] Ivanov, D. Emm, F. Sinitsyn, S. Pontiroli. Kaspersky Security Bulletin 2016. Syuzhet goda. Programmy-vymogateli: revolyutsiya [Kaspersky Security Bulletin 2016. The Plot of the Year. Extortion Programs: Revolution]. https://securelist.ru/analysis/ksb/29788/kaspersky-security-bulletin-2016-story-of-the-year/. Revised December 21, 2016. Accessed June 27, 2018.

[12] M. Sconzo, R. Valdez. Advanced Threat Protection, Detection and Response, Endpoint and Server Security, Prevention, Ransomware, Response, Tech Toolbox. Carbon Black. https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/. Revised March 25, 2016. Accessed June 27, 2018.

[13] N.N. Moshak, K.V. Evseiko, A.V. Logintsev, Problemy zashchity informatsionno-telekommunikatsionnoi infrastruktury RF ot kiberatak [Problems of Protection of the Information and Telecommunications Infrastructure of the Russian Federation from Cyberattacks], Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik nauchnykh trudov [Regional Informatics and Information Security. Collection of Scientific Papers], St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, St. Petersburg, 2017, 31-36.

[14] O.Yu. Piyukov, I.V. Gvozdkov, Obespechenie bezopasnosti informatsionnykh resursov obrazovatelnykh uchrezhdenii [Ensuring the Security of Information Resources of Educational Institutions], Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik nauchnykh trudov [Regional Informatics and Information Security. Collection of Scientific Papers], St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, St. Petersburg, 2017, 44-46.

[15] A.V. Shipilova, Modelirovanie uyazvimostei v sisteme bezopasnosti [Modeling of Vulnerabilities in the Security System], Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik nauchnykh trudov [Regional Informatics and Information Security. Collection of Scientific Papers], St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, St. Petersburg, 2017, 74-77.

[16] V.I. Kuvatov, A.I. Primakin, (2017). Model formirovaniya trebovanii k konfidentsialnosti, tselostnosti i dostupnosti dannykh v sisteme zashchity informatsii sredstv vychislitelnoi tekhniki i avtomatizirovannykh sistem [Model of Formation of Requirements to Confidentiality, Integrity and Availability of Data in the System of Information Protection of Computer Facilities and Automated Systems], Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik nauchnykh trudov [Regional Informatics and Information Security. Collection of Scientific Papers], St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, St. Petersburg, 2017, 122-126.

[17] V.A. Bogatyrev, S.V. Bogatyrev, Funktsionalnaya nadezhnost i ustoichivost vychislitelnogo protsessa [Functional Reliability and Stability of the Computational Process], Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik nauchnykh trudov [Regional Informatics and Information Security. Collection of Scientific Papers], St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, St. Petersburg, 2017, 131-133.

[18] A.V. Flegontov, A. Chernykh, P. Klykov, The Evaluation of the Efficiency of Control Systems for Organizational Systems, 2015 International Conference on "Stability and Control Processes" in Memory of V.I. Zubov, Proceedings, 2015, 558-559. DOI: 10.1109 / SCP.2015.7342224.

[19] V.S. Artamonov, A.K. Chernykh, P.N. Klykov, Podkhod k otsenke effektivnosti sistem upravleniya organizatsionnymi sistemami, funktsioniruyushchimi v realnom masshtabe vremeni [Approach to the Evaluation of the Effectiveness of Management Systems of Organizational Systems Operating in Real Time], Problemy upravleniya riskami v tekhnosfere 4(32) (2014) 60-68.

[20] I.G. Malygin, A.Yu. Krylatov, A.P. Shirokolobova, Marshrutizatsiya dvizheniya pozharnykh avtomobilei v usloviyakh zagruzhennoi transportnoi seti megapolisa [Routing of Firefighting Trucks in Heavy Traffic Environment of Megalopolises], Problemy upravleniya riskami v tekhnosfere 3(43) (2017) 87-95.

[21] A.N. Asaul, I.G. Malygin, V.I. Komashinskiy, The Project of the Intellectual Multimodal Transport System, Transportation Research Procedia, 12th International Conference "Organization and Traffic Safety Management in Large Cities", vol. 20, 2017, 25-30.