Developing information security competencies of applied informatics students of agrarian universities

Natalia Titovskaia[1*], *Sergei* Titovskii[1,2], *Tatyana* Pushkareva[2], and *Tatyana* Titovskaya[1]

[1]Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia
[2]Siberian Federal University, Krasnoyarsk, Russia

Abstract. The article is devoted to the theory and experimental verification of methods that ensure the quality of training of information security specialists for agro-industrial enterprises. Effective study of information security can be achieved through a spiral approach in the theoretical part and a practice-oriented approach in the laboratory-practical assignments, which ensures the formation of competencies in the field of study. The spiral approach implies a gradual study of theory, from the simplest to the most complex, with simultaneous consolidation of the acquired knowledge in practical classes. The practice-oriented approach consists of three stages. The first stage is the completion of educational practice at agricultural enterprises. The second stage is the mastering of laboratory practice using virtual machines for which students are given administrator rights. The third stage is a complex laboratory work to create recommendations for improving the security policy of the object under study (real enterprise of agro-industrial complex), and the development of a program containing various methods of cryptographic information protection. The approach described above has greatly improved the quality of understanding of issues related to information technology security in agriculture.

1 Introduction

The most important task of modern society is to guarantee information security (IS) at all stages of life. The rapid spread of automated systems for collecting, storing, analyzing and transmitting data has exacerbated this problem. At the same time, the threats of information theft, modification or misrepresentation are increasing. To date, it is especially relevant to master the methods of information protection when using personal computers, smartphones and other portable devices. The issues of information security are of particular relevance in agricultural production due to the shortage of qualified personnel in the field of information technology [1, 2]. The current situation requires agrarian universities, as the main suppliers of such specialists, to pay special attention to training in the field of applied informatics [3].

Consequently, students of agrarian universities should master competencies in the field of information security and acquire relevant skills. It is required to develop a full

* Corresponding author: nvtitov@yandex.ru

understanding of the principles of information security in the field of agricultural production, covering all aspects of its provision in this subject area [4].

There are new socio-economic and educational realities in the country and, in particular, in the agricultural industry that reflect the growing need for information security specialists [5]. Thus, there is a need to provide professional training in the field of information security and its scientific and methodological support, in accordance with the constant development of information and Internet technologies in all areas of life [6, 7].

Lack of attention to information security issues is already leading to the emergence of many destructive factors that have a negative impact on the person, society and the state. It becomes obvious that successful solution of such problems directly depends on specialists with competencies in legal, organizational and hardware-software spheres of information security [8]. In this regard, the training of specialists to work in this vast and multidimensional field is becoming more and more important and demanded by various agricultural organizations and institutions [9].

Purpose of the study: theoretical substantiation and experimental verification of methodological approaches that ensure training quality of information security specialists in Krasnoyarsk State Agrarian University (Krasnoyarsk SAU). For this purpose it is necessary to analyze the elaboration of the problem under consideration in scientific, methodological and technological literature, as well as to clarify the structure, goals and objectives of the information security training course, its components and their interrelation with other disciplines.

2 Methods

The presented research used: analysis of domestic and foreign literature on the described problem, study and generalization of teaching experience, surveys, observation and statistical processing of experimental data.

The theoretical basis for this study was research in the field of teaching the principles of information security and their implementation in the educational process.

The students of 09.03.03 "Applied Informatics" of Krasnoyarsk State Agrarian University were chosen as the experimental base of the study.

The study is based on the assumption that effective mastering of the discipline "Information Security" by students can be achieved if a spiral and practice-oriented approach is applied [10, 11] (Fig. 1).

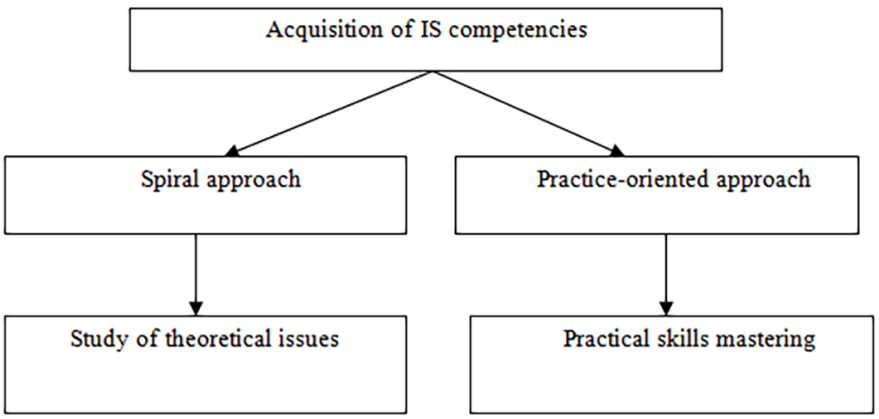

Fig. 1. An approach to formation of competencies in the field of information security.

This will make it possible to comprehensively apply various teaching methods taking into account interdisciplinary links, increase motivation for learning activities and improve the quality of students' individual work [12].

The main components of information security are ensuring confidentiality, integrity and availability of information [13]. Also, the principles of information protection are based not only on legal, moral and ethical aspects, but also on the peculiarities of technical processes. The course "Legal Protection of Intellectual Property" is focused on the study of legal aspects of information protection in Krasnoyarsk SAU.

3 Results and discussion

As a result of analysis and generalization of experience in teaching the discipline “Information Security” [14-16] the following structure of theoretical material is proposed for study:

- The concept of information security. The main provisions of the theory of information security. Security models and their application. The concept of threat. International standards of information exchange. Information threats to the Russian Federation security. Russian Federation information security doctrine. Application of the above-mentioned information in the agro-industrial complex.
- Main regulatory documents concerning state secrets, reference documents. Purpose and tasks in the field of information security. Types of intentional interferences and protection against them. Intellectual property protection.
- Types of possible breaches of the information system. Types of protection. General classification of information threats. Information technologies to ensure confidentiality and data security in the conditions of global networks functioning. Organizational measures to ensure information security. The procedure for using confidential archive documents. IS standards and policies. Information protection models. Implementation of IS means at the enterprises of agro-industrial complex.
- Malware. Notions about types of viruses. Software and hardware methods of fighting viruses and other malicious software.
- Information security breach and the reasons for its existence. Specialized software. Engineering and technical support of IS. Typical remote attacks using network protocol vulnerabilities. Classification of remote attacks.
- Analyzing possible vulnerabilities. Protected computer systems. Main technologies of protected Encrypted Information System construction. Types of possible information system violations. Legal regulation of information protection. Influence of peculiarities on the principles of construction.
- Methods of cryptography. Software and hardware means of information protection.

In modern conditions agrarian universities are faced with limited opportunities to acquire certified software and hardware tools to ensure the process of teaching. In this regard, students are invited to perform the following set of laboratory works, the purpose of which is to consolidate the theoretical material:

- Protection of programs and files from unauthorized access.
- Restoration of infected files.
- Typical remote attacks and its features.
- Preventing trojan infection.
- Configuring Windows authentication settings.
- Encrypting file system (EFS) and certificate management in Windows.
- Assigning user rights with arbitrary access control in Windows.
- Configuring logging and auditing settings in Windows.

- Security Template Management in Windows.
- Methods of storing and duplicating information. RAID technology.
- Configuring and using software RAID in Windows.
- Configuring and using software RAID in Linux.
- Configuring and using a firewall in Windows.
- Creating a VPN connection using Windows.
- System Recovery.
- Recovering deleted files.
- Certification of the allocated premises according to information security requirements.
- Hardware and software means of information protection.
- Cryptographic means of information protection.
- Implementation of cryptographic algorithms for information protection.

This list may be extended in case of acquisition of specialized information protection means.

The spiral principle of teaching consists in the sequential study of theoretical issues from simple to complex, with subsequent consolidation of the acquired knowledge in laboratory classes.

However, it should be noted that the set of laboratory works corresponding to the presented list does not meet the desired level of mastering competencies in the field of information security. Most often, the step-by-step instruction of laboratory work is presented; its purpose and output results are described [7, 11, 13]. This approach does not allow students to fully realize the applicability of the studied issues in real life.

To eliminate this shortcoming and improve the quality of mastering the material, the course uses a practice-oriented approach, which contains three stages of preparation Fig. 2.

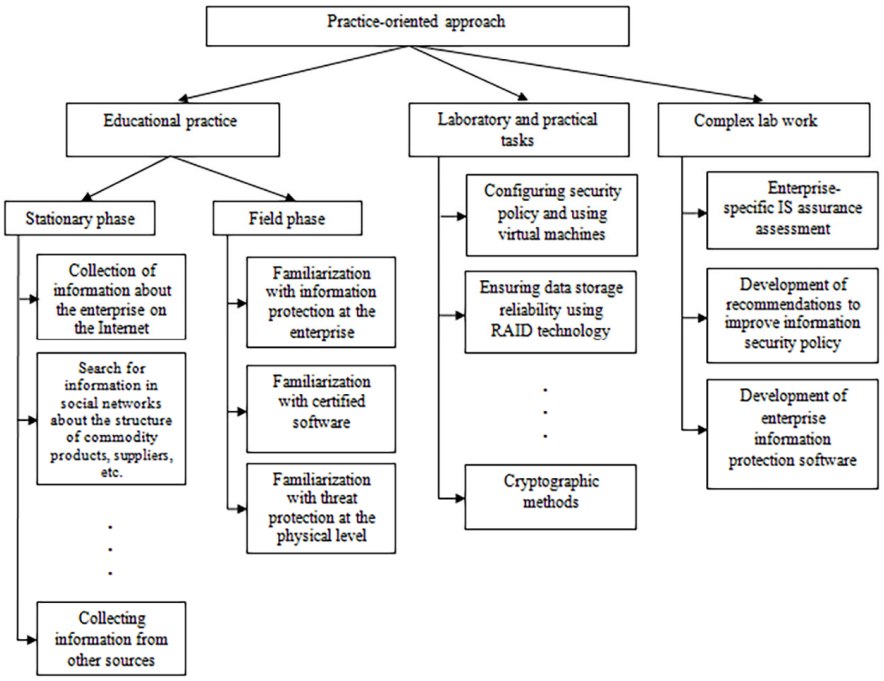

Fig. 2. Practice-oriented approach.

The first stage: educational practice called "Technological (design and technological) practice", which is held in the preceding semester. Knowledge and skills obtained and consolidated during this practice are further necessary for course projects and complex laboratory works, as well as in the development of software products to obtain a diploma.

The practice is conducted in two phases - stationary and field. This means that in the stationary (initial) phase, students study the issues outlined during the practice in the educational classes. The purpose of this phase is to collect initial information about the real enterprise of the agricultural sector, organization of its work, structure of commodity production, data storage, information about suppliers, customers and so on. Such information is collected through the study of data posted on the Internet and social networks. The data is collected bit by bit from different sources of information.

At the field practice students visit an agricultural enterprise and study the production process. The main objective of this stage is to study the certified software of the enterprise, which provides protection of information from various kinds of threats at the physical level from hacking, theft, or destruction. Students study the developed information security policy of the enterprise.

However, it should be noted that at the enterprises of the agro-industrial complex of Krasnoyarsk region to a greater extent, and the enterprises of the processing industry to a lesser extent, information security is implemented rather poorly, as these enterprises have a significant lack of qualified personnel in the field of information security.

The materials obtained as a result represent an important source of data for designing a security policy. The ability to form an information security policy for a particular company and its subdivisions is an integral part of a specialist's training process. The information collected during the summer practice at the enterprises of agro-industrial complex allows raising further training to a qualitatively new level.

After collecting and analyzing data, students are better prepared to perform profile tasks, as they use real data from specific agricultural enterprises rather than test data. Due to the low level of data digitalization in agricultural enterprises, the needs for qualified development of security policies and determining the composition of the necessary software are significant.

The second stage: works listed above.

This stage is necessary for consolidation of the studied theory and mastering skills in the field of information security. However, as noted earlier, this stage has disadvantages, as students follow a scheme of studying questions on the topic under consideration and have little idea where they can apply their knowledge and practical experience.

It should be noted that, despite the fact that students may face a shortage of certified software and hardware, there are various ways of organizing seminars on information security in agrarian universities [17, 18].

Most assignments require administrative privileges to complete, which is not possible when using public computers in classrooms. These privileges are not granted to students for security reasons. A great way to solve this problem is to use virtual machines where students are administrators and have all the necessary rights and privileges [19,20]. Assignments to ensure the reliability of data storage due to RAID technology are conducted using virtual machines running Windows Server and Linux operating systems; laboratory work related to local security policies requiring administrative privileges:

- configuring Windows authentication settings,
- Encrypting File System and Certificate Management in Windows,
- assigning user rights for arbitrary access control in Windows,
- configuring logging and auditing settings in Windows,
- managing security templates in Windows,
- are also run on virtual machines running Windows workstations.

Tasks related to the study of cryptographic methods are performed on virtual machines running Linux operating systems using the PGP package [21].

The third stage: during the study of the course, students, in addition to laboratory works, perform the so-called complex laboratory work on the subject "Information Security". When performing it, students should solve the following tasks:

- to study the issue of ensuring information security of the object under study (a specific enterprise of the agro-industrial complex),
- Identify the means of protection used and their features,
- propose strategies to improve the efficiency of data storage,
- develop software tools to protect the information of the object under study.

The purpose of complex laboratory work is to assess the level of information security at a particular enterprise (object of study) and develop proposals for its improvement, as well as to develop recommendations in the field of enterprise security policy, develop software that implements cryptographic methods of information protection for the enterprise.

In Krasnoyarsk SAU was conducted a study of the influence of educational practice and performance of complex laboratory work on the progress of students in mastering the discipline “Information Security” and obtaining competencies in the field of information security.

A survey was conducted, the results of which are presented in Table 1, and statistical processing of the obtained data was carried out.

Table 1. Results of the survey.

№	Questions asked. Score in the range from 1 to 5.	Score 1	Score 2
1	What was the impact of the practice and complex laboratory work on mastering the basic concepts of information security, on studying the issues of confidentiality and data security?	5.0	4.95
2	To what extent did the practice and complex laboratory work affect the study of issues related to possible types of information system breaches, types of information system protection?	5.0	4.8
3	How do you evaluate the quality of the material obtained during the practice and comprehensive laboratory work for practical and research activities?	4.9	4.8
4	How useful are visits to enterprises in studying the discipline?	5.0	4.95
5	How useful is practice and complex laboratory work in understanding and applying information security practices?	5.0	5.0
6	How satisfied are you with the knowledge, skills, and results obtained after completing the educational technology practice and complex laboratory work on the malware in use?	4.9	4.6
7	How satisfied are you with the knowledge, skills, and results obtained after completing the educational technology practice and complex laboratory work on software and hardware methods of counteracting malicious software?	4.8	4.5
8	How do you evaluate the study of issues related to the legal regulation of information protection during the practice and complex laboratory work?	4.4	4.1
9	How influential was the completion of the complex laboratory work and educational practice on the	5.0	4.3

№	Questions asked. Score in the range from 1 to 5.	Score 1	Score 2
	study and application of cryptographic methods of information security?		
10	How would you evaluate the acquisition of knowledge about specialized software, IS engineering and technical support obtained during the practice and complex laboratory work?	4.6	4.5
11	To what extent has the complex laboratory work and educational practice influenced your understanding and use of knowledge in neutralizing remote attacks using network protocol vulnerabilities?	4.9	4.6
12	How useful is the information gained from the practice and complex laboratory work in understanding questions about secured computer systems?	4.8	4.5
13	How do you evaluate the teacher's activity when studying the Information Security discipline?	4.9	5.0
14	Evaluate the teacher's use of tests, quizzes, questions, during the discipline.	5.0	5.0
	Average score	4.87	4.68

In the Table above, *Score 1* is the average grade, which reflects the impact of the complex laboratory work on the understanding of the essence and content of the discipline “Information Security”, *Score 2* is the average score, which reflects the impact of the practice "Technological (design and technological) practice" on the understanding of the essence and content of the discipline “Information Security”

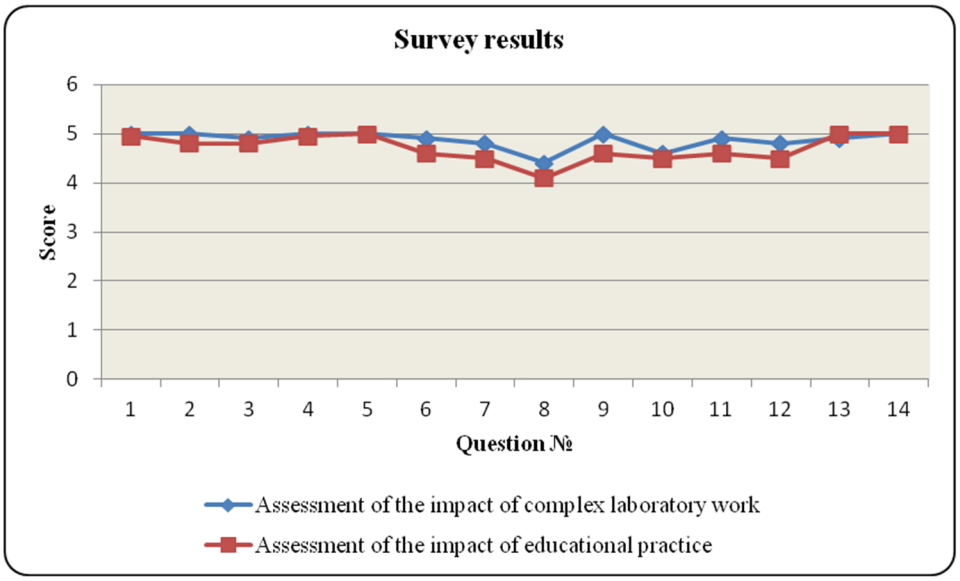

Fig. 3. Points for complex laboratory work and educational practice.

The analysis of the results suggests that for students, the knowledge gained during the educational practice and complex laboratory work on the development of recommendations to strengthen the security policy of the object of study and the development of a program that

implements various methods of cryptographic protection of information to a large extent qualitatively improved the understanding of issues related to information security.

It should be noted that complex laboratory work had the greatest impact (mean score was 4.87 points). However, as students note, without practice and without visiting the real object of study, it is difficult to master knowledge and skills in the field of information security, and this is evidenced by the average score (equal to 4.68 points), which evaluates the contribution of practice to the success of knowledge acquisition in the field of information security. As a result of applying the point-rating system, the grade for the practice and the grade for the complex laboratory work are assigned as a result of a set of points. The scores obtained for all practice assignments and scores obtained for the complex laboratory work are shown in Fig. 3. The sample includes data on 30 students who have fully passed all other disciplines.

When calculating the correlation of the given grades, a value equal to 0.83 was obtained, showing a high correlation between the grades received for the complex laboratory work and the grades received for practice.

4 Conclusion

This work developed and tested a practice-oriented approach to the study and acquisition of competencies in the discipline “Information Security” for students studying Applied Informatics at Krasnoyarsk State Agrarian University. It was revealed that agricultural universities face difficulties in access to certified software and hardware to support the educational process on information security. Application of practice-oriented approach to the process of studying the discipline “Information Security”, consisting in a number of stages, such as:

- practice, during which students get acquainted with information security at a real enterprise;
- study of theoretical material while performing a sufficient number of works on the Information Security course;
- complex laboratory work,
- definitely affects the quality of mastering competencies, which is confirmed by the grades received.

References

1. E.V. Vasilyeva, A.N Kamanina, Discussion **117**,108-118 (2023). https://www.doi.org/10.46320/2077-7639-2023-2023-2-117-108-118
2. L.A. Konstantinova, I.V.Kramarenko, E-Management **5(3)**, 50-63 (2022). https://www.doi.org/10.26425/2658-3445-2022-5- 3-50-63
3. A. Zubarev, V. Dushkevich, Information Security **6** (2019)
4. N.A. Bushmeleva, E.V. Razova, Scientific and methodological electronic journal "Concept" **(2),** 537-544 (2017)
5. E.K. Grosheva, P.I. Nevmerzhickij, Business education in knowledge economy **3(8)**, 35-38 (2017)
6. V.P. Polyakov, *Methodical system of teaching information security among university students: Doctor of Pedagogical Sciences dissertation: 13.00.08* (Nizhny Novgorod, 2006)
7. A.A. Altufieva, *Methodical bases of teaching information security on the basis of telecommunication resources of the Internet: dissertation of candidate of pedagogical sciences:13.00.02* (St. Petersburg, 2008)

8. O. A. Karaulova, *Interactive teaching methods as a factor in improving the quality of the educational process* in Proceedings of the 11th International Scientific and Practical Conference New Information Technologies in Education and Science NITO-2018, Yekaterinburg, 217-223 (2018)
9. E. B. Belov, Information and Communication **(2)**, 94–96 (2002)
10. Yuechuan Wei, *Some ideas on construction of course of mathematical foundations in information security*, in Proceedings of the 2015 Conference on Education and Teaching in Colleges and Universities, 10-12 (2016). https://www.doi.org/10.2991/cetcu-15.2016.4
11. Michael E. Whitman, Herbert J. Mattord *Designing and teaching information security curriculum,* in Proceedings of the 1st Annual Conference on Information Security Curriculum Development, 8 Oct 2004, 1-7 (2004). https://www.doi.org/10.1145/1059524.1059526
12. M. Richards, B. A Price, B. Nuseibeh, Progress in Informatics **5**, 91 (2008). https://www.doi.org/10.2201/NiiPi.2008.5.9
13. R. Gallo, R. Dahab, *Assurance Cases as a Didactic Tool for Information Security* in Proceedings of IFIP WISE 9 2015: The Ninth World Conference on Information Security Education, May 2015, 15-26 (2015). https://www.doi.org/10.1007/978-3-319-18500-2_2
14. C. Morales-Gonzalez, M. Harper, X. Fu, Journal of The Colloquium for Information Systems Security Education **10(1)**, 6 (2023). https://www.doi.org/10.53735/cisse.v10i1.173
15. G.D. Momcheva, T.I. Bakardjieva, V.G. Spasova, A.I. Ivanova, Education and Technologies **12(2)**, 516-518 (2021). https://www.doi.org/10.26883/2010.212.3903
16. Ahmad Fuzi Md Ajis, Rohayu Ahmad, Suhaila Osman, Isma bin Ishak, *Catalyst of Information Security in Malaysia Higher Learning Institutions,* 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), 18-19 April 2020, (2020). https://www.doi.org/10.1109/ISCAIE47305.2020.9108806
17. C.K. Chan, A.W.T. Yeoh, Journal of Computer and Communications **6(1),** 1-11 (2018). https://www.doi.org/10.4236/jcc.2018.61001
18. S.N. Titovskii, N.V. Titovskaia, T.S. Titovskaya, T.P. Pushkaryova, *Virtualization and problems of training IT specialists*, in European Proceedings of Social and Behavioural Sciences EpSBS: Proceedings of the International Conference on Economic and Social Trends for Sustainability of Modern Society (ICEST 2020), 20-22 May 2020, 794-799, Krasnoyarsk Science and Technology City Hall, Krasnoyarsk (2020). https://www.doi.org/10.15405/epsbs.2020.10.03.93
19. J. Stites, A. Siraj, E. L Brown, S*mart grid security educational training with thundercloud: a virtual security test bed,* in Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference, 12 Oct 2013, 105-110 (2013). https://www.doi.org/10.1145/2528908.2528927
20. G. Chryssolouris, D. Mavrikios, D. Fragos, V. Karabatsou, R. Pistiolis, International Journal of Computer Integrated Manufacturing **15(3)**, 214-221 (2002). https://www.doi.org/10.1080/09511920110034978
21. S.N. Titovskii, N.V. Titovskaia, *Use of virtual machines in KrasSAU*, in collection: Science and Education: Experience, Problems, Prospects of Development. Materials of the International Scientific-Practical Conference, 22–23 Apr 2015, 141-144, Krasnoyarsk State Agrarian University, Krasnoyarsk (2015)