Cybersecurity Specialists' E-learning Problems

Svyatoslav Birukov[1], Dmitry Vasilev[2(✉)], Lubov Kokoreva[3], Polina Shmarion[4], and Sergey Nikonovich[5]

[1] Volgograd State University, 100 Universitetskiy Avenue, Volgograd 400062, Russia
[2] Volgograd Academy of the Russian Ministry of Internal Affairs, 130 Istoricheskaya Street, Volgograd 400089, Russia
[3] Moscow Regional Branch, Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya, Moscow region, Ruzsky urban district, pos. Staroteryaevo Index, Volgograd 143100, Russia
[4] MIREA—Russian Technological University, Vernadskogo Avenue, 78, Moscow 119270, Russia
[5] Military University of the Ministry of Defense of the Russian Federation, St. B. Sadovaya, 14, Moscow 123001, Russia

Abstract. This article studies problems of data security e-learning systems. It covers the definition of e-learning and its attributes, as well as analyzes classifications of e-learning systems described in scientific literature, their advantages and downsides. It offers the main notions that need to be studied by cadets and attendees of non-technical programs within the Ministry of Internal Affairs educational system. It provides brief definitions and key methods of data protection that do not require special training.

Keywords: Data · Threat · Authorization · Cryptography · Electronic digital signature · Firewall

1 Introduction

In recent decades, information technologies have rapidly developed in all social spheres. Information is gradually becoming a more important strategic resource for the state and a demanded good. Like any other goods, data also need safety and reliable protection.

Data vulnerability in computer systems is caused by huge concentration of calculating resources, their spatial dispersion, long-term storage of large data volumes, simultaneous access of multiple users to computer system resources. Every day new threats are arising, so information security problems become more and more relevant [1].

Establishment of common information space, almost universal application of personal computers and introduction of computer systems determine the necessity to address the complex problem of data protection.

Various institutions of higher and professional education provide courses covering data security issues. Their content and educational approaches vary depending on specialty and preparedness of students.

© Springer Nature Switzerland AG 2021
A. G. Kravets et al. (Eds.): CIT&DS 2021, CCIS 1448, pp. 559–571, 2021.
https://doi.org/10.1007/978-3-030-87034-8_41

As higher educational institutions of Ministry of Internal Affairs are humanities-focused, it is necessary to determine how detailed this topic should be approached. This task requires taking into consideration not only the present situation concerning data security but also certain practical aspects. For instance, investigators regularly work with confidential data, however getting into technical specifics on data protection seems unreasonable, as these activities are beyond their responsibilities.

2 Data Security

Data protection in computer systems involves regular usage of systems, and methods as well as taking measures and actions to systemically uphold required safety of data stored and processed through computer equipment. The protected objects include data, storage devices and informational processes that need protection according to certain safety purposes.

Data security is understood as protection of information from unlawful familiarization, transformation and destruction, as well as protection of information resources from actions damaging their functionality. Data safety can be achieved by maintaining main properties of information: confidentiality, integrity, reliability and availability.

Confidentiality is the property indicating necessity for limiting data access to a certain group of people. In other words, it guarantees that transferred data would be known to lawful users only.

Integrity is the property of data to maintain content and/or structure during storage and transfer, so that they remain unchanged compared to some fixed state. Information can be created, transformed and destroyed only by an authorized person (a lawful user with access rights).

Reliability is the property understood as strict belonging of data to the subject that is either the source or submitter of these data.

Availability is the ability to provide users the well-timed and unobstructed access to required data [2].

Countering multiple threats to data security requires complex application of various organizational, legal, engineering and technical, hardware and software, cryptographical and other means and activities.

2.1 Information Security Complex

Organizational activities on data security include recruiting and training personnel to prepare and operate data and software, as well as regulating development and functioning of computer systems.

Legal measures and methods include effective laws and regulations imposing data handling rules and responsibility for their violation.

Engineering and technical means are diverse and consist of physical, technological, hardware, software, cryptographical and others. They establish the following lines of protection: controlled territory, building, area, specific devices and data storages.

Hardware and software security means are used directly in computers and computer networks and include various network-integrated electronic and electromechanical

devices. Specialized programs and packages implement such protection functions as limiting and controlling access to resources, registering and analyzing ongoing processes, events and users, preventing potential damage to resources, etc.

Cryptographic protection involves changing (transforming) information, making it implicit through special algorithms or hardware and encryption keys.

Software security is aimed at protecting data from the most common threats: unauthorized access, copying and malware (viruses). Computer systems are protected against unsanctioned intervention by so-called "three A's" (Authentication, Authorization and Accounting).

Authorization (sanctioning, permission) is the procedure, during which a user entering the system is recognized and gets rights specified by the system administrator to access certain resources (computers, discs, folders, peripheral equipment). Authorization is performed by software and consists of identification and authentication.

Identification means providing an identifier: a non-secret name, word or number for user registering. The subject inputs the username that is compared with the list of identifiers. The user who has an identifier registered in the system is considered as rightful (lawful). Identifiers are synonymous to logins: a combination of letters and digits, unique for a given system.

Authentication is the procedure confirming that the input identifier actually belongs to the subject, performed by comparing the username and the password. After the authentication, subjects are granted access to system resources according to permissions given to them [3].

The most common authorization methods are based on passwords (secret combinations of symbols). Launching a program or performing certain activities on a computer or in a network can be password-protected. Apart from passwords, plastic cards and smart cards can also be used for authentication.

Accounting involves registering user's network activities, including attempts to access certain resources. In order to prevent unsanctioned actions, the controlled compliance with access rights requires regular collection, documenting and providing upon request information on any access to protected computer resources. The main registering form is software-managed special logs - files on external storage devices.

There are different methods to prevent unsanctioned copying of data:

1. Countering reading of copied data. These methods are based on making certain features while recording data on storage devices (non-standard marking, storage device formatting, hardware key installation), so that copied data cannot be read on devices not belonging to the protected system. In other words, these methods maintain compatibility of storage devices only within a specified computer system.
2. Countering and hindering usage of copied software and data. The most effective protection method of this type involves storing data in a cryptographically transformed form. Another way to counter unsanctioned running of copied programs is to use software environment control unit. This unit is created during program installation and includes characteristics of environment, in which the program is located (computer device or data storage device characteristics), and means to compare these characteristics.

2.2 Varieties of Antivirus Programs

Special antivirus software has been developed to protect computer systems from malware. Antiviruses detect malware, offer to disinfect files and delete uncurable ones. There are several types of antivirus programs [4]:

1. scanners, or phages, are programs that search files, memory and boot sectors for virus signatures (unique program code of a particular virus), check and treat files;
2. monitors (type of scanners) check Random Access Memory (RAM) during operating system boot, automatically inspecting all files when they are getting opened or closed in order to prevent opening and recording infected files, as well as to block viruses;
3. immunizers prevent file infection by detecting suspicious activities during computer work, typical for early stages of infection (i.e., before the virus replicates) and inform the user on it;
4. inspectors memorize initial state of programs and catalogues before they were infected and compare it with their current condition on schedule (or upon user's request);
5. doctors not only detect infected files but also cure them by removing virus software from files, restoring their initial condition;
6. blockers track events and intercept suspicious activities (performed by a malware), prohibit such activities or request user's permission.

An effective way to counter various threats to data security is to apply cryptographic transformation. As a result, protected data become unavailable for familiarization and direct usage by unsanctioned persons.

For blocking threats coming from public systems, special hardware or software appliances are used, known as firewalls. A firewall enables to divide common network in two or more parts and implement a set of rules for transferring data package between parts of public network. Network protection fully blocks incoming traffic but allows internal users to freely communicate with the outside world. Firewalls are generally used to protect local networks from interventions from the Internet and perform four main functions:

1. filtering data on several levels;
2. using proxy servers that act as intermediaries and establish connection between access object and subject for further data transfer, while maintaining control and registering;
3. transmitting addresses in order to conceal actual internal addresses from outside parties;
4. registering events in special logs. The log analysis helps to document attempted violations of network data exchange and find the perpetrator.
5. SIEM systems (Event Collection and Correlation System) track suspicious activity both inside the circuit and outside.

To accomplish their task, modern SIEM systems use the following sources of information (Fig. 1) [5].

Intrusion Detection System (IDS), unlike firewalls, which operate on the basis of predefined policies, are used to monitor and detect suspicious activity. Thus, IDS can be called an important addition to the network security infrastructure. It is with the help of an intrusion detection system that an administrator will be able to detect unauthorized access (intrusion or network attack) to a computer system or network and take steps to prevent an attack [6].

IPS (Intrusion Prevention System) is based on IDS, that is, each IPS includes an IDS module.

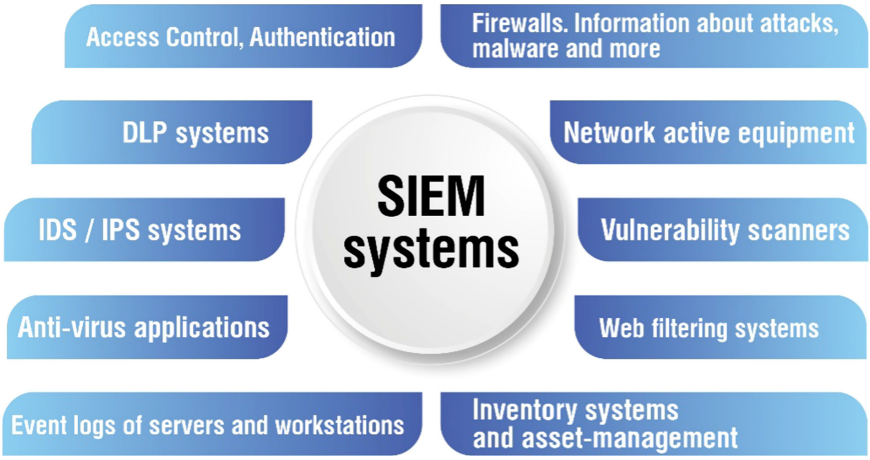

Fig. 1. Sources used in SIEM systems.

In terms of their functions, the systems are similar, but there are also differences:

- IDS is a "passive" solution that monitors network packets, ports, compares traffic with a certain set of rules and alerts when malicious actions are detected;
- IPS blocks malicious attacks from attempts to penetrate the network. If there is a risk of intrusion, the network connection is disconnected, or the user's session is blocked and access to IP addresses is stopped, account, service or application.

3 Problems of E-learning Systems

E-learning has been deeply integrated in modern educational process. It brings qualitative changes to traditional views on educational purposes, replacing acquisition and reproduction of teacher-provided information with students' independent search and assessment; changes to educational content by providing new knowledge and skills not through one-dimensional gradual retelling of textbook materials but through hypertextual implementation of individual learning trajectories; changes to educational methods by establishing an educational network as an intermediary between students and faculty stuff (Fig. 2). There is no doubt that defining the notion of e-learning and its differences

from other education types, revealing its psychological and pedagogical tendencies and developing classifications of e-learning systems are of great interest to pedagogical theory and practice.

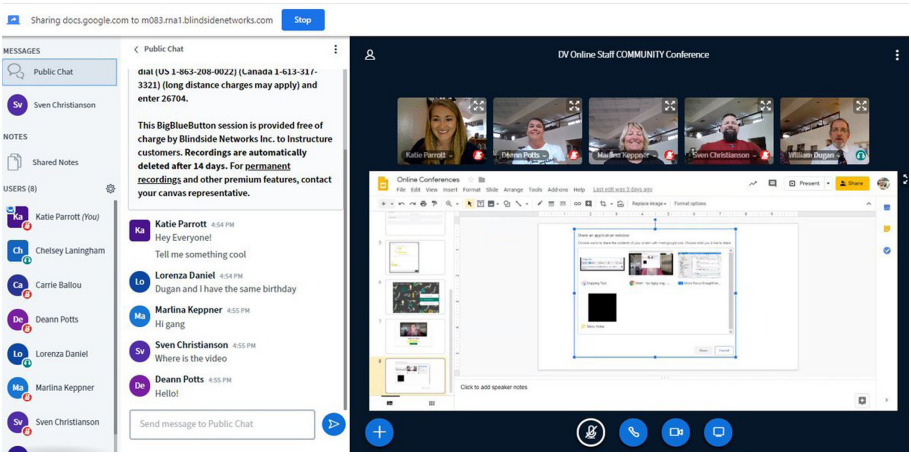

Fig. 2. Sample of the virtual classroom in BigBlueButton's platform [7].

Some researchers believe a full-fledged e-learning system consists of three standard modules: the learning management system (LMS), educational content (e-courses) and authoring tools. LMS is generally understood as an online platform enabling to upload various formats of electronic educational materials, differentiate access to files, control learning progress and task performance, facilitate interaction between participant via network communication, create electronic educational materials [8]. Educational content is commonly understood as a set of functional data blocks, interconnected according to specified rules. Authoring tools are means to developing educational content (e-textbooks, presentations, simulations, video trainings, test) that is uploaded to the LMS. There are several types of authoring tools: course editors, presentation programs, tools for creating tests, surveys and questionnaires, screen capture software, online seminar tools. As we can see, this model represents e-learning as a hierarchy comprised of learning tools only. On the contrary, other theorists focus on qualitative attributes of e-learning: interactivity, hypermedia, mobility, variability, multifunctionality, availability. It is worth noting that these characteristics describe not only procedural but also content-related aspects of e-learning.

In Russia, the definition of e-learning is stipulated by law – organization of educational activities involving information, contained in databases and applicable to educational programs, and implementation of information-processing technologies, equipment and ICT networks maintaining transfer of said data through communication lines in order to establish interaction between students and faculty stuff. Given this definition, we can conclude that e-learning process adopts educational databases technologies; educational information processing equipment and technologies; network technologies

transferring educational information via their channels; network technologies for interaction between students and faculty stuff. This allows to classify e-learning resources, learning systems using computer equipment, distant learning systems and systems of indirect student-teacher interaction as e-learning systems. This definition focuses on diversity of e-learning systems and considers distant learning to be a type of electronic education [9].

Classification of electronic courses by their purpose distinguishes managing, demonstrational, generating, operating, controlling and modeling types (Fig. 3).

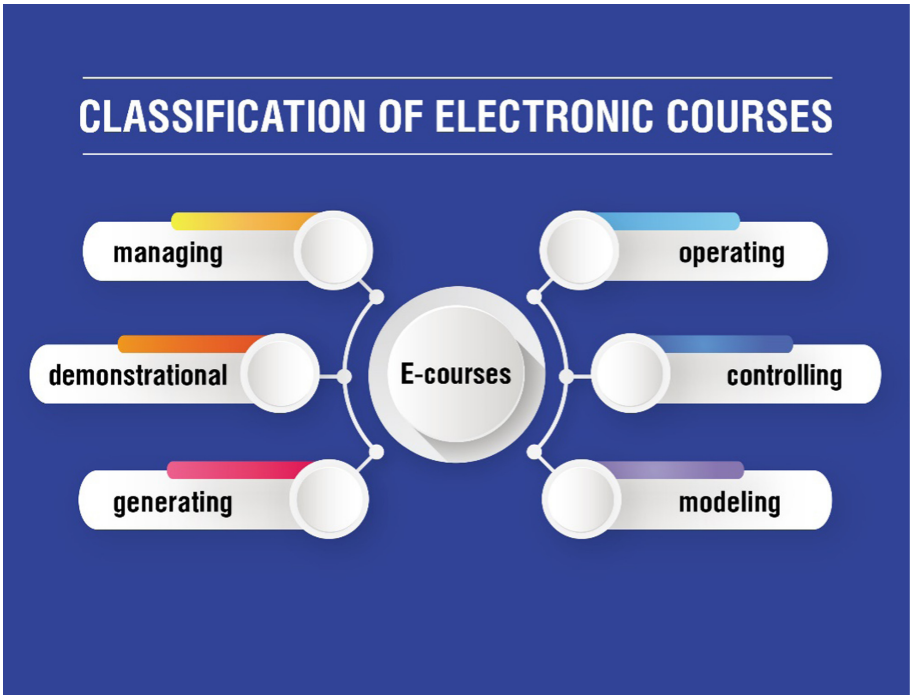

Fig. 3. Classification of electronic courses

Managing and demonstrational programs are aimed at managing learning process during classes, additional individual and group work. Demonstrational programs also give an opportunity to provide on-screen dynamic illustrations. Generating ones prepare a set of topic-related tasks, allowing to perform in-person tests or individual work, while providing each student with specific tasks according to their personal abilities. Operating programs give students an opportunity to set and perform tasks themselves via a computer, graphically illustrate studied notions, etc. Controlling ones are aimed at managing current or final examinations of students, helping to score assessment points, get feedback during the education, dynamically check performance of each students, compare study results with task difficulty, individual aspects of students, education rate, volume and type of study materials. Modeling programs imitate complex experiments and introduce students to research labs used by scientists, designers, architects, etc.

4 Improvement Data Protection Skills via Built-In Operating System Features

One of the basic ways to protect data is to use built-in OS functions. Modern operating systems have powerful built-in tools for security, authentication, authorization, audit of user activity, malfunction protection, cryptographic security of OS objects, network attack prevention. These functions are easy to apply and do not require profound technical skills from their users. This factor is important for teaching non-technical students, as federal standards for their education do not provision in-depth study of specialized disciplines that develop data protection knowledge skills.

Choosing the method of delivering topic materials requires determining objectives, number and format of classes. For instance, the main objective of the topic titled "Data protection via built-in operating system means" is to provide general knowledge on forms and methods of data protection via built-in OS tools, establish practical skills on cryptographic and password data protection, access rights differentiation and standard system recovery.

4.1 Data Protection via Built-In Operating System Means

Given these objectives, it seems reasonable to study this topic during a lecture and a practical class. The lecture should provide the basic description of OS functioning and an overview of its built-in data protection mechanisms. The practical class is recommended to be fully devoted to learning the simplest and most effective data protection tools, provided as part of OS delivery package.

In terms of methods for conducting the topical lecture, it seems sufficient to choose a classical approach, with gradual, structured material delivery and demonstration of specific examples. This is why we should give more attention to methods and order of practical study.

The key attribute of these practical learning methods is that during the class students must have full, unlimited access to all operating system resources, i.e., they should be given administrator rights. Thus, it seems necessary to isolate the system used for study from the main workstation system that is planned to be applied for performing educational tasks. The easiest way to establish a fully isolated system is to apply virtual machines.

Virtual machine technology helps to get rid of all restrictions and make experiments imitating system functioning as realistic as possible. Meanwhile, any mistakes that can be possibly made by students will not cause a malfunction of the workstation's main system. Thus, the abovementioned practical class should begin with launching the virtual machine and pre-installed operating system.

Before students start performing practical tasks, they need to be persuaded that the skills they are about to learn will help them in their professional daily activities.

The main structure of the practical class can be divided in four stages [10] (Fig. 4).

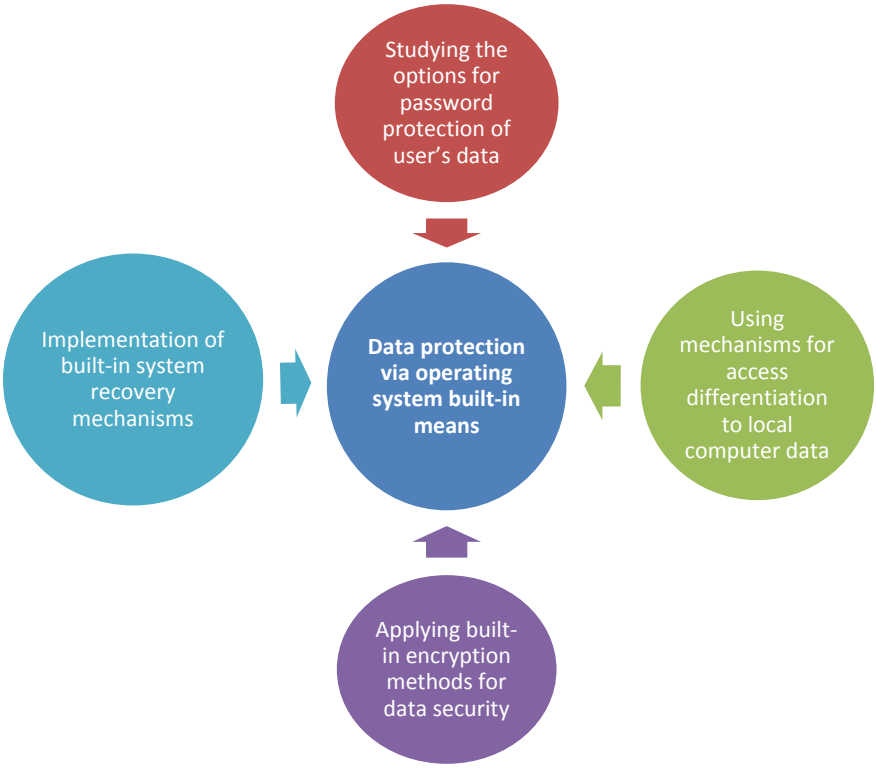

Fig. 4. Structure of the practical class.

At the first stage, students need to learn the basics of password protection via built-in OS mechanisms. To do this, they are supposed to perform the following tasks:

1. Create two additional user accounts in the system, giving them individual names and passwords.
2. Use one of the new accounts to enter the system and save several files in user's personal folders (e.g., My Documents folder) and in random location on the hard drive.
3. Enter the system from another account and try to access previously saved files.

Upon completing these tasks, students should individually make conclusion on efficiency of this protection method [11].

Modern operating systems give administrators vast opportunities for flexible setting of users' access to different computer resources. Detailed study of all administering options is time-consuming and requires specific skills. However, students do not need special knowledge for learning basic access differentiation.

4.2 Access Restriction Method

During the second stage, students are learning the access differentiation method that restricts access to certain files and folders in addition to default rules formed automatically when a new account is made [12].

When performing this task under the supervision of a faculty member, students make a list of users and their access rights (to read, save, change files etc.) to files or folder chosen in advance. The first thing that must be taken into consideration is that all activities at this stage are performed by the administrator, not a common user.

For consolidating obtained knowledge, students should enter the system in turns, trying to access said folders and files. The main conclusion students are supposed to make after this task is that access differentiation enables effective protection of data from common users working on a same computer, yet this mechanism cannot be used against users with administrator rights.

It is necessary to focus students' attention on the fact that an account password must be chosen responsibly. A password must contain at least 8 symbols, including uppercase and lowercase letters and special symbols, and should not be a derivative of existing words. Besides, students need to realize that even if only one user works on the computer, automatic login option should not be activated, because in this case any person, who turns on the computer, gets access to all files and parameters of this account [13].

4.3 Standard Encryption Function

For better protection of data against unsanctioned access, students are expected to learn built-in encryption functions. Before getting to practical tasks, students need to be briefly reminded about main principles of cryptographical transformation and special importance of encryption keys. For learning the built-in OS mechanism for folder and file encryption, students are asked to enter the system from one of the accounts and then create a random file at any location, setting its encryption parameters in file properties.

For checking efficiency of this protection method, students can try to access encrypted files and folders as another user or as the administrator. While performing this task, it is necessary for them to understand that if files are copied or a user password is changed, access to encrypted files will become impossible without the key. This is why it is obligatory to save the key formed by the system after the encryption, which can also be password-protected.

Sometimes, operating system integrity is damaged due to malfunctions, malware or perpetrators' activities. The fourth stage of the class helps to develop skills on operating system recovery via built-in tools. At first, students need to realize that no operating system, no matter how sophisticated, is flawless and can guarantee perfectly stable computer functioning. There is always a possibility that an improper combination of hardware and user-installed software will lead to operating system failure [14].

Besides, operating system boot can become impossible because of users and third parties. IT specialists can help with its recovery, but this will require additional time and resources – which is unacceptable if the information required for user's work is stored on this computer only.

As Microsoft Windows is the most commonly used operating system in Russia, it seems reasonable to study recovery tools provided by this system during the class. At first, students should learn system recovery options that involve restore points. To do this, they create a restore point and then recover computer status on that moment via Windows GUI. Students need to pay attention that if properly set, operating system will create restore points automatically; however, in some cases it is reasonable for users to make their own points, e.g., while installing or updating drivers, setting up unknown software, etc. Besides, this method is applicable only in case of a successful OS boot.

Often, operating system cannot boot at all due to a failure, making it impossible to restore the system through Windows environment. This is why students need to learn additional ways to start this operating system. To do this, they reboot the system, activate the menu of additional options for OS boot and then, supervised by a faculty member, choose one of the following options.

Last Known Good Configuration option is the first mechanism that can be recommended in case of an OS failure. If selected, it loads the last configuration of device drivers and register, during which Windows demonstrated stable work. This configuration does not have a component that could have caused the malfunction: it will be deleted when the last known good configuration is being loaded, without a possibility for its recovery. If this option was unable to solve the malfunction, it seems worthy to run the OS in safe mode.

Safe mode launches the minimal number of services and drivers required for Windows to function. It helps to recover the system from a restore point, delete software that could have caused the malfunction, delete drivers, etc. Running Windows in safe mode also helps to find out, on which level the problem has appeared. Students also must take into consideration that if the system is working properly in safe mode, the malfunction was caused by bootable files.

Safe Mode with Command Prompt option enables to launch the command prompt instead of standard Windows graphical shell. This mode can be helpful in case of problems with the file manager and of utmost importance if the GUI is blocked by malware. When studying this mode, students should pay attention to two useful utilities than can be run from the command prompt: CHKDSK and SFC. The former checks hard drives for file system errors, including physical damages, and corrects them, while the latter checks system files and enables users to look for damages and restore damaged system files. It has to be noted that these utilities can be run only from the administrator's account.

After learning to run several types of safe modes, students need to familiarize with Windows Recovery Environment opportunities. To do this, they should choose Troubleshoot option in the boot menu. This environment contains many tools designed for restoring computer functionality, including means to automatic boot recovery, restore point recovery, system image recovery, RAM diagnostics and the command prompt option. It seems unreasonable to study all recovery tools during the class, yet some of them should be highlighted, so that students can understand which purpose each of these tools serves.

At the end of the class, a faculty member must summarize its results by making a group discussion of studied methods of data protection via built-in operating system

mechanisms. This method of conducting practical classes allows students, who have no special knowledge on data security and recovery, to learn skills of password protection, access differentiation and basic built-in methods of data encryption and recovery, available at any computer device. These skills will be useful not only to specialists dealing with confidential information but also to everyone who use computer equipment in their professional activities.

It is also worth mentioning that while selecting tools for this practical class, preference was given to built-in software, pre-installed on every computer and provided by almost all operating systems. This will help future specialists to apply obtained skills in their professional activities, regardless of software they are going to use.

5 Conclusion

Data security issues are becoming more relevant every year. Many believe these problems can be solved through technical means only – by installing firewalls and antivirus software. However, the main prerequisite for reliable protection is awareness of existing threats and ways to counter them. This applies not only to IT specialists but to everyone dealing with various information systems in their professional activities. Famous "forewarned is forearmed" principle works in computer security as well: if a threat is promptly detected, many unpleasant consequences can be avoided. This is why security measures must be upheld at all network points, when any subjects are working with data.

References

1. He, J.: The Rules of Judicial Proof. In: Methodology of Judicial Proof and Presumption. Masterpieces of Contemporary Jurisprudents in China (2018). 280 p.
2. Bulgakova, E., Bulgakov, V., Trushchenkov, I., Vasilev, D., Kravets, E.: Big data in investigating and preventing crimes. In: Kravets, A. (eds.) Big Data-driven World: Legislation Issues and Control Technologies. Studies in Systems, Decision and Control, vol. 181, pp. 61–69 (2019)
3. Luo, Y., Cheung, S.S., Lazzeretti, R., Pignata, T., Barni, M.: Int. J. Inf. Secur. **17**, 261–278 (2018)
4. Kravets, A.G., Kravets, A.D., Korotkov, A.A.: Intelligent multi-agent systems generation. World Appl. Sci. J. **24**(24), 98–104 (2013)
5. Vasilev, D., Kravets, E., Naumov, Y., Bulgakova, E., Bulgakov, V.: Big data-driven world: legislation issues and control technologies. Stud. Syst. Decis. Control **181**, 249–258 (2019)
6. Dronova, O., Smagorinskiy, B.P., Yastrebov, V.: Counteraction to e-commerce crimes committed with the use of online stores. In: Kravets, A. (eds.) Big Data-driven World: Legislation Issues and Control Technologies. Studies in Systems, Decision and Control, vol. 181, pp. 121–131 (2019)
7. Sample of the virtual classroom in BigBlueButton's platform. https://support.bigbluebutton.org/hc/en-us/articles/1500005315982-Show-recordings-from-deleted-activities. Accessed 14 May 2021
8. Kravets, E., Birukov, S., Pavlik, M.: Remote investigative actions as the evidentiary information management system. In: Kravets, A.G. (ed.) Big Data-driven World: Legislation Issues and Control Technologies. SSDC, vol. 181, pp. 95–103. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-01358-5_9

9. Bui, N.D., Kravets, A.G., Nguyen, T.A., Nguyen, L.T.T.: Tracking events in mobile device management system. In: IISA 2015 - 6th International Conference on Information, Intelligence, Systems and Applications, article № 7388127 (2016)
10. Saltykov, S., Rusyaeva, E., Kravets, A.G.: Typology of scientific constructions as an instrument of conceptual creativity. In: Kravets, A., Shcherbakov, M., Kultsova, M., Shabalina, O. (eds.) CIT&DS 2015. CCIS, vol. 535, pp. 41–57. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23766-4_4
11. Klimmt, C.: Virtual worlds as a regulatory challenge: a user perspective. In: Cornelius, K., Hermann, D. (eds.) Virtual Worlds and Criminality, pp. 1–18 (2011)
12. Kravets, A.G., Al-Ashval, M.: Mobile corporate networks security control. In: 2016 International Siberian Conference on Control and Communications, SIBCON 2016 - Proceedings, article № 7491811 (2016)
13. Kopyltsov, A.V., Kravets, A.G., Abrahamyan, G.V., Katasonova, G.R., Sotnikov, A.D., Atayan, A.M.: Algorithm of estimation and correction of wireless telecommunications quality. In: 2018 9th International Conference on Information, Intelligence, Systems and Applications, IISA 2018, article № 8633620 (2018)
14. Kravets, A.G., Skorobogatchenko, D.A., Salnikova, N.A., Orudjev, N.Y., Poplavskaya, O.V.: The traffic safety management system in urban conditions based on the C4.5 algorithm. In: Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - Proceedings, 2018-March, article № 8337254, pp. 1–7 (2018)