"Network Security Intelligence" Educational and Research Center

Natalia Miloslavskaya, Alexander Tolstoy, Anton Migalin

"Network Security Intelligence" Educational and Research Center

Natalia Miloslavskaya, Alexander Tolstoy and Anton Migalin

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{NGMiloslavskaya, AITolstoj, ASMigalin}@mephi.ru

Abstract. The paper presents a recent experience (since 2016) in establishing and running the "Network Security Intelligence" educational and research center (NSIC) in the framework of the new NRNU MEPhI's Institute of Cyber Intelligence Systems (ICIS). The created center is designed to provide training and research on effective network security management based on intelligent approaches and applications, the use of Big Data technologies for processing information security information, the study of the compatibility between different network protection tools, as well as the evaluation of network security. The educational NSIC's basis currently consists of two laboratories with Next-Generation Firewall (NGFW) and Data Loss Prevention (DLP) systems at their cores respectively. Here we discuss the use of the first one. The main areas of further work in expanding NSIC's operation for training and research conclude the paper.

Keywords: Network Security Intelligence, Educational and Research Center, NGFW, DLP, information security

1 INTRODUCTION

Intensive development and use of modern information and communication technologies (ICT) has led to serious qualitative changes in the economic, socio-political and spiritual spheres of public life. Nowadays we witness dramatic changes in ICT that are driving current information security (IS) trends and require sophisticated structures and adequate approaches to manage IS on different scales: for individuals, for organizations, for countries and for the entire world. The wide range of new and ever-growing IS threats, especially those related to new ICT, network technologies, services and devices, are all around us.

The "e-Skills for the 21st Century: Fostering Competitiveness, Growth and Jobs" Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions says that "There is an important need to address ICT-related skills (e-skills) issues in order to respond to the growing demand for highly-skilled ICT practitioners and users, meet the fast-changing requirements of industry… Shortages of ICT practitioner skills have

been endemic due to technological innovation and the fast growth of ICT activity in comparison with the relatively low supply and availability of new employees and entrepreneurs with relevant educational qualifications " [1].

In 2015 the World Summit on the Information Society (WSIS) noted that it should explicitly recognize ICT Professionalism because the implementation of WSIS action lines and Sustainable Development Goals requires the services of a skilled, competent, ethical, accountable, and trustworthy ICT workforce [2].

In its 2016 Cybersecurity Skills Gap graphics [3], ISACA has shown that more than 1 in 4 organizations have experienced an APT attack and by 2020 the average cost of a data breach is estimated to be $150 million, while 53% of organizations experience delays as long as 6 months in finding qualified security candidates. A global shortage of 2 million cybersecurity professionals is expected in 2019.

Hence the demand for highly-skilled ICT practitioners ready to act in modern heterogeneous ICT systems, which are vulnerable to various sophisticated attacks, is more obvious than ever before. To meet this challenge, to achieve business objectives, to stay competitive and to operate legally, organizations of all types (e.g. commercial or non-profit organizations, government agencies), sizes and spheres of activity need to have a unified, inclusive, scalable, effective security system with proper security intelligence services in place and "best-in-breed" information protection tools (IPTs), measures, and staff to truly manage IS for their sensitive assets.

The paper describes our experience with the recently established (in 2016) educational and research center for intelligent network security management, called the "Network Security Intelligence Center" (NSIC), within the framework of the new NRNU MEPhI's Strategic Academic Unit called the Institute of Cyber Intelligence Systems (ICIS). At present we only consider educational purposes (because the hardware and software base of the center is still not fully developed for research purposes). Prof. Bart Preneel from the Catholic University of Leuven is NSIC's Scientific Leader.

Our current work is aimed at developing the NSIC concept in general, and our own NSIC in particular, as a world-class educational and research center. The goal of this work is to present a model of NSIC for its study and continuous improvement, taking into account the characteristics of today's networks and the forecast for networks in the not so distant future. For our purposes, our NSIC will be based on three bearing laboratories with Next-Generation Firewalls (NGWFs), Data Loss Prevention (DLP), and Security Information and Event Management (SIEM) systems at their cores respectively. The NSIC can be reasonably used as a basis for creating a trusted educational environment for blended learning with many e-learning components.

Our paper is organized as follows. Section 2 provides a brief review of related work. The general NSIC's description is given in Section 3. The use of NGFWs for educational purposes is presented in Section 4. The main areas of further work in expanding the NSIC's operation for training and research conclude the paper.

2 RELATED WORK

The world's leading IT research and advisory firm, the Gartner Company, identified the top 10 strategic technology trends that organizations of different sizes and spheres of activities cannot afford to ignore in the next three years (up to 2018) [4]. Gartner highlighted the advent of intelligence everywhere, meaning three wide-spreading trends. First, "Advanced, Pervasive and Invisible Analytics" will take center stage as the volume of data generated by embedded systems increases, and data lakes of structured, semi-structured and unstructured data [5] inside and outside the organization should be analyzed for more informed decision-making. Second, embedded intelligence combined with deep analytics will drive the development of "Context-Rich (and context-aware) Systems" that monitor their rapidly changing surroundings and respond appropriately. And last, but not least, "Deep Analytics" applied to an understanding of context provide the preconditions for a world of smart machines that learn for themselves and act autonomously. Our key task is to teach them to act constructively, not destructively.

Most publications discuss centralized network security management in terms of first generation SIEM systems run from a Security Operations Center (SOC) (e.g. [6], with more detailed analysis in [7]). Cisco Systems in particular contributed to the SOC idea [8]. Subsequent publications focus on either tools for computer network defense [9-11] or on people and processes.

Then people began to talk about a Security Intelligence Center (SIC) with an integrated IS architecture and a 2nd generation SIEM system, providing full visibility and control and context-driven security intelligence in one place to temporarily deal with network-level and more important higher-level IS events. SIC as a separate term exists since 2011 [12], with a few papers on the topic [13-15]. In [16] a short comparison of SOC and SIC is given which was a starting point for our research.

To empower the autonomy of network security management within one organization and to deepen its knowledge of the computing environment, our research is aimed at uniting all the advantages of a SIC and a Network Operations Center (NOC) [17] with their unique and joint toolkits and techniques in a unified NSIC. NSIC changes the security model from reactive to proactive, supports more effective responses to IS incidents, enhances communications between the network and security teams, management and board members, drives IS investment strategies, and more directly connects IS priorities with business risk management priorities. The research in this area has just begun.

As for the work about laboratory support of IS education, we mention only the pioneers like [18-21], followed by many lab descriptions worldwide in the next years. These works provide useful instructions in designing labs and developing an education process based on them. The authors also have their own experience in starting the "Network Security" laboratory in 2000 [22], and continuing through the present [23]. Subsequent publications show how to use virtualization technologies in the education process (like [24]). These technologies are very useful as they have the necessary tools to build complicated virtual networks on virtual machines and show all the IPTs' functionality.

3 GENERAL NSIC DESCRIPTION

Automating all routine operations and IS incident response that do not require expert decision-making is an urgent need for any modern organization. It should set up a more advanced IS management center than a traditional SOC. The so-called SIC with an integrated attack defense architecture provides full visibility, control and context-driven security intelligence (SI) in one place to temporarily deal with higher-level IS events. By implementing SICs, organizations get a holistic, in-depth view of their "IS health" and can not only detect and recognize attacks, but also effectively predict, prevent, and address IS incidents before they cause harm, thus constantly gathering data and producing new IS-related knowledge. The SI concept emphasizes the need to not just collect data but also learn from it in order to continually stay ahead of intruders. Viewing time-stamped historical data or logs is very important for IS incident investigation. But stopping IS incidents is possible only when you have a real-time view in a concrete context of what is happening right now so you can find something unusual, across the entire network. Any delay, and only reactive actions, put an organization's assets at risk. Hence, the goal of SI is to provide proactive, predictive (forward-looking), actionable and comprehensive protection and insight into IS that reduces the IS risks and operational effort through advanced analytics. All information that SI deals with is processed, sorted, aggregated from reliable sources, cross-correlated for accuracy, assessed for relevancy, evaluated and interpreted by analysts at the final stage if needed.

The NOC's aim is to support a centralized place from which network administrators can remotely supervise, maintain and monitor their telecommunications networks using appropriate management software, and visualize their detailed status with all devices that are being monitored. The NOC can be considered the focal point for the following typical activities: network discovery, assessments and management; optimization and quality of service management and reporting; domain name management; constant research of anomalies and problems (troubleshooting) to make adjustments, marshal resources and respond to emergency situations; application software installations, distribution, troubleshooting and updating; performance monitoring, reporting and improvement recommendations; backup and storage management; email management services; voice and video traffic management; basic (elementary) IS controls like authentication and authorization, IP- and MAC-address filtering, etc.

The NSIC's key objective is to move SI to organizations' NOCs, allowing them to stay ahead of IS challenges while being fully integrated around their main business processes. To implement this idea of migration to the NSIC is possible because both the SIC and NOC operation functions are frequently organized in a similar way, which is based on a tiered approach with similar roles, and share some tools. Their union would be very beneficial in the long-term as the NOC's primarily concern is serving the business, while the SIC's main focus is to ensure its security. When an outage is detected, the NOC's staff is likely to attribute the disruption to device malfunction or system issues and attempt to address it through hardware replacement or configuration adjustment. But the SIC's personnel are likely to attribute the problem

to malicious activity and will thus prompt an investigation before initiating IS event response actions.

While designing the NSIC, we have focused first on its self-protection. For that purpose, we defined all information resources that are to be protected within the NSIC (using the common approaches of asset inventory and categorization as the initial steps of IS risk assessment [25]). It is typically sensitive data used in a typical network of an educational institution, for example proprietary information of limited propagation, sensitive information related to the NSIC's activities, personally identifying information (PII) of its staff and trainees, learning and testing materials protected by copyright, keys, credentials and passwords, etc.

Then, based on a comprehensive analysis of the security level of our department network (investigating logs, using security scanners, for example), we worked out two generalized IS models for the given network, presented in documents of many pages. The first one – an IS threat model – included a formalized description of IS threat sources [26], vulnerabilities exploited by them, objects suitable for the threats' realization, threats implementation techniques (actual attacks), types of possible loss, extent of the potential damage and some additional information such as likelihood of threats implementation; destructive impact (including interconnecting); damage elimination/limitation; impact frequency and duration, etc. The second model (an IS intruder model) contained a formalized intruders' classification and description of their experience, knowledge, available resources for IS threats implementation, possible motivation of their actions and IS threats implementation techniques.

After that, we developed an IS policy for the NSIC that ensured meeting the key goal of its IS, namely achieving adequate protection of NSIC's information assets and business processes, and allowing its continuous operation under IS threats. Among the most important IS policy requirements are the following:

- Usage of all applicable IPTs and IS controls;
- Establishing monitoring and auditing policies and procedures;
- IS event and incident processing;
- Vulnerability management;
- Configuration and changes management;
- User' s activity registration;
- Filtering of incoming and outgoing traffic;
- Protection against computer viruses and unauthorized software modification and insertion;
- Control over all NSIC's computer port usage;
- Protection against DoS attacks and unauthorized scanning; and
- Setting responsibilities for IS policy violation, etc.

4 NGFW STUDY

Now, the most common IPTs are hardware and software firewalls (FWs), which provide network traffic control based on packet filtering in accordance with the rules of

organization's IS policy. As a result of their evolutionary development, the first specialized solution with Deep Packet Inspection (DPI) and detailed and customizable control at the application level appeared in 2007. NGFW unites on one platform multiple IPTs such as FW, IPS (Intrusion Prevention System) and Web security gateway. Policies for applications, users and sessions are defined in a NGFW within certain contexts, not just for ports and IP addresses. User identification, which allows integration with various organization's directory services, is implemented in a NGFW. A NGFW can work with encrypted SSL-traffic on all ports. This IPT can receive black and white address lists from trusted external sources and apply them to the relevant filtering rules. Indeed, NGFWs work faster and support more complex rule sets than their predecessors. According to a Gartner survey [27], 40% of companies use NGFWs to protect their intranets, and by 2018, 85% of all FWs will be NGFWs.

Based on the analysis of the leading vendors for NGFW, as well as NGFW functionality, we concluded that the Palo Alto Networks NGFW [http://www.paloaltonetworks.com] meets the requirements of our NSIC. It also can be implemented in the VMware environment (as a virtualized NGFW) that is well suited for carrying out laboratory work with NGFWs. Due to our collaboration with Palo Alto Networks, we obtained this solution for our educational purposes.

To develop students' skills in configuring NGFW settings and customizations and taking into account its capabilities, we created a laboratory bench. The laboratory bench is designed to test all basic NGFW functionality (Fig. 1) in the form of a one-way gate. One student uses one computer with VMWare Player and one image of the VM-300 (Palo Alto Networks) virtual machine. All computers in the classroom are connected in a single local network and receive their IP addresses using DHCP from the 192.168.1.0/24 network. The students run a virtual machine image, configure NAT and routing for the virtual 172.168.1.0/24 network. When they are trying to connect to the Internet, the traffic generated passes through the NGFW.

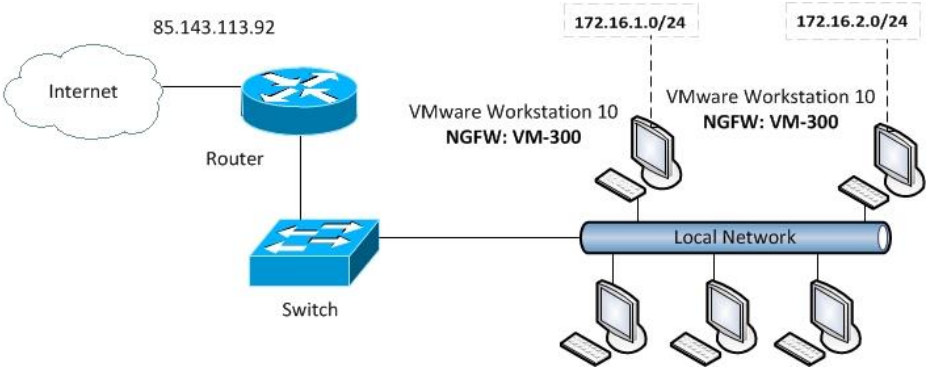

Fig. 1. The scheme of a one-way gate

This laboratory bench meets the following requirements:

- Flexibility, as its structure should be easily reconfigurable: different lab tasks require specific network topologies and host configurations,

- Scalability, for simultaneous task performance by 16 students in the NGFW laboratory and two others (with DLP and SIEM systems); the main resources are located on each computer, and we have a distributed network which does not depend on a centralized server;
- Profitability, as the cost of NGFW installation and maintenance in the laboratory is significantly less than the cost in the real intranet, taking into account that the lab should effectively simulate the processes in real networks;
- Reliability, as the laboratory should be able to easily recover from accidental damage by the students, as well as be able to quickly restore the default settings and network configurations; and
- Isolation, as it should be isolated from the remaining part of the NSIC and not affect its operation; the internal LAN is isolated from the outside NSIC's network. Each student works within the same LAN. The work task implementation will not cause any inconvenience to other NSIC users. Thus, the laboratory bench allows each student to test the NGFW functionality by himself.

On the basis of the rules of the IS policy (Section 3), the following context for laboratory work was defined:

1. To prohibit all traffic between some subnetworks, except for that authorized by a network administrator;
2. To use the NGFW only in a router mode;
3. To allow all hosts from 192.168.2.0/24, 192.168.20.0/24, 192.168.21.0/24, 192.168.200.0/24 networks to access the Internet;
4. To identify the applications at OSI layer 7 by signatures;
5. To decrypt all SSL traffic from the 192.168.200.0/24 network, and if that fails, then block this traffic;
6. To allow access to the DMZ servers from the internal network;
7. To permit only those web-mail applications that use MEPhI's email;
8. To block access to phishing and malicious URL-addresses from the 192.168.200.0/24 network;
9. To analyze the frequency of HTTP, TCP, UDP, ICMP packets to web and DNS servers;
10. To analyze .exe, .dll, .bat, .sys, .flash, .jar, .doc, and .pdf files for malware using behavioral anti-virus mechanisms; and
11. To block encrypted documents and files downloaded to the 192.168.200.0/24 network, etc.

To start with, we created 5 laboratory exercises, and will be adding more to these in the future. Each lab is designed for 4 academic hours (with all controls and tests).

1. Lab #1 "First NGFW installation and configuration".

Objective: to get skills in installing a NGFW, configuring routing rules, and defining user accounts and security certificates (create, import, and export).

Student assignment: to configure the static routing rules (e.g., all incoming traffic is redirected to the next router at 192.168.1.1); to configure the network address trans-

lation (NAT) rules (for example, translate dynamic IP and port type, interface address type, Ethernet ½ interface, etc.); to create a trusted client's connection to the NGFW; to create a user with administrator privileges; and to set up two-factor authentication for the NGFW administrator.

To confirm the successful task execution, it is necessary to demonstrate to an instructor the following features (controls): the ability to connect to the Internet from the 172.16.1.0/24 network; a trusted connection to the Palo Alto Networks Web interface; multiple users authenticated as administrators; two-factor authentication of an administrator, using a password and a client certificate.

2. Lab #2 "SSL/SSH traffic decryption" (Fig. 2).

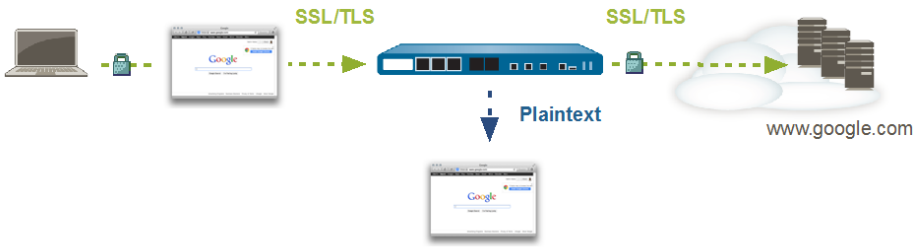

Fig. 2. SSL traffic decrypting scheme

Objective: to gain skills in installing a security certificate, decrypting SSL/SSH traffic, and intercepting and analyzing packets captured with the Wireshark traffic analyzer software.

Student assignment: to create a self-signed certificate; to configure SSL decrypting rules; to capture packets using the Packet Capture technology; to analyze packages using Wireshark.

Controls: interception and decryption of https traffic from the student's computer; filled-in data from an authentication form (such as https://accounts.google.com/) found by the Wireshark.

3. Lab #3 "User identification (User-ID)".

The authentication profiles define the configuration of a local database, RADIUS, LDAP and Kerberos, and can be assigned to administrative accounts and provide VPN access. The NGFW checks the authentication profile assigned to the account and authenticates the user based on the specified settings.

Objective: to gain skills in identifying the users who have requested access to the Internet, configuring the authentication profiles, creating a local user database, configuring LDAP server settings, and using security certificates for authentication.

Student assignment: to configure user authentication rules; to set up forwarding to a Web form to enter a login name and password; to set up a security policy based on user ID.

Controls: redirection to a web form and user network authentication; the use of various filtering rules depending on the user authenticated in the network.

4. Lab #4 "Identification of applications (App-ID) and data control (Content-ID)".

Creating and managing security policies based on application and user identification, regardless of device or location, is more effective for network security than making a decision based solely on ports and IP addresses. Integration with enterprise user directories allows the users of Microsoft Windows, Mac OS X, Linux, Android, and iOS, who are accessing the applications, to be identified. The combination of application usage monitoring and control means that the protected usage of Oracle, BitTorrent, Gmail or any applications used in the network, regardless of where and how the user accesses it, can be ensured.

Objective: to gain skills in identifying applications (regardless of port, protocol, encryption or masking techniques used), traffic analysis, limiting unauthorized transfer of files and data traffic, filtering by URL addresses, and blocking unknown or targeted malware.

Student assignment: to add new URL filtering rule; to set the time interval following the Continue action of the user; to set the time interval after the user enters the admin override password; to apply different filtering rules to the URL categories; to select different filtering rules for all the proposed file extension types; and to apply the filtering rules created in the policies section.

Controls: the use of different filtering rules depending on the application, for example, to block all Tor connections; the use of different filtering rules depending on the extensions of transmitted files, for example, to block downloading executable files; the use of different filtering rules depending on the web page category or URL, for example, to block all anonymizer sites; the application of any method of traffic masking, such as TCP over DNS tunneling; and a demonstration of the ability to protect different applications used in the network.

5. Lab #5 "Prevention of threats and vulnerabilities".

An NGFW with an Intrusion Prevention System (IPS) inside neutralizes the threats associated with network blocking, application level vulnerabilities exploitation, buffer overflows, DoS attacks, port scanning, etc. Antivirus and antispyware software blocks malware, as well as command and control traffic generated by malware, viruses in PDF files and malware hidden in compressed files or web traffic. Based on security policies, the decryption of SSL traffic for all applications and ports provides protection against malware that attempts to gain access through applications using the secure SSL protocol.

Objective: to gain skills in protecting networks against computer viruses, worms, spyware and other malicious traffic using security profiles; detecting and eliminating vulnerabilities of network applications inside the LAN; identifying hosts infected with bots; and detecting and preventing known attacks.

Student assignment: to set the rules for signature-based anti-virus tools; to set the rules for behavioral anti-virus tools; to set the rules to detect attacks such as HTTP, ICMP, UDP and SYN flooding.

Controls: blocking malicious files by the signature-based anti-virus tools; blocking computer virus (obtained from the instructor) by the behavioral anti-virus tools; any method known to the student to conduct HTTP, ICMP, UDP and SYN flooding and its detection and prevention using the NGFW.

We make one short note on the current context, in which the students carry out their exercises: all of them are given the lab descriptions (30 pages in total) in advance, to provide the opportunity to be better prepared to work and demonstrate their knowledge on the progress test after it. In order to complete the labs successfully, the students must pass tests consisting of 30 questions.

Another note concerns privacy. It is a separate issue that requires special study in the framework of different disciplines (not only technical network security). That is why it is not been considered in this paper.

The labs have been successfully tested within the "Information Security of Open Systems" course for the 5th year Specialists (2 groups, 40 students) and the "Objects' Information Security Maintenance Technologies" course for the 2nd year Masters (5 groups, 60 students).

5 CONCLUSION

All scientific studies facilitate new learning and vice versa – some interesting issues that require additional investigation can be found during practical work. An NSIC can be regarded as expanding knowledge and skills through creative research and discovery. Consequently, the NSIC's project relevance is determined by the urgent needs to create a scientific, methodical and material base for network security professional training through the use of modern and advanced ICT and educational technologies, as well as the conditions necessary for MEPhI to compete successfully among world educational centers. The vision of the center is to be recognized at national and international levels for excellence in advanced network security management and professional training.

We shared our short-tem experience in starting the development and use of our NSIC in the framework of the MEPhI ICIS. As can be seen, it is a work in progress and there is still much to do. Our future work is intended to finalize the creation of the second and third NSIC's DLP and SIEM laboratories. After that, all three core IPTs (NGFW, DLP and SIEM systems) for the NSIC will be deployed.

We presented the NSIC's usage only in term of educational process improvement, in particular for studying NGFWs. Our ambitious plans in this direction include but are not limited to the following: development and subsequent implementation of educational standards; new programs (curricula) and competency models for different educational levels for specialized professional training in the field of network security; supervising PhD students carrying out their research within the NSIC's topics; conducting summer schools with intensive network security programs, etc. NSIC can

be reasonably used to create a trusted educational environment for blended learning with a set of e-learning courses on network security management.

The created center is also expected to carry out research on the NSIC's design, effective network security management practices based on intelligent approaches and applications, the use of Big Data technologies for IS-related data processing, and the study of the compatibility between different IPTs and make recommendations to address arising issues, as well as evaluating network security.

To publicize the NSIC's activities and to post its news and offers in education and joint research, we are creating a secure web site for it.

6 ACKNOWLEDGEMENT

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

7 REFERENCES

1. e-Skills for the 21st Century: Fostering Competitiveness, Growth and Jobs. http://ec.europa.eu/growth/sectors/digital-economy/e-skills_en (access date 03.11.2016).
2. Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels. Report of the Secretary-General. United Nations. General Assembly. Economic and Social Council. http://unctad.org/en/PublicationsLibrary/a71d67_en.pdf (access date 03.03.2017).
3. 2016 Cybersecurity Skills Gap. ISACA. http://www.isaca.org/cyber/PublishingImages/Cybersecurity-Skills-Gap-1500.jpg (access date 03.03.2017).
4. Gartner's Top 10 Strategic Technology Trends for 2015. URL: http://www.gartner.com/smarterwithgartner/gartners-top-10-strategic-technology-trends-for-2015/ (access date 03.03.2017).
5. N. Miloslavskaya and A. Tolstoy, "Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues". Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016). August 22-24, 2016, Vienna (Austria), Pp. 148-153.
6. R. Bidou, "Security operation center concepts & implementation", 2005. URL: http://iv2-technologies.com/~rbidou/ SOCConceptAndImplementation.pdf (access date 31.01.2016).
7. N. Miloslavskaya, "Security Operations Centers for Information Security Incident Management". Proceedings of the 4th International Conference "Future Internet of Things and Cloud" (FiCloud 2016). Vienna (Austria). 2016. Pp. 131-138.
8. Security operations center: building, operating, and maintaining your SOC. Cisco Press. 2015.
9. C. Sanders and J. Smith, "Applied network security monitoring: collection, detection, and analysis", Boston, MA: Syngress, 2013.
10. R. Bejtlich, "Practice of network security monitoring", San Francisco, CA: No Starch Press, 2013.

11. Insights on governance, risk and compliance. Security Operations Centers — helping you get ahead of cybercrime. EY GM Limited. 2014.
12. J. Burnham, “What is Security Intelligence and why does it matter today?” URL: https://securityintelligence.com/what-is-security-intelligence-and-why-does-it-matter-today/ (access date 03.03.2017).
13. E.M. Hutchins, M.J. Clopperty, and R.V. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and Intrusion Kill Chains”. Lockheed Martin Corporation. 2013.
14. Threat intelligence platforms. ThreatConnect, Inc. 2015. URL: http://www.informationweek.com/whitepaper/ (access date 03.03.2017).
15. Security Intelligence. Prevent fraud. Achieve compliance. Preserve security. URL: https://www.sas.com/en_us/software/fraud-security-intelligence.html (access date 03.03.2017).
16. SOC vs. SIC: the difference of an Intelligence Driven Defense® Solution. A White Paper Presented by: Lockheed Martin Corporation. 2015.
17. What is a Network Operations Center (NOC)? URL: http://www.continuum.net/msp-resources/mspedia/what-is-a-network-operations-center-noc (access date 03.03.2011).
18. G.B. White and R.E. Sward, “Developing an Undergraduate Lab for Information Warfare and Computer Security”. Proceeding of the IFIP TC11 WG11.8 First World Conference on Information Security Education. 17-19 June 1999, Kista, Sweden. Pp. 163-170.
19. C.J. Armstrong and H.L. Armstrong, “The Virtual Campus”. Proceeding of the IFIP TC11 WG11.8 Second World Conference on Information Security Education. 12-14 July 2001, Perth, Australia. Pp. 161-168.
20. D. Gritzalis D. and T. Tryfonas, “Action Learning in Practice: Pilot delivery of an INFOSEC University laboratory course”. Proceeding of the IFIP TC11 WG11.8 Second World Conference on Information Security Education. 12-14 July 2001, Perth, Australia. Pp. 169-182.
21. L.J. Hoffman, R. Dodge, T. Rosenberg, and D. Ragsdale, “Information assurance laboratory innovations”. Proceedings of the 7th Colloquium for Information Systems Security Education, Washington, DC, USA. 2003.
22. N. Miloslavskaya and A. Tolstoy, “Network Security Scientific and Research Laboratory”. Proceedings of the 3st World Conference on Information Security Education WISE3. USA, Monterey, 2003.
23. A. Ismukhamedova, Y. Satimova, A. Nikiforov, and N. Miloslavskaya, “Practical Studying of Wi-Fi Network Vulnerabilities|. Proceedings of the 3rd International Conference DIPDMWC2016. 1st International Workshop on Education for Secure Digital Information Processing, Data Mining and Wireless Communications (ESDIPDMWC2016). July 6-8, 2016, Moscow (Russia), Pp. 227-232.
24. R.C. Dodge, B. Hay, and K. Nance, “Using Virtualization to Create and Deploy Computer Security Lab Exercises”. Proceeding of 6th World Conference on Information Security Education (WISE6). IFIP. Vol. 278. January 2010.
25. ISO/IEC 27005:2011 "Information technology -- Security techniques -- Information security risk management".
26. A. Malyuk, and N. Miloslavskaya. Information Security Theory for the Future Internet. Proceedings of the 3rd international conference «Future Internet of Things and Cloud» (FiCloud 2015). Rome (Italy), 24-26 August 2015.
27. Magic Quadrant for Organization Network Firewalls 2015. URL: http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Organization-Network-Firewalls.pdf (access date 03.03.2017).