LABORATORY SUPPORT FOR INFORMATION SECURITY EDUCATION

Natalia Miloslavskaya, Alexander Tolstoy, Dmitriy Ushakov
Moscow Engineering Physics Institute (State University)
{milmur; ait; udv}@mephi.edu

Abstract: The Information Security Faculty of MEPhI has felt the necessity of designing educational environment for teaching information and network technologies and their security. MEPhI has already designed and implemented the Network Security Scientific and Research Laboratory, It consists of several logical segments: the Internet emulation segment, teams segments for mutual attacks and defense, control segment (a workplace of the administrator/instructor and entrance to the Internet), Distance Learning System and transport medium connecting all the segments. We defined traditional and distance educational courses utilizing the Laboratory, study objects and methods, preliminaries and resulting knowledge and skills, configuration of student/administrator working places, topology, methodical maintenance, scientific and research works, and technical support. Laboratory users carry out the following works: vulnerability and security testing and computer-aided testing facilities; familiarization with instruments used for ensuring system security; design of secure systems and subsystems. Several electronic tutorials for the different parts of the information security educational courses have been created.

Key words: security education, information security, network security, laboratory support, distance learning

1. INTRODUCTION

The Information Security Faculty of the Moscow Engineering Physics Institute (State University) (MEPhI) has felt the necessity of designing new educational environment for teaching information and network technologies. Higher education is undergoing structural changes in terms of not only

student populations, but of learning paradigms and curricula. The student becomes an active participant in the classes. We need a testing area for student practices today more than ever, especially for the educational courses on computer and network security. This testing area should be "a real world in miniature" ready to different experiments on the network attacks and protection techniques that we cannot permit to our students in the real world of the University intranet or the global Internet. This is not surprising as it has pretty high theoretical foundation and at the same time has lacked any practical training. Of course, students were taught lectures, were recommended extra literature. Even various ways of implementing the obtained knowledge in everyday experience were described to them. Never the less we have to admit that all those activities are not sufficient nowadays. Applying for a job the person who has worked with the real equipment, who has designed and implemented even a small project, who is more or less familiar with the software in use, will undoubtedly have advantages over others. So, in fact, till now the students could oblige the knowledge and experience that they have got only to themselves, mainly because those knowledge and experience had been obtained with their own hands at the expense of aside activities during their free time.

MEPhI together with the Moscow's Microsoft representatives and some Russian commercial companies (such as STC Electron-service and CROC) has already opened the "Network Security" Scientific and Research Laboratory last year. Its main goal is to implement the "education-science-business" approach in practice. This, in turn, means:

1. new level of scientific and research activities of the MEPhI faculty;
2. increase of efficiency of specialist training in the group of "Information security" specialties and refreshing stuff training in the field of "security of information technologies";
3. adjustment of new educational technologies.

Having such a Laboratory, it is possible not only to continue the training of specialists in specialties "Complex protection of informatization objects", "Complex information security of computer-based systems" and "Computer security", but also increase its qualitative level. And having monthly personnel retraining courses for the Bank of Russia, Sberbank, Vnesheconombank, etc. on the basis of the faculty, it is possible to significantly increase the results of that training with the help of, for example, expansion of practical training or carrying out extra laboratory works.

Owing to such a considerable support we can use new educational technologies, for example, distance learning, distance progress testing (certification) and informational support of educational process.

Thus, there is evident increase of efficiency of specialist training and

success in adjustment of new educational technologies. Students and even instructors themselves get real assistance in improvement of their theoretical and practical professional skill.

2. LABORATORY DESIGN

When only limited resources are available accurate planning and projection are a must for the most effective way of utilization those resources and high-quality implementation of the project. We defined the following stages of creation of the "Network Security" Scientific and Research Laboratory (further complex): preproject and projection stages, search for partners, project adjustment, assembling and start-and-adjustment work, presentation; operation testing and operation.

At the preproject stage the aforenamed Laboratory design premises were explored and the necessity of its creation was motivated. The project stage followed. It, in turn, included several stages at which the undermentioned points were defined:

- goals and tasks for the complex creation;
- educational courses utilizing the complex;
- objects and methods of Laboratory studies;
- preliminaries and resulting knowledge and skills;
- models of intruders, attack scenarios => necessary hardware configurations;
- configuration of working place of administrator and instructor;
- structure of complex;
- firmware requirements and specifications;
- teaching and methodical maintenance for laboratory, scientific and research works (textbooks, tutorials, policies, etc.);
- support of complex operation.

That is the projection stage related to compiling the logical project of the Laboratory and defining firmware requirements. At the same time after thorough analysis of the courses which will use the Laboratory the following main tasks for computer and network security education purposes were designated:

- research of the hardware, operating systems, data warehouses, software, and firmware and technical means of network protection;
- design of operational models of protected networks on the basis of new informational and network technologies on different platforms;
- adjustment of main methods and scenarios of distance learning and progress testing;
- creation of informational database of security technologies;

- education of users and students;
- detection of local and remote network attacks;
- analysis of mechanisms and means of attacks;
- discovery of channels of unauthorized information leaks from the system;
- definition of security policies and measures;
- elimination of the consequences of unauthorized intrusion into computer systems;
- evaluation of system's protectability;
- installation, configuration and administration of security equipment;
- development of new methods and systems for information protection;
- creation of "sandboxes" for temporary software and new technologies testing.

We know that "sandbox" laboratories for security education are not a new idea, however they are an excellent teaching and learning tool [for example 2, 3]. That is why we decided to implement it at the University.

To successfully carry out all those tasks the Laboratory should meet definite requirements. For example, when modeling secure networks it is essential to have sufficient flexibility of configuration and scalability, whereas when evaluating system's protectability and designing new methods of information protection – adaptability to new operational environment. Full list of project requirements was the following: maximum flexibility, simulation of various attacks, heterogeneity, low cost and availability.

The resulting logical structure of the complex satisfying all given requirements and able to carry out all listed tasks is depicted on the figure 1.

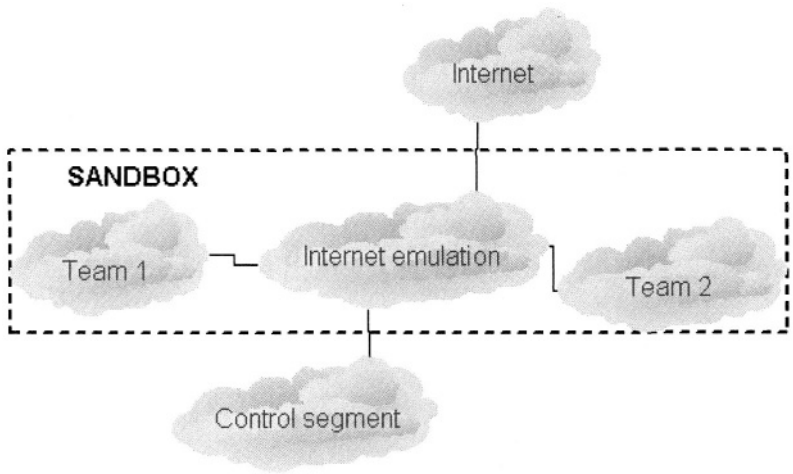

Fig.1: logical structure of the Laboratory.

Thus the Laboratory consists of several logical segments or areas performing different functions. This increases flexibility of the complex as a whole and allows its easy modification and/or expansion to fit new needs. The complex includes:

1. Internet emulation segment – a model of public data network.
2. "Team 1" and "Team 2" segments – for mutual attacks and defense.
3. Control segment – workplace of the administrator/instructor and glue to the Internet.
4. Transport medium, connecting all segments.

All segments include appropriate security equipment, the ultimate make-up being defined by the current solved problems.

Internet emulation segment plays the role of public data network and is the transit area, passing all the traffic of participating parties. That is why it is a proper location for various informational warehouses, "public" servers (DNS, proxy, Web, etc.) and a management system. The management system controls operations of the segment and executes the established security policy.

Team segments simulate different corporate subnets with typical for today set of work stations and network services. These segments play the roles of attacked networks, attacking networks or perform other functions (for example, serve as mini-sandboxes for temporary software testing). Accordingly team segments should contain the following widely used modern firmware:

- workstation software (OS on the most popular and probable platforms – Microsoft, Unix, Novell; as well as Web-browsers and other software necessary for the problem solution);
- communication facilities (may be absent if segment is being used as an "isolated" area);
- databases (Oracle, Informix, MS SQL, MySQL, etc. – the ultimate choice is defined by the problem being solved);
- e-mail facilities (servers and client software);
- different servers (application, Web-, file- and other, not yet defined);
- security subsystems and firmware security facilities;
- programming tools (for analysis of the existing and creation of own security facilities, for analysis of vulnerabilities and various technologies);
- adaptive network security and management tools, including systems for evaluation of protectability, for monitoring user activity, systems for traffic analysis and intrusion detection.

Control segment is the working place of the administrator (an instructor will play his role during the laboratory works) and controls access of participating subjects to external (relative to the complex) services (for

example, the Internet). That is why this area should include adaptive network security and management tools, security subsystems and firmware security facilities, e-mail facilities and other servers.

All segments are linked into a single complex with the transport medium, which should be built with the most popular technologies used nowadays in private networks (intranet). In our case the transport medium is Ethernet because it is the most flexible, cheap, and scalable technology able to satisfy nearly all speed and QoS requirements.

Team segments (and the control segment) use various software varying from freeware, downloaded from the Internet for analysis, to licensed operating systems and security facilities (for example, network audit tools, software firewalls, antiviral software, etc.). Besides, organization of the unified database about all investigated vulnerabilities and methods of defense, about used firmware, as well as maintenance of centralized support server in the control segment are of special interest.

Implementation stage followed the project stage. But the faculty was unable to afford the self-dependent creation of the Laboratory because of limited resources. That is why executives addressed exterior organizations. They needed to open business relations and to attract investments. This was the search for partners' stage. The partners had to be interested in the creation of the Laboratory, maintaining it, at least because they could use it as a test-bed for their new ideas and shift their everyday routine research and testing activities to students' and post-graduate's shoulders. The partners were found (they are the Moscow's Microsoft representatives, the STC Electron-Service and the CROC company), but they made some modifications to the initial Laboratory topology so that it would be more flexible and more effective for solving various problems.

The final project of the complex compiled by the joint efforts is depicted on the figure 2.

All that was made by the students themselves. During the summer months the work was finished and the complex was ready for presentation and operation testing.

The Laboratory is divided in two main parts. One part of the Laboratory is designed for carrying out the following works within the complex's framework:

- examination of system vulnerabilities and analysis of unauthorized access to computers and networks;
- security testing and computer-aided testing facilities;
- extending students' knowledge of security concepts and principles;
- familiarization with instruments used for ensuring system security;
- design of secure systems and subsystems.

The second part of the Laboratory is intended for improvement of the

basic techniques and scripts of distance learning and testing. Some new educational technologies based on multimedia computer systems and tools are widely used in many educational programs of various educational institutions from primary schools to universities. Their efficiency has already been proved in teaching foreign languages, in physical processes and phenomena simulation, and also as help-systems with a large amount of stored information. The application areas of computer learning systems along with many other fields of knowledge can become objects of study not only in classes but also during independent student's (or trainee's) work.

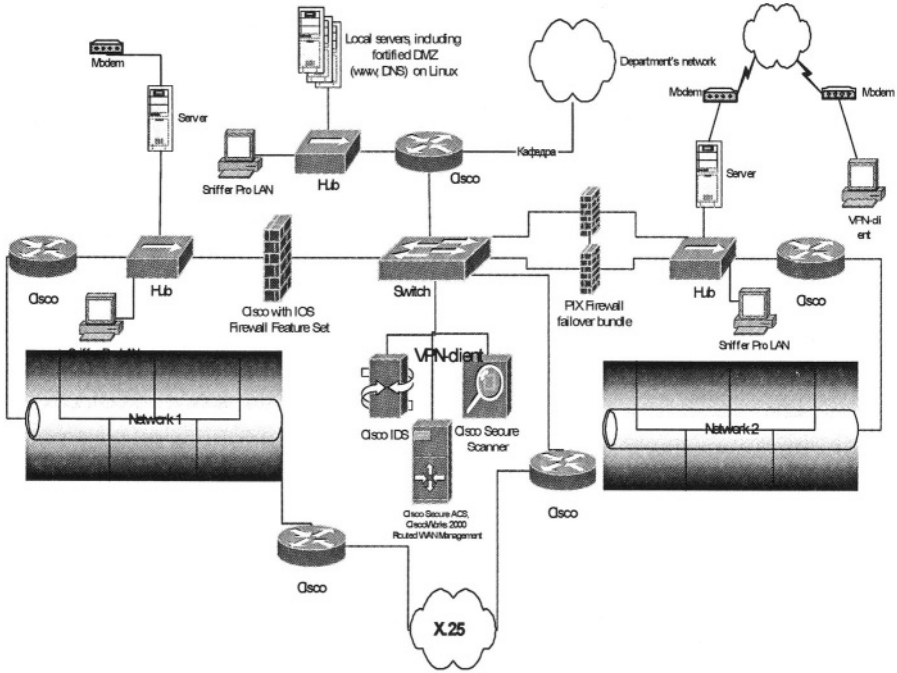

Fig.2: final Laboratory topology.

The basis of this part of the Laboratory is earlier developed at MEPhI's Distance Learning and Testing Systems (DLTS). It is a complex of software and methodical tools for distance learning and certification of the personnel based on the advanced Internet technologies and modern educational and testing techniques and accompanied by the specially trained personnel. Interactive DLTS Web site is constructed upon the Microsoft ASP technology. The Internet Information Server 5.0 provides the ASP support. VBScript language is used for the ASP scripts creation. The DLTS information environment consists of the educational material in the HTML

format and the centralized database working under the Microsoft SQL Server 2000 control. The tools for new educational course development, the test creation tools and DLTS operation support tools are implemented as the Internet and Delphi applications. All DLTS's resources should be protected. That is why it is located in the Laboratory.

MEPhI's DLTS has more that 1500 tests on the different topics of the information and network security. We define test as a combination of interdependent or independent tasks of equal or different complexity, assigned "from simple to complicated", and allows adequately defining knowledge and other trainee characteristics important for the tutor (they are named in the brackets). The tests have the following aims:

- self-testing of trainees during the educational process on the information security programs,
- testing the level of preliminary training (so called pre-knowledge) before the laboratory works,
- testing comprehension of the studied theoretical material as addition to another forms of traditional progress testing during a term,
- testing student's ability to apply the newly acquired knowledge and skills for making own decisions and implement them as completed products and work out concepts, strategies, techniques etc.,
- certifying trainees and testing their competence as the final progress testing.

MEPhI's DLTS implements the following task types of different complexity: selection from a set, multiple selection, conformity, logical chain, term, object selection, situational task, symbol sequences input. We added one interesting point to that list – dialogue emulation. It is not trivial to implement it because all the possible actions of a trainee and emulated system process reactions should be determined in advance. We need to foresee all possible event development in artificially created situations. But that approach has positive features - trainee's practical experiments do not impact the real parameters of the network environment.

3. LABORATORY ACTIVITIES

Even now the Laboratory is used not only in "exterior" projects but also directly participates (or will participate in the nearest future) in student training in the following educational courses:

- "Information security basics",
- "Theoretical foundations of information security",
- "Operating system security",
- "Network security",

- "Database security",
- "Complex information security of computer-based systems",
- "Cryptographic tools of information protection",
- "Technical methods and tools of information security",
- "Firmware methods and tools of information security",
- "Legal aspects of information security",
- "Organization of information security" and
- "Building secure computer-based systems".

Besides there are plans to introduce the following new courses: "Secure network technologies", "Monitoring of network security", "VPN management", "Informational and mail systems", "Information security administrators", "Building data networks" and "Network management tools".

But the most important are, probably, the knowledge that trainees could learn in the Laboratory. For example, it allows to obtain knowledge in the undermentioned areas:

- reveal unauthorized computer access;
- reveal network attacks;
- analyze the procedures and means for performing attacks;
- discover threats to informational computer systems;
- discover vulnerabilities and bugs in systems, services and network protocols through which adversary's intrusion can be expected;
- discover channels of unauthorized information leaks from the system;
- perform the network security monitoring;
- operate the access isolation systems providing a controlled access to informational and network resources;
- design secure informational systems;
- elaborate the system's security policy;
- define measures and procedures of accident prevention;
- eliminate the consequences of unauthorized intrusion into a system;
- evaluate the system protectability;
- define the purpose, basic functions and place of information security standards in the system; usage peculiarities of the specific standard;
- evaluate the functional capabilities of the existing security equipment and determine the applicability of firmware in network architectures;
- configure the security facilities built into many systems;
- ensure the secure operation of system applications;
- administer security equipment;
- develop methods of defense;
- implement new systems and means of information protection;
- know the basic legal documents and standards in information security;
- prepare documentation for new security equipment for further state level certification.

This is not a comprehensive enumeration. But even it should not be understood literally because every student will choose his own specialization and questions that he will thoroughly study. It is just impossible to be a specialist in every field. Never the less all students will obtain the necessary minimum of knowledge in the aforementioned problems to continue independent studies and research.

But to make the most of working in the Laboratory, without distracting attention to "secondary" questions when solving definite problems, there is a list of prerequisites: TCP/IP stack, network services, basic principles of network security and technologies of security, network operating systems (Unix, Windows 98/2000, NT, Netware...), database management systems, computer viruses (malware) and programming technologies and languages.

The following works are going to be carried out within the complex's framework:

- examination of system vulnerabilities and analysis of unauthorized access to computers and networks;
- security testing and computer-aided testing facilities;
- extending students' knowledge of security concepts and principles;
- familiarization with instruments used for ensuring system security;
- design of secure systems and subsystems.

Titles of the possible works are very different. For example, the work with the title "Buffer overflow attacks" is designed for the "Programming technologies" course. For the "Computer hardware" course functioning of packet filters, channel encryption devices and other hardware should be studied in the Laboratory. Revealing of leakage paths is a good illustration for the "Communication networks and systems" course. Analysis of OS's protectability and setup of configuration files corresponds to the "Operating systems" course. Specific DBMS threats and built-in protection capabilities are the main topics for the "Database management systems" course. Network attacks and methods of their detection best of all suits the "Computational networks" course. The "Management basics" course should imply designing of security policies and studying of the main administrator's responsibilities etc.

At that objects of Laboratory studies are network hardware & software, protocols & services, standards, legal and normative documents, standalone computers or groups of computers in the internal and external networks with specific hardware platform and installed software — primary (for example, OS) and applied (network), with the Internet access. As for protection hardware & software students should study means designed for intrusion detection, security monitoring and audit, protection means (such as firewalls, encryption tools), access control implementation, security policy development and, of course, document base, regulating actions in the field of

information security. This is achieved with the following methods of research:

- emulating intruder's activities;
- discovery of system vulnerabilities by scanning and probing;
- experiments with security facilities and means of unauthorized access detection to determine their functional capabilities and to elaborate recommendations for their installation and improvement;
- control of network information flows through traffic analysis;
- assessment of protection of computers, networks, services, protocols, hardware and software in accordance with fixed procedures and in compliance with Russian standards and guidelines;
- testing of security policies and new procedures of protection in order to determine their comprehensiveness and validity;
- analysis of documents, regulating information security.

With reference to learning network security this means:

- examination of standard attacks described in different publications;
- intrusion detection and elimination of their consequences;
- discovery of software and hardware vulnerabilities of standalone computers or network as a whole;
- operation of access control systems with respect to informational and network resources;
- elaboration of system security policy and definition of means of its achievement;
- evaluation of functioning systems' protectability and elaboration of recommendations for its enhancement;
- design, installation, configuration, and administration of security facilities and patches for present software and hardware.

On the basis of those typical basic tasks as well as on the basis of personal experience of complex design the following immediate problems were prepared for students. All of them are the titles of the practical assignments for one laboratory work.

1. Emulation of network protocols.
2. Emulation of secure network protocols.
3. Emulation of specific attacks.
4. Creation of interfaces emulating operation of security facilities.
5. Research of dependence between network topology and attacks.
6. Research of dependence between transport medium in use (Ethernet, FastEthernet, FDDI, ATM...) and attacks.
7. Research of peculiarities of telephone channel attacks.
8. Research of peculiarities of fiber-optic attacks.
9. Research of peculiarities of attacks from the Internet.
10. Research of attacks on network hardware.

11. Research of vulnerabilities and protection of Web-servers and applications.
12. Research of vulnerabilities of network services and commands.
13. Research of attacks on electronic document interchange.
14. Crypto protection. Digital signature. Public key infrastructure.
15. Research of attacks on firewalls.
16. Research of attacks on proxies and their detection.
17. Research of vulnerabilities of client/server architecture.
18. Research of vulnerabilities of databases and database management systems.
19. Research of basic means of network protection – protection against an unauthorized access.
20. Research of basic means of network protection – firewalls.
21. Research of basic means of network protection – adaptive network security.
22. Research of basic means of network protection – anti-viruses.
23. Research of basic means of network protection – virtual private networks.
24. Research of basic means of network protection – security policy development and management.
25. Research of means for file and session encryption.
26. Research of network-based intrusion detection systems.
27. Research of host-based intrusion detection systems.
28. Research of attacks on intrusion detection systems.
29. Research of system security scanners.
30. Research of network security scanners.
31. Research of security services: intrusion tests.
32. Research of application-level attacks and application protection.
33. Research of trusted operating systems.
34. Vulnerabilities and protection of workstations.
35. Design of own means and methods of defense.

4. ELECTRONIC TUTORIALS FOR INFORMATION SECURITY EDUCATION

Let's allocate main objectives of creating the electronic tutorials for information security educational process. They are the following:

– to help teachers to present their professional knowledge in a new, most effective — electronic — way that would give them necessary modern level and high quality of stated material;

- to apply teaching based on automated and involving extensive information resources of the Internet approaches to educational schedule exposition to students;
- to place students in such an environment, where they can creatively use this technology as a part of their daily exercises within the framework of self-education; students can actively construct their own knowledge setting their individual style of training and mastering of new information in this environment;
- to give state-of-the-art information on the theme at the expense of usage of hypertext references to Web-sites with the newest documents, demos of the latest software information protection tools for networks, and descriptions of functionality of hardware protection tools.

In 2003 several electronic tutorials used to study network security at the laboratory have been developed and tested on the under- and post-graduate students. Their themes are the following: "Secure network protocols", "Remote network attacks", "Firewalls", "Intrusion detection systems" and "Scanners". "Virtual private networks" tutorial is under construction now.

On an example of the first named tutorial we would like to show main features of the others. The product named ZSPs (from the Russian abbreviator of Secure Network Protocols) is used both to learn theory of the protocols and to get initial practice in their configuring (during laboratory works). To achieve the goal the emulation of the basic dialogs is performed. The main purpose of it is to make the education persistent and to exclude the gap between the theory and the practice. ZSPs gives the possibility to put through persistent educational process – students get the knowledge and use it in practical tasks immediately - and thereby increase the quality of education.

The ET is meant for those familiar with network technologies foundations, system and security managers. ZSPs is intended to be used by the students of the Information Security and Network Security specialties.

ZSPs is directed to study secure network protocols, tightly integrated in different network environments. It realizes some elements of client-server configuring of the basic network protocols such as creating PPTP and L2TP tunnels and IP Security connections. Windows 2000 Advanced Server has been chosen as the basic system, because it's one of the most widely used Microsoft OS for creating powerful and convenient network environments. The product aids in solving the following tasks in the common concept of learning: giving the basic knowledge in the protocols functioning, methods of their application and so giving skills in configuring network connections to use security services of them.

The configuring of protocols inside ZSPs does not impact the real parameters of the OS. The following reasons have chosen such kind of

realization:

As the inexperienced students use the application, there is the possibility of incorrect configuring the protocols, and thereby breaking the functioning of the whole complex.

As the product does not change the OS parameters, it can be used in any Windows system, and not only Windows 2000 Advanced Server.

ZSPs, emulating work of the basic network protocols, has the following characteristic features:

- Granting of an opportunity to receive both knowledge and practical skills.
- Independence from concrete OS and opportunity to be used in any Windows environment.
- Exclusion of the probability to infringe the OS under which the application is used.
- User-friendly interface.
- Realization of theory as HTML documents that allows the teacher to modify and supplement the material easily without a threat to the application.
- Help system, including instructions for tutors and trainees.
- Implementing the system of user registration, logging and reporting.
- Realization of a test system to examine trainees.

Subjects of teaching, as well as everything concerned with the modern networks, the Internet and intranets, are very dynamical: literally each day malefactors develop new methods of system breaking and crashing; in return the market of protection tools responds with releasing appropriate products for intrusion detection and defense. For the reason the dynamic principle should be incorporated into the basis of the approach to creating electronic tutorials on the given area of knowledge.

5. CONCLUSION

Thus, the "Network Security" Scientific and Research Laboratory allows not only to significantly improve student training in existing group of information security specialties, but also to bring the educational and research activities of the faculty up to a new standard. This results in both increased efficiency of training and retraining courses in old and new educational programs and participation in federal special programs. Besides, availability of the complex allows online exchanges of experience with foreign partners and to carry out joint investigation and research. Moreover, having mutual agreement it is possible to participate even in joint laboratory works when, for example, Russian and foreign students from Australia [2] or

Italy [3] compete with each other for better knowledge of network protocols, technologies, and network security tools. Several electronic tutorials for the different parts of the information security educational courses have been created.

REFERENCES

[1] Miloslavskaya N., Tolstoy A. "Network Security" Scientific and Research Laboratory" Proceeding of the IFIP TC11 WG11.8 Third World Conference on Information Security Education. 26-28 June 2003, Monterey, USA. Pp. 231-242.

[2] Armstrong C.J., Armstrong H.L. 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.

[3] Vigna.G. Teaching Network Security Through Live Exercises. Proceedings of the IFIP TC 11 WG 11.8 Third World Conference on Information Security Education, June 2003, Monterey, USA. Pp. 3-18.