Developing Hands-On Laboratory Works for the "Information Security Incident Management" Discipline

Natalia Miloslavskaya, Alexander Tolstoy

Developing Hands-On Laboratory Works for the "Information Security Incident Management" Discipline

Natalia Miloslavskaya and Alexander Tolstoy

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

{NGMiloslavskaya, AITolstoj}@mephi.ru

Abstract. The paper presents our recent experience in developing the hands-on laboratory works for the "Business Continuity and Information Security Maintenance" Master's Degree programme in the framework of the NRNU MEPhI's "Network Security Intelligence" Educational and Research Center (NSIC). These labs are designed for the "Information Security Incident Management" discipline to provide training on information security (IS) incident practical and actionable response, in particular its investigation on the basis of computer forensic approaches and specialized tools being used for these purposes. The main areas of further improvement of these labs conclude the paper.

Keywords: information security incident, online banking services, money transfer, hands-on laboratory work, computer forensics

1 INTRODUCTION

In the face of ever-increasing Information Security (IS) incidents, many standards determine the need for organizations to timely identify and respond to them [1]. In 2012, satisfying the urgent demand for a specific IS specialists, the "Business Continuity and Information Security Maintenance" two-years (4 semesters) Master's Degree programme was launched at the "Information Security of Banking Systems" Department of the NRNU MEPhI. The "Information Security Incident Management" discipline is included in the curriculum. Its main provisions are illustrated on the typical transferring money cases for the Online Banking Services (OBS).

Taking into account the OBS specifics, IS incident when transferring money refers to an IS event or their combination, indicating an accomplished, ongoing or probable IS threat implementation, which results in 1) the destructive impact on organizations' or clients' information infrastructure components (together called II components) used for money transfer (MT), which led/may lead to a violation of the payment service provision continuity, or 2) an unauthorized MT by persons without the right to dispose of funds that led/may lead to MT by order of persons who do not have such rights, non-temporal MT or MT using distorted payment details in the MT orders [2]. The key areas of response to these IS incidents are the following: identification of IS

adfa, p. 1, 2018.

threat implementation methods and schemes based on the collection and analysis of technical data (TDs) generated by II components (including Information Protection Tools, IPTs), used by organizations and clients for MT; prevention of repeated IS incidents based on previously used methods and schemes; identification of IS threats' sources, based on TDs processing results; and conducting timely detection of markers for "hidden" unauthorized II components' management (known as Indicators of Compromise, IoCs) based on TDs processing results. To ensure that these activities can be performed within the IS incident management system (including collection and recording of information about the IS incident), organizations should apply methods of collecting, processing, analyzing and documenting the TDs. At the same time, the TDs collection and further extracting the content (semantic information) from them should be conducted by persons having the necessary experience and competence.

All teachers are aware that a theory is not viable without practice, as any theory is better understood when it can be practiced. That is why to develop more enhanced students' skills in IS incident management within the greater opportunities that appeared after creation of the "Network Security Intelligence" Educational and Research Center (NSIC) at the NRNU MEPhI [3] it was decided to update the laboratory works (labs) for the above discipline, which was previously focused on the study of Intrusion Detection and Prevention systems (IDPSs), Security Information and Event Management systems and security scanners. Thus the paper is organized as follows. Section 2 provides a brief review of related work. General description of the developed labs is given in Section 3. The basic principles of performing the labs are presented in Section 4. Section 5 is devoted to the regulatory framework used for the labs creation. Students' assignments and labs' scenario are described in detail in Section 6. The recommended strategies for the collected TDs analysis and investigative software are listed in Sections 7 and 8 respectively. The laboratory testbed is discussed in Section 9. The main areas of further improvement of our labs conclude the paper.

2 RELATED WORK

Computer forensics learning has begun to be dealt with for a long time and a lot has already been written on this topic by now. Let us mention only a few most interesting from our point of view publications, showing their main focus. Majority of publications from the early 2000s examined forensics education in general (like in [4]) and its possible curriculum [5]. Further works were devoted to teaching forensics to a specialized target groups like undergraduate students [6] or experts with their further certification [7-10]. In parallel, the issues of implementing common labs [11-13] and conducting some specific labs within the framework of courses offered by different training centers [9, 14-16] are discussed. For example, at present there are a lot of certifications in the area: *Vendor-Specific*: EnCase Certified Examiner (EnCE) and AccessData Certified Examiner (ACE); *Vendor-Neutral*: Certified Forensic Computer Examiner (CFCE) and Electronic Evidence Collection Specialist (CEECS) by International Association of Computer Investigative Specialists; Certified Forensic Analyst (GCFA) and Examiner (GCFE) by SANS GIAC; Computer Hacking Forensic Inves-

tigator (CHFI) by EC-Council; Certified Computer Crime Investigator (CCCI) and Forensic Technician (CCFT) by High-Tech Crime Network, and other certifications by Computer Technology Investigators Network, High Technology Crime Investigation Association, etc.

The usage of open source tools while teaching computer forensics is also long and widely popularized [17, 18].

As we have so far developed only one, but useful for the purpose of IS incident management lab, we do not want to be compared and compete with all these recognized leaders in computer forensics training and certification; we just want to learn their best practices.

3 GENERAL DESCRIPTION OF THE LABS DEVELOPED

The "Information Security Incident Management" discipline (3 credits) is one of the core courses of the above Master's Degree programme, and computer forensics and investigation is not its main specialization. It is obvious and does not require long explanations that "Incident Response" is more general concept than "Computer Forensics" originated in the late 1980s (of course, with this wording, we do not want to underestimate its importance). At a minimum, incident response involves also pre-incident preparations, all necessary organizational activities around the computer forensics process and post-incident actions with lessons learnt. In turn, computer forensics process is initiated after an incident is detected for its actual investigation.

The discipline is taught at the 3rd semester (after the "Information Security Risk Management" discipline and in parallel with the "Information Technology Security Assessment" discipline) and consists of 16 hours of lectures, 16 hours of labs and 36 hours of various forms of student's independent work under instructor's supervision.

The discipline goal is to study the methods and tools of IS incident management (with cases for the banking organizations of the Russian Federation), as well as the main approaches to the development, implementation, operation, analysis, maintenance and improvement of IS incident management systems (ISIMSs) of a particular organization to be protected. One of the sections of the discipline is devoted to the IS incident response teams (ISIRTs). Among other things, the ISIRT's work with the IS incident's digital evidence should be given special attention. Hence, we developed our hands-on labs keeping in mind their target audience – future ISIRT's experts.

As it is approved in the discipline's syllabus and following the requirements of the Bank of Russia Standard STO BR IBBS-1.3-2016 [2], after these labs our students will obtain the following basic skills and abilities (learning outcomes), namely:

- To organize IS incident management, in particular the collection and analysis of IS incident information to decide on a subsequent response;
- To participate in the design and operation of the organization's ISIMSs, in particular in the activities of ISIRTs;
- To develop drafts of organizational and administrative documents, as well as technical and operational documentation for ISIMSs and make a choice and use tools for managing IS incidents.

4 BASIC PRINCIPLES OF PERFORMING THE LABS

On the labs, the activity of ISIRT's members is simulated when collecting the TDs from the II components involved in MT and searching for and extracting the content (semantic information) from the collected TDs for further deep analysis. Doing this, students should learn to observe the following important principles of their behavior. All downloads and installations during labs must be coordinated with the instructor. Any procedures and service commands performed for TDs processing should not make changes to the original TDs and/or their reference copies. The implementation of all procedures and service commands for TDs processing should be accompanied by the implementation of procedures and service commands that should provide their availability and confidentiality, as well as the opportunity to monitor their integrity (invariability). TDs processing should be accompanied by the description and logging, among other things, of all procedures and service commands performed, as well as a list of the technical tools used. When collecting the TDs, any means/materials that produce/emit a static or electromagnetic field should be avoided, as it can damage/destroy the collected TDs. Less powerful PCs should be used for routine tasks and multipurpose PCs for high-end analysis. This list can be expanded if necessary.

5 REGULATORY FRAMEWORK FOR THE LABS

When developing the labs we followed all the recommendations of the following regulations (excluded from the References deliberately not to make them very large and not cited on every page again and again as the basis for all our conclusions):

1. International: Standards by ISO/IEC: 27035:2016 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management and Part 2: Guidelines to plan and prepare for incident response; 27037:2012 Guidelines for identification, collection and/or acquisition and preservation of digital evidence; 27041:2015 Guidance on assuring suitability and adequacy of incident investigative method; 27042:2015 Guidelines for the analysis and interpretation of digital evidence; 27043:2015 Incident investigation principles and processes; 30121:2015 IT -- Governance of digital forensic risk framework; Special Publications (SP) by NIST: 800–61r2 Computer Security Incident Handling Guide; 800-86 Guide to Integrating Forensic Techniques into Incident Response; 800-92 Guide to Computer Security Log Management; 800-101r1 Guidelines on Mobile Device Forensics; Publications by the SANS Institute, the European Network of Forensic Science Institutes, the Scientific Working Group on Digital Evidence; etc.;
2. National: Bank of Russia Recommendations on Standardization RS BR IBBS-2.5-2014 «Maintenance of Information Security of the Russian Banking System Organizations. Management of Information Security Incidents» and Standard STO BR IBBS-1.3-2016 «….Collection and Analysis of Technical Data When Responding to Information Security Incidents during Money Transfer» [2].

6 STUDENTS' ASSIGNMENTS AND LABS' SCENARIO

The objective of these hands-on labs is to provide our students an expert knowledge about the tools used in computer forensics for gathering digital evidence, viewing files of various formats, locating files needed for investigation, performing image and file conversions, handling evidence data, creating a disk image file of a hard disk partition, recovering deleted files from a hard disk, etc., as well as to gain practical skills in locating and examining evidence on devices and forensic images, analyzing and reporting findings. For that purpose the labs follow a cohesive scenario simulating a real IS incident investigation.

Based on the goals and complexity of tasks performed during the labs, the time required to complete the labs assignment is 4 hours (2 times 2 hours each in 2 different days). From our point of view it is sufficient to obtain the appropriate basic skills and abilities listed above. The work is divided into two days deliberately in order to teach the students to retain digital evidence in case they cannot be collected at one time.

At the time of labs one group of Masters is divided into a few subgroups (4 students in each subgroup), who are assigned to investigate different categories of IS incidents. When performing the labs, the students get assignments related to 6 categories of IS events when transferring money (leading to the specific IS incident types):

1. Identification and authentication of OBS administrators, customers and processes;
2. Access control to all II components used by OBS front-/back-office and clients;
3. Remote access to the II components;
4. Changing the state of the II components;
5. Anti-virus protection;
6. IPTs' functioning.

During a week before labs devoted to investigation of one predefined category of IS events the students of the same group, but from other subgroups (not assigned to study it), are invited to the laboratory at any working time to implement this event and create a lot of traffic and emulate a variety of suspicious activities. Before any actions taken, they should inform their instructor on what they are going to do and what specific tools they are going to use for that purpose and get his consent to this. Thus, everything that happens in the laboratory is under the constant supervision of the instructor and will not harm other users of the laboratory.

As a part of the labs, the students must collect and document the TDs for each detected IS incident of a specific type, which was given them by their instructor, and overview information about it (so called IS incident profile) describing the way they used to identify the IS incident; the source of information about the IS incident; the content of information about the IS incident received from the source; the scenario for the implementation of the IS incident; the date and time of IS incident detection; the II components involved in the implementation of the IS incident, as well as suffered from it, including the level of the IS incident severity for the object being selected by the students for labs; the ways to connect the II components involved in the implementation of the IS incident to the Internet (including information about an Internet service provider) or another University subnetworks, etc.

Before the TDs collection, the students must describe and fix by a camera (with a correct date and time stamp and information about its manufacturer, model and serial number) the TDs collection site, including the following: type, location, power state of the II components; availability and way of their connecting to networks, including wireless networks and the Internet; and information about events and processes on the II components displays (if applicable).

Based on our deep analysis of a huge number of different typical network attacks' scenarios that we conduct since 1995 and our 22-years experience of teaching network security at the NRNU MEPhI (one short note: our first textbook entitled "Vulnerabilities and Protection Methods in the Global Internet" was published in Russian in 1997), we work out our own IoCs for wide-spread IS incidents when transferring money using OBS. Further, we will no longer refer to our experience and long-term studies, but we will imply that the results presented are based on them.

Thus, the students must collect, analyze and document the following TDs containing these IoCs, specific for the event category assigned to them:

- Nonvolatile TDs located on the II components' memories (including those used to maintain the functioning and administration of the network, not just OBS);
- Volatile TDs located in the RAM of the II components and volatile TDs of the II components' operating systems (OS): data on network configurations and connections, running software processes, open files; list of open access sessions; system date and time;
- Logs of database management systems (DBMS); network equipment used in the network: routers, switches, wireless access points and controllers, modems; tools used to provide remote access (VPN gateways); DHCP services; IPTs used on the II components: authentication, authorization and access control tools; IPTs against unauthorized access; firewalls; IDPSs; antiviruses; cryptographic IPTs;
- Logs and data of mail servers and e-mail content filtering tools as well as web-servers and web protocols content filtering tools;
- Network traffic data (its copy and/or headers) from/to a network segment, in which the II components are located and so on.

To collect the TDs, the following scenario of the students' actions was developed:

- Disconnecting the II components (their network cable) from the network and/or turning off the network devices (including Wi-Fi/Bluetooth adapter, etc.);
- Forensic copying of volatile TDs from the II components, including copying the contents of RAM and copying OS data;
- Disconnecting the II components by interrupting the power supply (disconnecting the power cord or removing the battery), disconnecting the network cable (for the use of network interfaces supporting power over the computer network, for example, Power over Ethernet), and then removing the memory devices;
- Copying of IPTs' logs and network traffic;
- Forensic copying (creation of images) of nonvolatile TDs of the II components' memory devices by bit copying and/or "bit-copy plus" copying, including copying (creating images) of hard magnetic disks of the II components.

The detailed recommendations for the students were worked out and are given to them in advance to provide the opportunity to be better prepared to work and demonstrate their knowledge on the progress test after it. For example, the specific recommendations for copying the logs, in most cases stored as data files, are the following:

1. The choice of storage media and repositories for collecting the logs of sufficient capacity, that allows to avoid the rewriting and/or loss of information significant for the purpose of responding to IS incidents;
2. Connection to the monitored object via the console port (performing remote connection via Telnet or SSH protocols is not recommended), and it is strictly recommended not to change its current configuration by entering any commands;
3. Uploading (copying) of logs for a certain required period of time in data files;
4. Calculation and saving of checksums or hashes for the copied data files;
5. Logical copying to external media (compact disks) of the source data files created at step 1;
6. Calculation and saving of checksums or hashes of the source data files created at step 1, and collection of data files copied ay step 3, comparing the calculated values with the values calculated at step 2, to confirm the integrity of the copied data with the written fixing of the results of this comparison;
7. Ensuring the adoption of all necessary measures to restrict access to collected data copies and the safe packaging and storage of information carriers containing them.

In order to complete the labs successfully, students of one subgroup must demonstrate their joint report with the results obtained, indicate each student's contribution and pass quizzes. All this forms an assessment of each student separately.

After the labs completion, the computers should be restored to their original condition by the same subgroup of students, whom prepared it for investigation before.

7 RECOMMENDED STRATEGIES FOR TDS'S ANALYSIS

To conduct an in-depth analysis of the collected TDs, the students are recommended the following general strategies as well as scripting experience (Python, Perl, Ruby, etc), which will help them to automate the analysis and reporting of results from the tasks performed.

The analysis strategy in a certain time range, which can be used if there is information about the date and time of the initial (base) IS event or their group, and includes two methods: 1) Analysis of the content information about the attributes of data files to determine the composition of data files and the subsequent analysis of the contents of data files created and/or modified for the time range associated with the IS incident; and 2) analysis of the composition and content of the logs for the time range associated with the IS incident.

The analysis strategy of deliberately hidden data, which provides the following: conducting comparative analysis and discrepancies in the content of the headers of data files (file header), data file extensions and structures; analysis of the structure and content of encrypted data files, data files protected by passwords (including ar-

chives) and data files, the contents of which are generated using steganography; analysis of information from hidden areas of hard disk drives (host-protected area, HPA); analysis of objects embedded in data files (for example, in document files); and analysis of the possible data file allocation in non-standard places in the file system.

The strategy of comparative (correlation) analysis of data files and applications, which provides the following: comparison of the composition of data files with installed applications; comparative analysis of the composition and integrity of executable data files based on the calculation of hashes and reference values; analysis of possible relations between data files and/or applications, for example, correlation of data logs of using the Internet with cache files, and data files with files contained in the attachment of e-mail messages; and identification of unknown types of data files.

For each IS incident type studied during labs, special recommendations have been developed for the students concerning the content (semantic information) that should be given special attention in the analysis. Thus, when analyzing the destructive impact of computer viruses on the II components for OBS, the students are encouraged to pay special attention to the following:

- The date and time when computer viruses appeared on the II components;
- Detection of computer viruses by antivirus, their classification by the antivirus manufacturer and the initial location of the detected components of computer viruses on the II components;
- The presence of infected files in the antiviral "quarantine" for the date range;
- The presence of extraneous software processes similar to system processes, but launched either from an uncommon place (temporary folders, folders of roaming profiles), or software processes that have a similar name to system ones;
- The presence of files and folders similar to system files and folders, but located in a different place than the standard location in the file system (for example, the Windows Update folder in the root of the Windows folder);
- The presence of uncharacteristic software launching at the II component's OS startup in startup folders, services, system drivers, the Windows registry, the task scheduler and other specific places defined by the OS type;
- The presence of a small volume of constant and/or periodic outgoing/incoming network traffic to network addresses outside/in Russia, not belonging to the list of IP addresses being maintained for an authorized data exchange;
- The presence of devices' connection data in OS's or specialized software logs;
- Atypical network traffic routes; non-typical routing tables for network devices;
- The presence of incoming messages in e-mail server logs from e-mail addresses that have a similar spelling to the government agencies' domains, or from domains, correspondence with which is not characteristic for the organization; etc.

8 INVESTIGATIVE SOFTWARE

The STO BR IBBS-1.3-2016 [3], adopted and put into effect since 2017, was taken as the basis of the software list, from which the students is recommended to make their

choice. This list contains some of the most common and well-proven tools like Forensic Toolkit (FTK) from AccessData and it can be extended by EnCase from Guidance Software, Forensic Recovery of Evidence Device (FRED) from Digital Intelligence, the Velocity series from Tritech Forensics. These tools are available in many configurations and range in price (3,000-16,000 $ and above). We give some names of a specific open-source and commercial tools being a base for performing the tasks by the students. They should use them or if they are paid they should find their freeware analogues available on the Internet (of course, the success of this Task 0 is also evaluated by the instructor). Thus, the list below will be constantly expanded and updated.

Task 1. Perform a forensic copy (create an image) of the II components' memory devices using the following software tools or their free analogues for:

- A forensic copy: for Linux (L): dd (stands for Data Duplicator) and dc3dd; for Windows (W): FTK Imager, The Sleuth Kit, EnCase Forensic Imager and Redline; W+L: Belkasoft Evidence Center;
- Calculating hashes: L: md5sum and sha256sum; W: Memoryze; W+L: dff;
- "Write-blocker"/"Forensic bridge": W+L: Raptor; dff.

Task 2. Copy the contents of the RAM of the II components and collecting the OS data using the following software tools or their free analogues for:

- Copying the RAM content: W: FTK Imager, Redline, MoonSols Windows Memory Toolkit and Memoryze; W+L: dff and Belkasoft Evidence Center;
- Collecting the OS data on network configurations: L: ifconfig and arp; W: ipconfig, netstat, arp, route and Sysinternals; W+L: Rekall Memory Forensic Framework and Volatility Framework;
- Collecting the OS data on 1) network connections: W: nbstat, net and Sysinternals; W+L: netstat, Rekall Memory Forensic Framework and Volatility Framework; 2) running processes: W: Task Manager, Memoryze and Sysinternals; L: ps, top and w; W+L: dff, Rekall Memory Forensic Framework and Volatility Framework; 3) open files: W: Sysinternals; L: lsof; W+L: Rekall Memory Forensic Framework and Volatility Framework; 4) open access sessions: W: netstat and Sysinternals; L: w; W+L: Rekall Memory Forensic Framework and Volatility Framework;
- Collecting data on registered users, the time of their last authentication: W: net and Sysinternals; L: last, lastlog, who and w;
- Collecting the OS system date and time: W: date, time, nlsinfo and Sysinternals; L: date; W+L: Rekall Memory Forensic Framework and Volatility Framework.

Task 3. Collect data about the attributes and structure of OS files using the following software tools or their free analogues:

- L: file; W+L: dff, Belkasoft Evidence Center and The Sleuth Kit;
- For analysis of files: executable: packerid, pescanner, exescan, PEiD, PeStudio, CFF Explorer; PDF: PeePDF, PDFiD, AnalyzePDF, pdfextract, pdfwalker, pyew, pdf-parser, pdf.py, pdfsh, Malzilla; MS Office: OfficeMalScanner, Offvis, peOLEScanner; graphic: Photo Investigator, Adroit Photo Forensics, Exiftool.

Task 4. Analyze logs for registering web servers and proxy servers using the Log Analysis Tool Kit (LATK).

Task 5. Copy and analyze network traffic using the following software tools: packet sniffers like tcpdump and Wireshark (W+L); W+L: ntop; L: Network Miner, Foremost and Kismet; ssldump (for SSL/TLS traffic); DINO (for visualization of network connections and IP address geolocation).

Task 6. Analyze anomalous/malicious actions of files using Cockoo Sandbox.

Task 7. Analyze the Cisco network equipment used in the laboratory: show (with keys clock detail, version, running-config, users, who, log, debug, processes, ip route, ip ospf, ip bgp, ip arp, interfaces, ip sockets, tcp brief all, ip nat translations, snmp…).

Task 8. Analyze mobile devices in the laboratory: Belkasoft Evidence Center (demo is available), .XRY for iOS, Android, Windows Phone, Blackberry.

Task 9. Identify the owner of an IP/DNS address: web service whois; traceroute for Linux and tracert for Windows; ip source-track for Cisco routers.

Task 10. Analyze the collected TDs using the following software tools or their free analogues: REMnux, PALADIN Forensic Suite, which contain a number of software tools specified above that allow analysis of malicious and suspicious files, creation of forensic copies of RAM, memory devices and network traffic.

9 THE LABORATORY TESTBED

The idea of giving our students an opportunity to gain practical experience in collecting and analyzing the TDs for further response to IS incident when transferring money using OBS by the way of hands-on labs lies in building and maintaining a suitable for training labs' environment. It is a daunting undertaking due to the many considerations that must be made to include room requirements, software, hardware, peripherals, devices, network topography and many other things. Our testbed is able to effectively facilitate student learning, meeting the following main requirements:

- Profitability, as the cost of forensic tools used in the laboratory should be significantly less (or even free of charge) than their cost for the real networks;
- Flexibility, as its structure should be easily reconfigurable: different labs' tasks require specific network topologies and host configurations (that is why we decided not to draw any schemes as it is one of the first tasks for the students to conduct mapping of the network under investigation);
- Scalability, for investigating all 6 categories of IS events. During one lab only one assignment to investigate only one category of IS events is fulfilled by 4 students from the main subgroup. The remaining students observe the process and can give their advice when the instructor permits;
- Reliability, as the laboratory should be able to easily recover from permitted for investigation damage by the students, as well as be able to quickly restore the default settings and network configurations for another subsequent use;
- Isolation, as the internal testbed should be isolated from the remaining part of the NSIC and not affect its operation. Each student works within the same testbed and his work should not cause any inconvenience to other NSIC users.

We deliberately do not draw the testbed's diagram here, because it will be different for six different investigations. But for all investigations its hardware includes 16 PCs on the basis of Intel Core i3 with 4 GB RAM, 500 GB of HDD, Gigabyte graphic card and DVD-ROM drives (we are going to upgrade them in 2018), and one lightweight mobile forensic workstation using a laptop PC (Lenovo ThinkPad T450s) with USB 2.0/3.0 ports and Wireless Network Interface Card.

As for the software: 16 PCs and the laptop have access to Windows and Linux installations either as a virtual machine or on the PC directly. PDF reader, MS Office, special viewers, a decompression tool that can handle a wide variety of formats (tar, gzip, bzip, RAR, etc) and all typical software are installed on all computers. For the educational purposes a few licenses for the OBS system were provided by our partners, but they asked not to disclose its name. In general, depending on the monetary constraints, the PCs in the testbed can be outfitted with different software solutions that range from commercial investigative suites to free command line tools. In much the same way, the forensic PCs that will be running the software can be vendor supplied standalone units or can be built with individual components in house [12].

10 CONCLUSION

The relevance of specialized computer forensic labs for the "Information Security Incident Management" course was determined by the urgent needs to develop more enhanced students' practical skills within the NRNU MEPhI's NSIC. We emphasize once again that we developed only one but very useful for that purposes lab with six different assignments for 6 subgroups within one student group; so it makes no sense to compare it with long-term courses of the recognized training centers specializing in forensic studies – we just learned their best practices. As for privacy, it is a separate issue that requires special study and it is out of this technically-focused paper's scope.

Our labs have two undoubted advantages: their descriptions are presented in Russian and they take into account the specifics of IS incidents for OBS as much as possible. The originality of our results is using the scenario of money transfers as a way of engaging students in a specific risk-laden activity performed globally.

One of our findings is that the successful construction and management of the testbed can be accomplished even with a small budget so long as focus remains on students' skills. The labs have been successfully tested in 2018 spring semester by two groups the 2nd year Masters during their Internship (totally 40 students). Their validation demonstrates that the proposed scenario truly works within the student groups and testbed described. All the students perform the labs with great interest.

We shared our short-term experience in designing the labs – it is a "work-in-progress" and there is still much to do. Our future work is intended to develop a unique cloud-based learning platform for investigating IS incidents and on this basis to deepen and increase the number of investigations being conducted by students.

Acknowledgement. This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

11 REFERENCES

1. ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.
2. Bank of Russia Standard STO BR IBBS-1.3-2016 "Maintenance of Information Security of the Russian Banking System Organizations. Collection and Analysis of Technical Data When Responding to Information Security Incidents during Money Transfer".
3. Miloslavskaya N., Tolstoy A., Migalin A. "Network Security Intelligence" Educational and Research Center. In: Information Security Education for a Global Digital Society. WISE 2017. IFIP AICT, Vol. 503. Springer. Pp. 157-168.
4. Yasinsac A., Erbacher R.F., Marks D.G., Pollitt M.M., Sommer P.M. Computer Forensics Education. IEEE Security and Privacy. Vol. 1, N 4 (Jul. 2003). Pp. 15-23.
5. McGuire T.J., Murff K.N. Issues in the development of a digital forensics curriculum. Journal of Computing Sciences in Colleges. Vol. 22, N 2 (Dec. 2006). Pp. 274-280.
6. Batten L., Pan L. Teaching Digital Forensics to Undergraduate Students. IEEE Security and Privacy. Vol. 6, N 3 (May. 2008). Pp. 54-56.
7. Wassenaar D., Woo D., Wu P. A certificate program in computer forensics. Journal of Computing Sciences in Colleges. Vol. 24, N 4 (Apr. 2009). Pp. 158-167.
8. Digital Intelligence Computer Forensics Training. Available at: https://www.digitalintelligence.com/forensictraining.php (accessed 22.06.2018).
9. InfoSec Institute's Authorized Computer Forensics Boot Camp. Available at: https://www.infosecinstitute.com/courses/ (accessed 22.06.2018).
10. Computer and Hacking Forensics. Available at: https://www.cybrary.it/ course/computer-hacking-forensics-analyst/+ (accessed 22.06.2018).
11. Scott S. Implementing a Digital Forensics Lab in Education. Available at: http://www.infosecwriters.com/Papers/SScott_Forensics_Lab_in_Education.pdf (accessed 22.06.2018).
12. Lawrence K., Chi H. Framework for the design of web-based learning for digital forensics labs. Proceedings of the 47th Annual ACM Southeast Regional Conference. March 19-21, 2009. Clemson, SC.
13. Floyd K.. Yerby J. Development of a Digital Forensics Lab to Support Active Learning. In: Southern Association for Information Systems (SAIS) 2014 Proceedings, 2014.
14. DFIR Training & Courses. Available at: https://digital-forensics.sans.org/training (accessed 22.06.2018).
15. Forensic Tool Kit. Available at: http://accessdata.com/training (accessed 22.06.2018).
16. List of Free Online Computer Forensics Courses and Classes. Available at: https://study.com/articles/List_of_Free_Online_Computer_Forensics_Courses_and_Classes.html (accessed 22.06.2018).
17. Manson D., Carlin A., Ramos S., Gyger A., Kaufman M., Treichelt J. Is the Open Way a Better Way? Digital Forensics Using Open Source Tools. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS 2007), January 3-6, 2007, Waikoloa, Big Island, Hawaii, USA. IEEE Computer Society. P. 266.
18. Austin R.D. Digital forensics on the cheap: teaching forensics using open source tools. Proceedings of the 4th Annual Conference on Information Security Curriculum Development (InfoSecCD'07), September 28, 2007, Kennesaw, Georgia, ACM, NY. Pp. 1-5.