Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network

E V Grechishnikov¹, M M Dobryshin¹, S S Kochedykov² and V I Novoselcev²
¹FSO Academy of Russia, Moscow, RUSSIA
²ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irutskaya Street, Voronezh, RU
E-mail: Dobrithin@ya.ru

Abstract. A substantial increase in financial losses accruing because of computer and network attacks on RuNet objects indicate that existing methods of protection are not sufficiently effective. Analysis of information security incidents shows that criminals in order to achieve the objectives apply dissimilar and multidirectional cyberattacks. Existing solutions are not fully able to counteract the harmful effects, including due to the inability to identify several such impacts held simultaneously. Developed algorithmic model makes based on the modeling and assessment of the damage from these threats, generate rules for systems counter cyber attacks, as well as identify conditions that enable timely modify these rules and reconfigure your network topology.

1. Introduction

Use of resources in all areas of the global communications network, contributed to the fact that the attackers for over a decade actively committing various offences in the sphere of high technologies [1] and is currently actively developing different ways and strategies of information technology influences. For the first time, the concept of information technology impact in legal literature found in the doctrine of informational security of the Russian Federation, article 11 the doctrine [2] this effect refers to the negative factor, influencing the State of information security in our country.

Under the information technology should understand the effects targeted by using the assets and capabilities of information technology and other unauthorized attacker's destructive impact on global network objects its operational processes that violate the stability of its functioning and its information security [3-5]. Thus, as the information technology impact may make cyber attacks [6] cost of which is very significant. Data on financial damages caused by various cyber attacks for the year 2017 [7] indicate that existing solutions ensuring information security, not fully capable to protect from this type of effects [8-9].

To protect against data threats currently being developed and widely used different systems to detect and counter cyber attacks [10,11]. However, such systems do not take into account the dynamics of changes in the data transmission network and do not take into account the harm [12].

2. Problem statement

The analysis of the tactics of successful cyberattacks on RuNet objects shows that criminals in order to achieve this goal, quite often use dissimilar cyber attacks [13-15]. Under disparate attacks refers to cyberattacks aimed at the victim's network infrastructure network and the protected
One of the possible scenarios for cyberattacks can be an attack consisting of the impact on the detection system and counter cyber attacks with subsequent penetration into protected local area network or a network share. Challenge of network cyber attacks is partial or full disabling of the system to detect and counter attacks (as a variant of a DDoS attack). The attack on the protected local network aimed at the theft or misrepresentation of information processed (as a variant of SQL injection, the introduction of malicious code, etc.).

This tactics is that existing solutions are not able to effectively detect and counter accordingly various types of cyber attacks. These disadvantages are associated with the fact that existing detection systems counter cyber attacks do not use dynamically changeable (tunable) rules of operation and did not take into account the harm.

To resolve lack of security and enhance specified hosts virtual private network (VPN) algorithm, provides a dynamic change (reconfiguring) the rules of functioning of the systems to detect and counter cyber attacks based on the prediction of possible damage caused by those sites.

3. Algorithmic model of functioning of the system to detect and counter cyber attacks

The essence of developed algorithmic model to simulate the functioning of the system to detect and counter cyber attacks explained structurally-logical sequence shown in figure 1.

4. Description of the algorithm of modeling detection system and counter cyber attacks

In the block 1 measure parameters of network traffic to subscribers on the white list IP addresses. Define VPN node functioning parameters where possible to provide the required services to the Subscriber connection. Retain the measured values in the database settings network settings.

in block 2 measure parameters of known network attacks and gather statistics.
in block 3 perform modeling sequence functioning VPN in terms of reference for computer and network attacks, depict separate VPN modeling process algorithm in terms of cyber-attacks in figure 2.

**Figure 2.** Algorithm of VPN simulation process in cyber attack conditions.
4.1. Algorithm description VPN modeling process in conditions of cyber attacks

3.1 block specify maximum values deviations from the statistical values of the measured parameters and describe the parameter values possible anomalous behaviour from the white list IP addresses. 3.2 block create models of normal behavior and VPN sites. Keep models in the database.

3.3 block create models of computer and network attacks. Keep the model database attacks.

3.4 block specify and complement the 'white' lists of IP addresses of subscribers of this network.

In block 3.5 define or complement network traffic filtering rules based on behavioral criteria including analysis of measured parameters attacks. Develop options for reconfiguring the VPN.

3.6 create models block attack detection system [16-18] and placing sensors in the system. Keep models in the database.

3.7 block placed sensors detection system attacks, determine the required values of reliability measurement for computer and network attacks, and also determine the required values for speed detection system attacks.

3.8 block mimic simultaneous exposure to several different computer and network attacks on one of the nodes in different VPN network traffic load VPN subscribers.

3.9 block handle obtained from sensors detecting system parameter values simulated attacks, measure the value of controlled parameters and performance of the detection system.

3.10 block evaluates the reliability of detection of computer and network attacks, as well as performance detecting attacks.

If the reliability of measured parameters or attack detection system performance does not meet the specified values, in block 3.11 exercise extra made sensors and detection systems in block 3.8 re model attack.

If the reliability of measured parameters satisfies the specified values, the expected harm VPN. If you cannot achieve the desired value performance, carry out a reduction in the number of monitored parameters [19-21] in block 3.12 determine the value of damage to various attacks site VPN [22,23].

3.13 block estimate damage parameter values with valid values functioning VPN.

If the value of the damage exceed the allowed values, the block 3.5 Supplement and modify network traffic filtering rules.

If the value of the damage does not exceed the permissible values, then in block 4 deploy VPN, place and configure system sensors detect attacks, establish rules for network traffic filtering.

4.2. Continued description of algorithm of modeling detection system and counter cyber attacks

In block 5 implementing functioning VPN.

In block 6 defines the end time of the VPN.

In block 7 monitor network traffic parameters characterizing the reference computer and network attacks. Collect statistics about network traffic element VPN and send the measured values in block 17 for analysis.

In block 8 based on specified criteria, decide on the beginning of the reference network and computer attacks. If signs of reference not discovered attacks, continue to monitor the functioning of the VPN, network and computer attacks.

When it detects signs of the beginning of the computer or network attacks in block 9 allocate and control options for attack.

In block 10 based on selected parameters attack decide to belonging to a network or computer classes of attacks. If the detected network attack, 11 block model of network attack effect on VPN host [16-18].

In block 12 estimate possible damages caused to the identified network attack, using existing models of network attacks. If damage values VPN host exposed network attack modeling results meet the required values, then in block 7 continue to monitor network traffic and collect statistics about it.
If the value of the damage site VPN exposed network attack based on the results of the simulations below required values in block 13 change to verify network traffic [24] and (or) reconfigure VPN under available options, reconfiguring. Measured parameters of network attack sent in block 17 for statistical data collection and analysis.

If in block 10 identified the computer attack, block 14 model the impact of computer attacks on VPN node.

In block 15 estimate possible damages caused to the identified computer attack using existing models of computer attacks [18]. If the value of the damage site VPN, the affected computer attack on simulation results meet the required values, then in block 7 continue to monitor network traffic and collect statistics about it.

If the value of the damage item VPN exposed computer attack on modeling results below the required values.

in block 16 filter incoming traffic according to the order for a functioning VPN in the midst of a cyber attack, depict an inbound filtering algorithm in detail in figure 3.

4.3. Inbound filtering algorithm description VPN in terms of cyber attacks

16.1 block IP address is compared with the 'white' list of IP addresses.

If the packages are not 'white' from the list of IP addresses, then in block 16.6 blocked connection.

Figure 3. Inbound VPN filtering algorithm in terms of cyber attacks.
If the package is received from the Subscriber from the list of 'white' IP addresses, then in block 16.2 use additional algorithms for identification.

In the block of 16.3 authenticate subscribers with additional identification algorithms.

If the additional identification of the Subscriber has failed to renew its affiliation to the VPN, 16.6 block connection is blocked.

If the additional identification of the Subscriber confirms his affiliation to the VPN, then in block 16.4, the process of establishing a connection with the Subscriber or continue to work with the Subscriber, if the connection has already been established.

16.5 block using the normal behavior of network traffic by specified criteria control the anomalous behavior of the connection, for signs of computer attacks.

If signs of abnormal behavior of the connection and the presence of signs of computer attacks, continue to control before the end of the connection.

If the connection behavior of abnormal signs or signs of computer attacks, 16.6 block connection is blocked.

4.4. The algorithm description of the collection and analysis of statistical data
In block 17 collect and analyses statistical data on the characteristics of the normal functioning of the VPN settings, and VPN vulnerable to cyber attacks Cyber collection and analysis of statistical data on the characteristics of the normal functioning of the VPN settings cyber attacks and the VPN vulnerable to cyber attack, a detailed discussion of the content of this algorithm is shown in figure 4.

Figure 4. Algorithm for statistical data collection and analysis.
17.1 Block handle statistical values of the parameters of the VPN network traffic operating under normal conditions.

In the block parameters selected compare 17.2 attacks with existing similar parameters in the database.

If the selected settings differ from the available options, in block 17.3 collect statistical data about the attack.

If the selected parameters did not differ from the available options, block attacks 17.5 estimate accuracy and number of installed sensors and system performance, detect and counter attacks.

In the block of 17.4 based on specified criteria fix fact end attack and send statistics on attack in a block of 17.5.

17.5 block after verify placement and number of sensors, as well as evaluation of system performance to detect and counter attacks, you decide to block 2 Add-on value settings for network or computer attacks, specify the parameters of functioning of the system to detect and counter attacks.

5. Conclusion
Thus developed algorithmic model of functioning of the system to detect and counter cyber attacks through possible damage forecasting allows you to dynamically change the rules of operation and detection system combat, as well as to switching channels [25], which in turn increases the security of the VPN sites.

The analysis shows that efficiency using data algorithms for secure VPN nodes is increased by 15-18%. The algorithm can be used when designing advanced systems to detect and counter cyber attacks. The specified algorithm is implemented in the form of RF patents for invention [26]. However, this algorithm does not guarantee 100% protection of the VPN nodes and one can say that the following mathematical problem to calculate the probability of blocking such sites. In this case, you might encounter the following task which may need human intervention [27], professionally and psychologically cope with the task to achieve maximum effect the protection of transmitted and the processed information.[28] But it is not included in the scope of this article, so we look forward to further scientific cooperation.

References
[1] Sushkov P F, Kochedykov S S, Kiselev V V and Artemov A A 2001 Primary investigative Technique in the investigation of crimes in the sphere of high technologies Herald of the Voronezh Institute of the Ministry of Internal Affairs of Russia 2 (9) pp 152-155
[2] Decree of the President of the Russian Federation from 05.12.2016 N 646 ‘on approval of the doctrine of informational security of the Russian Federation SZ RF., 12.12.2016, no. 50, art. 7074
[3] Kochedykov S S 2002 Mathematical model of counter to ITKS multiple NDN GIS in terms of minimizing the distraction of computational resource (Voronezh) p 145
[4] Kochedykov S S, Kravchenko A S, Rodin S V, Perminov G V and Dushkin A V 2015 The subject of the information structure of the interim resource allocation process between different means of protection from unauthorized access Basic research. 5-1 pp 89-93
[5] Kochedykov S S, Novoseltsev V I, Noev A N, Orlova D E 2017 Deterministic methods of diagnosis of crises in automated systems for critical assignment Herald of the Voronezh Institute of the Ministry of Internal Affairs of Russia 1 pp 86-89.
[6] Kochedykov S S, Dushkin A V, Novoseltsev V I, Zdolnik V V and Minin Yu V 2018 Mathematical models of cyber threats to the software of the automated control system Industrial Automated Control Systems and controllers 2 pp 43-55
[7] Medvedev D A 2018 Told about giant damage Russia from cyber attacks Moskovskiy Komsomolets Electronic resource. Access mode
https://www.mk.ru/economics/10/16/medvedev-rasskazal-o-gigantskom-ushherbe-rossii-ot-kiberataki.html.

[8] Kochedykov S S, Ilyin A A, Potanin V E and Bataronov I I 2001 Peculiarities of functioning of information and telecommunication systems in the face of threats to the security of the information being processed *Information and security* 1 pp 63-68

[9] Kochedykov S S, Novoseltsev V I, Sumin V I, Dushkin A V and Eliseyev A I 2017 Mathematical model of information processing and protection in automated systems manage critical objects in view of reciprocal effect software components in terms of the impact of threats to information security *Industrial Automated control systems and controllers* 9 pp 33-46

[10] A joint-stock company Kaspersky Lab. System and method for filtering traffic when detecting DDoS attacks/RF patent № 2649290 30.03.2018 Newsletter. №. 10.

[11] Limited liability company 'trust'. Method and system for analysis malware, protocols for interaction with the control centres and identifying computer attacks/RF Patent No. 2634211 24.10.2017 Newsletter. №. 30.

[12] Novoseltsev V I, Kochedykov S S and Noev A N 2017 Effect of cyber attacks on the outcome of the competition *Actual problems of applied mathematics, informatics and mechanics* 1 pp 843-848

[13] Qrator Labs. Evolution of DDoS attacks and means of countering this threat/electronic resource. Access mode https://qrator.net/presentations/DdosEvolution.pdf.

[14] Vladimir Neumes. Stages of cyberattacks About tactics/electronic resource. Access mode https://vasexperts.ru/blog/etapy-provedeniya-kiberatak.

[15] A joint-stock company Kaspersky Lab Anatomy targeted attacks/electronic resource. Access mode https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/

[16] Grechishnikov E V, Dobryshin M M and Zakalkin P V 2016 VPN access node Model as a network and streaming computer intelligence and DDoS attacks *Cybersecurity Issues* 3 (16) pp 4-12

[17] Dobryshin M M etc. 2016 *Calculation of capacity of the network and streaming computer intelligence to open virtual network connection* Certificate of registration of computer programs 2016618853

[18] Dobryshin M M 2017 *Timing of occurrence of group denial of services (the services) under conditions of DDoS attacks, taking into account the possibilities offered by telecommunications services* Certificate of registration of computer programs 2018610012

[19] Grechishnikov E V and Dobryshin M M 2017 Proposals for improving the performance of distributed monitoring system of computer networks, integrated telecommunication network Questions of defence materiel. Series 16: technical means of countering terrorism 3-4 pp 24-29

[20] Dobryshin M M 2018 *The program of calculation of system performance monitoring of technical state of communication* Certificate of registration of computer programs 2018618661

[21] Dobryshin M M 2018 *Calculation of correlations between the values of the parameters of the technical condition of means of communication* Certificate of registration of computer programs 2018615232

[22] Dobryshin M M and Zakalkin P V 2018 *Integrated security monitoring VPN nodes algorithm from computer intelligence and DDoS attacks* Telecommunications 7 pp 46-52

[23] Dobryshin M M 2017 *Calculation of site features computer network to provide telecommunications services, in conditions of DDoS attacks, taking into account the various ways to minimize the destructive impact* Certificate of registration of computer programs 2017616948

[24] Dobryshin M M 2018 *Proposal to improve systems to counteract DDoS attacks* Telecommunications 10 pp 32-38
[25] Kochedykov S S, Noev A N, Dushkin A V and Gubin I A 2018 Method of optimum channel switching in equipment of infocommunication network in conditions of cyber attacks to their telecommunication infrastructure Journal of physics: conference series "International Conference Information Technologies in Business and Industry 2018 - Mathematical Simulation and Data Processing" pp 124-145

[26] Grechishnikov E V, Dobryshin M M and Belov A S 2017 Modeling Method of assessing damage to network and computer attacks virtual private networks Patent RF № 2625045

[27] Goncharov I, Goncharov N, Parinov P, Kochedykov S and Dushkin A 2015 Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security Probabilistic Modeling in System Engineering Andrey Kostogryzov, IntechOpen pp 233-253.

[28] Dushkin A V, Kochedykov S S and Novoseltsev V I 2017 Tool and algorithmic diagnostic devices of operability of actuation mechanisms of automated control systems Proceedings. 2017 2nd International Ural Conference on Measurements (UralCon) South Ural State University (national research university), Chelyabinsk, Russian Federation DOI: 10.1109 URALCON 8120709 pp 193-198