AUTHOR'S PRESENTATION

OF DOCTORAL (PhD) DISSERTATION

NATIONAL UNIVERSITY OF PUBLIC SERVICE
FACULTY OF MILITARY SCIENCES AND OFFICER TRAINING
DOCTORAL SCHOOL OF MILITARY ENGINEERING

Veronika Dr. Debreceniné Deák

The educating opportunities of cyber defence capabilities in the public sector

Supervisor:

Dr. Csaba Krasznay, PhD

Budapest, 2023.

TABLE OF CONTENT

INTRODUCTION

Cybersecurity is a rapidly changing, evolving, and expanding field, presenting us with new challenges and threats every day, thanks to the unprecedented scale of technological development in our rapidly changing world. The various infocommunication technologies are essential components of our modern society. Consequently, the use of these tools and technologies is also becoming increasingly widespread in the public service.

However, their everyday use and growing dependence can entail several risks. Achieving the right level and quality of cyber security is a complex task and is critical to both the creation and continued viability of the public and private sectors. The continuous increase in cyber-attacks and the emergence of new tools and alternatives to attacks create new challenges and require the development and constant improvement of additional protection mechanisms. Responding immediately to challenges and threats places a significant burden on organisations. The public service and the various critical and critical-information infrastructures can be seen as indispensable for the day-to-day functioning of society. Therefore, it is necessary to ensure the continued reliable and secure operation of the information systems on which they are based.

Experience from recent years shows that the public service is a prime target of cyber-attacks, and cyber-attacks against public service organisations have become commonplace. Attacks are mainly aimed at obtaining internal and confidential information and limiting various services' functioning. Therefore, the whole organisation - from the smallest element of the system, through information systems, to the people working in them - must be prepared to prevent an attack and to respond to events that may occur. In the public service, too, it is vital to continuously improve cyber defence, cyber protection capability and cyber security, and the development and delivery of cyber security training, education and exercises are essential elements of this. A significant proportion of attacks target the unpreparedness and lack of security awareness of users, which is why the primary objective is to develop and continuously improve the awareness and cyber defence capabilities of civil servants, and to achieve this, it is essential to create a training format that will help to achieve these objectives.

THE FORMULATION OF THE SCIENTIFIC PROBLEM

The basis of the scientific problem hinders **the global cybersecurity workforce shortage**. According to the International Information System Security Certification Consortium Inc. (ISC) 2021 survey, the cybersecurity workforce shortage has decreased (from 3.12 million to 2.71 million

cybersecurity professionals) but still results in a severe shortage. ISC states that the global cybersecurity workforce needs to grow by 65% to protect critical systems and assets of organisations effectively. The study points out that one of the most essential options to overcome the mentioned workforce shortage is the professional training of staff.[1]

The lack of suitably qualified professionals can be a significant barrier and obstacle to the functioning of the public service and the state. To address the workforce shortage and improve the cybersecurity awareness and skills of public service employees, it is crucial to establish training for the public service, which aims at developing and improving organisational and personal cybersecurity.

Lacking a cybersecurity-literate workforce and the cybersecurity-related additional tasks and pressures on available human resources can have several negative consequences. Such real adverse effects may include but are not limited to lack of detection of cyber-attacks, failure to detect them, failure to comply with internal regulations, misconfigured information systems due to inattention and overload, slower patching, slower updates, poor risk assessment, inadequate performance of the control or even supervisory role. **Poor task execution results in several cyber security and operational risks.**

A further element of the scientific problem is that, based on the current situation in the country, there are many training courses for cyber attack and protection capability, which require, as a prerequisite, some basic IT qualification. **However, those without a mathematical or IT qualification are not assured of completing the currently available courses.** Therefore, there is a need to develop a training programme to develop the cyber security skills of non-IT-educated civil servants. This capability aims to ensure that those who do not have the necessary basic knowledge and need to become more familiar with the subject are adequately prepared to develop effective and efficient protection, prevent cyber threats and effectively counteract incidents that have already occurred. These people are in the public service and are involved in decision-making on a daily basis, so it is essential to develop their cyber defence skills, not only to develop a comprehensive defence but also to make informed strategic decisions on cyber defence.

[1] (ISC)², „Cybersecurity Workforce Study," 2021. [Online]. url: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

RESEARCH OBJECTIVES

The main objective of my research is to define a training course for the development of cybersecurity in the public sector, which can be integrated into the public sector training system and which, through the acquisition of theoretical and practical knowledge, enables the efficient and effective implementation of protection against threats from cyberspace, thus ensuring the unhindered and unrestricted functioning of the state. Taking into account the scientific problem and the main objective described above, the objectives of my research and the sub-objectives are presented in this section:

- First, the research underlying this thesis aims **to define a process containing the steps of a science-based higher education training design process**. My goal here is to identify the clear tasks and steps necessary to define a training course in such a way that it has academic relevance and is considered evidence-based.
- In order to assess and design the need for cybersecurity training for the public sector, it is essential **to define the knowledge and skills required to achieve an appropriate level of cybersecurity and identify the target group for the training**. In this context, it is necessary to examine the specific target group within the public service and the generic cybersecurity tasks that civil servants need to perform in their daily work or in the event of a cyber-attack. Only then can the necessary and sufficient set of knowledge and skills that the target group needs be determined.
- A further aim of the research is **to explore whether there is currently a practical training programme for developing cyber defence capability in the public service, both in our country and internationally**. **In this context, my aim is to map and compare international and domestic cyber defence capability training programmes, and to identify domestic and international "good practices".** The rationale is to justify the need for cybersecurity training in the public sector by identifying related training and possible gaps. In addition, the comparative analysis will help to identify a number of good practices, the translation of which into domestic training could significantly contribute to the definition of internationally recognised training.
- Moreover, my research aims at **defining a training programme for public service cyber defence capability** using the defined knowledge and knowledge set. This requires a formal specification of the training, its core elements, its purpose and its input and output requirements. In addition, this research aims to explore the feasibility of using public service cybersecurity training in a specific area of the defence sector, the Volunteer Reserve System. To this end, it is necessary to examine what additional elements, based on the

specific characteristics of the role and status of the Voluntary Reserve, are needed to expand the previously identified body of knowledge and skills to be acquired to use the training.

- Once the training has been defined, it is necessary **to define the technical framework needed to support the training objectives and the means to put it into practice**. This objective seeks to answer the question of how cyber defence skills can be acquired and how the necessary knowledge, different defence strategies and techniques can be transferred to people who do not have a background in IT. The aim is to train professionals who have practical knowledge. As a result, part of the research objective is to create an environment through which the trainees can be exposed to known cyber-attack techniques and test the defence mechanisms they have learned during the training in a simulated real environment.

RESEARCH HYPOTHESES

At the beginning of my research, I formulated the following hypotheses after formulating the scientific problem.

H1 Cybersecurity training programme for higher-level education can be defined on a scientific basis.

H2 The target group needed to achieve public service cybersecurity and the set of knowledge to be acquired by them can be identified.

H3 No practical training programme for developing and improving cyber security capability in public service has been developed before.

H4 A training programme for developing cybersecurity in the public service can be defined, which does not require any prior IT training.

H5 A technical framework for cyber security awareness can be defined that provides the opportunity for practical application of protection mechanisms against cyber attacks.

RESERARCH METHODS

The research methods used to prove the above hypotheses are described in this section. I have used both quantitative and qualitative research methods in my research. The inter- and multi-disciplinary nature of the research topic requires a comprehensive examination of related disciplines. In order to achieve the set objectives, I participated in academic events, conferences and exercises related to cybersecurity, information and IT security and data protection, and subsequently processed, analysed and evaluated the experiences and knowledge gained there. In addition, I have continuously monitored the latest news and developments related to cybersecurity, information and IT security and data protection by studying relevant journals and through the communications-

oriented media. I have analysed, processed and evaluated the recent significant events and experiences in the field of cyber defence. I have examined and analysed the accumulated relevant educational materials, teaching aids, PhD dissertations, international, EU and national regulations, legal instruments, standards, recommendations and methodological guidelines on cybersecurity regulation. The collected domestic and international literature was processed by analytical method and then synthesized after systematization. I used both the methods of induction and deduction to process the literature.

In my scientific work, I used both general and specific research methods. Among the general methods, I used observation and the comparative method to examine international experiences in order to study the application of foreign examples in the domestic context, to identify possible shortcomings and to identify 'good practices'. Among the observation methods, I have used both direct and indirect observation in examining the potential and limitations of applying different attack alternatives.

During my research, I consulted experts with national and international practical experience and conducted interviews to implement "good practices" and experiences in training and to define training according to real needs. In addition, I collected opinions, experiences and feelings about the role of practical training in a focus group discussion with a similar group of stakeholders as the participants of the training on which the research is based.

The partial results of my research have been published continuously and presented at several academic and professional conferences, events and forums to inform, promote professional reflection and explore the related reactions.

BRIEF DESCRIPTION OF CHAPTERS

In Chapter 1, I examined whether precise tasks could be identified necessary to define a cybersecurity training course in such a way that the course has academic relevance. In addition, in this chapter, I have analysed the research methodologies that should be used in a research project to perform the tasks in order to demonstrate that these tasks are academically valid. I have identified and organised the key points and steps needed to define training by defining an eight-element process model and the research methodologies required to design training.

In Chapter 2, I presented the differences between public and private sector cybersecurity through an interview and then used this to identify the current challenges in cyberspace. In this chapter, by concluding the interview and reviewing the relevant literature through document analysis and

examining the concept and components of the public service, I defined some of the elements and exceptions to the target group for public service cybersecurity training.

In addition, after defining the target group of the training and the current cybersecurity challenges, I identified the common cybersecurity tasks that public service employees need to perform, either in their daily work or in the event of a cyber-attack. In addition, in this chapter, I have identified the knowledge, skills and competencies that civil servants need to acquire to perform the identified cybersecurity tasks fully.

This is followed in Chapter 3 by the identification and comparative analysis of domestic and international cybersecurity-related higher education courses. In designing the training programme, the feasibility of the programme and similar domestic and international training courses, including their content and elements, will be explored to justify the training and to identify any gaps, remedies and 'good practices' to be applied to transfer them into the domestic training system. In this chapter, I have defined a selection methodology and comparison strategy to identify and compare relevant domestic and international cybersecurity training and the elements and practices of such training that can be transferred to domestic public-sector cybersecurity training.

In Chapter 4, I examined the need for prior IT training as a function of the effective acquisition of cybersecurity skills. I also described the definition and interpretation of the basic concepts and elements of public service cybersecurity training and the definition of training according to the Hungarian Qualifications Framework. In this chapter, I have described the status of the Volunteer Reserve Military Service and its current and future role in the provision of cyber defence. In addition, I have proposed the establishment of a cyber defence sub-unit within the Volunteer Reserve System and described the possible use of public service cyber security training in their training. To ensure the continuous improvement of the training, the chapter presents a set of criteria and a measurement method to measure the effectiveness of the knowledge transfer, which can be used to implement iterative improvements of some training subjects.

In Chapter 5, I presented the operational environment of a two-stage practical training programme, where participants identify the general architecture, components and their protection mechanisms of a fictitious organisational infrastructure and then apply protection strategies during simulated cyber attacks. To achieve this, I have identified a framework describing the simulation environment on which the practical training is based, which is designed to prepare civil servants to detect and respond to cyber attacks. In addition, I have described a simplified simulation environment that I have created for the training programme in connection with the protection of private information

communication assets, where I have demonstrated practical examples of cyber attacks to students that do not equire deep IT knowledge to be countered.

SUMMARIZED CONCLUSIONS

The number of cyber-attacks is growing exponentially, with significant implications for the economy, society and the basic functioning of organisations. We are facing more complex and sophisticated cyber-attacks every day, which are creating new types of challenges for organisations. In this context, it is necessary to emphasise the need to develop and improve the cyber security capabilities of the organisation and its employees, as an adequate level of user security awareness can significantly contribute to reducing the likelihood of cyber attacks occurring and mitigating the adverse consequences of such attacks.

Recruiting and employing professionals with relevant cybersecurity skills is a challenge, given the current cybersecurity workforce shortage and the ever-increasing demand for such workers. Developing and continuously improving cyber defence capabilities are essential to prevent and counter cyber-attacks effectively. A wide range of options is available for acquiring these skills, from higher education courses and awareness campaigns to implementing cyber exercises, to an extensive range of cyber security training programmes. When choosing the right type of training, several factors should be considered, such as, but not limited to, its delivery format, duration, input requirements, practical experience of previous participants, content, and the theory/practice ratio.

Detecting and anticipating cyber-attacks is a significant challenge, and a key element in addressing it is to develop and improve the theoretical and practical cyber defence capabilities of users. This is the purpose of the definition of public cybersecurity education presented in this thesis, given the crucial role of cybersecurity education in preparing current and future cybersecurity professionals. Along with the objectives defined in this dissertation, I have identified hypotheses that, if proven, will achieve these objectives.

My thesis is based on the scientific problem that there is a global cybersecurity workforce shortage that can create significant constraints and obstacles to the basic functioning of the public service. For example, the lack of professionals with the right competencies in the event of a cyber-attack can have a significant impact on the business continuity of an organisation. To mitigate and prevent these adverse effects, the main objective of my dissertation is to define a scientifically based training programme for the development of public sector cyber defence capability.

At the beginning of my research, I started from the assumption that a higher education course can be defined on scientific grounds. In order to prove this hypothesis**, I defined an eight-element process that specifies the steps in the design of science-based higher education courses and identified the research methods needed to define a course on a scientific basis.** The process and research methods presented here define only those elements necessary to define training. The more specific the target area, the more each part of the process should be further broken down, and additional research methodologies can be used to provide a sufficient basis for demonstrating the appropriateness of the training. I demonstrated the applicability of the process model and the associated research methods by fully defining public service cybersecurity training.

In line with my research objectives, I hypothesised that the target group required for the implementation of public service cybersecurity and the knowledge set they need to acquire can be identified. To verify this, **I identified the target group necessary for the implementation of cybersecurity in the public service as a criterion for designing the training programme, as well as the set of knowledge, skills and abilities they need to acquire, with the help of which the cybersecurity tasks in the public service can be achieve in line with the current cybersecurity challenges.**

This is because the target group and the knowledge set to be acquired are essential to justify the need for training, to identify similar types of training and to identify related practical experience. In order to define this target group and knowledge set as fully as possible, an in-depth interview and document analysis were used to identify the current challenges in cyberspace, to which the knowledge set to be acquired during the training is closely aligned.

This thesis is based on the assumption that there has not been a specific training programme for the development of cyber defence capability and practice in the public service. To prove this, I have compared and analysed national and international cybersecurity-related higher education courses based on a set of comparative criteria that I have defined. The aim of the comparison was to explore the feasibility of the training programme, with a view to avoiding duplication of training, since if there is already a training programme with the same content as the one targeted in this thesis, there is no reason to design it. In addition, the comparison was used to identify the shortcomings of the training courses examined and the 'good practices' followed. The advantage of implementing domestic and international experiences is that these are tried and tested practices that have already been proven in the domestic and international arena and whose effectiveness has already been demonstrated by the results of universities so their implementation in the domestic training system

can make a significant contribution to raising the quality of training and to creating quality. Through the above, **I have demonstrated the need for designing a training programme in the domestic training environment, which does not yet exist, to provide an opportunity to develop the cyber defence skills of non-IT-educated people working in the public service.** I have also demonstrated that public service cybersecurity training can be considered relevant internationally. Almost all the knowledge elements defined previously are included in the curricula of the courses examined, which shows that these knowledge elements are relevant for public service cybersecurity training.

In defining my research objectives, I hypothesised that a training programme for the development of the public service could be defined, the completion of which would not require a prior IT qualification. In order to prove this hypothesis, **I have defined a public service cybersecurity training program, the basics of the training, and the related core concepts, input and output requirements**. In this context, I identified the structure of the training and, using a curricular grid, I defined the topics and content of the theoretical and practical knowledge to be acquired during the training. I then proposed the possibility of applying the public service cybersecurity training in the Voluntary Reserve System by restructuring the training previously defined. In addition, I defined a set of criteria and a measurement method to measure the effectiveness of knowledge transfer during training, based on which we examined the appropriateness of the content of a course that fits the profile of public cybersecurity training and the effectiveness of knowledge transfer during university education. Measuring the effectiveness of knowledge transfer can be used to ensure the continuous improvement of the training subjects.

In my research, I hypothesised that a technical framework could be defined that would allow for the practical application of cyber defence strategies. In order to verify this hypothesis, **I defined the operational environment of a two-stage practical training. I identified a framework describing the simulation environment on which the practical training is based and defined an automated assessment system** to account for the knowledge delivered during the practical training part**.** The need for a framework describing the simulation environment is indicated by the fact that it can be used to prepare civil servants to detect cyber-attacks and, if they occur, to prevent and mitigate their consequences. The framework is based on practical experience and provides a learning environment for individuals and groups to learn effective and efficient cyber defence techniques. The framework allows the simulation of cyber-attacks and the practical application of protection mechanisms against cyber attacks through automated processes based on predefined specifications.

NEW SCIENTIFIC FINDINGS

E1 I have defined an eight-element process that defines the steps designing science-based higher education courses and the associated research methods.

For this scientific result, I have defined an 8-step process. I have demonstrated the validity, applicability and academic relevance of the process model by demonstrating the solution of each step by presenting possible scientific research methods and applying them to a case study.

E2 I have identified the target group for public cybersecurity training and the set of knowledge, skills and competencies they need to acquire.

I conducted a targeted in-depth interview to explore the differences between public and private sector cyber defence. Through the interview, I drew several conclusions (e.g. the role of user awareness in mitigating cyber security risks and the role of technological improvements) that can be incorporated into the content of public sector cyber security training. I identified the target group for the training and the tasks that belong to this group. I also identified the knowledge, skills, abilities and skills required to perform the tasks necessary to carry out the cybersecurity-related activities of the organisation.

E3 I have demonstrated the need to design a training programme in the domestic training environment that does not yet exist and that offers the opportunity to develop the cyber security skills of non-IT educated people in the public service, which is also relevant at international level.

In the context of this scientific result, I have demonstrated the need to design a training programme in the domestic training environment that does not yet exist, which provides an opportunity to develop the cyber defence skills of non-IT-educated people working in the public service. In addition, I have demonstrated that cybersecurity training in the public service can be considered internationally relevant training. The curricula of the training courses examined cover almost all previously defined knowledge elements, which shows that these elements are suitable for public service cybersecurity training.

E4 I have defined the structure, training programme, components and overall evaluation system of cybersecurity training in the public service that does not require a prior IT qualification.

I have defined the structure and elements of the public service cybersecurity training and the general content of the theoretical and practical part of the two-stage practical training, which includes the

cyber defence mechanisms and knowledge to be acquired. Furthermore, I have defined public service cybersecurity training, its input and output requirements and its main elements using the previously described knowledge set. I have determined a concept to measure the effectiveness of knowledge transfer, based on which the adequacy of the content of a course that fits the profile of public service cybersecurity education and the effectiveness of knowledge transfer in university education has been examined.

E5 I have defined a technical framework that allows for the practical application of protection strategies against cyber-attacks.

For this scientific result, I have defined a framework describing a simulation environment and outlined the hardware architecture of the framework and its components, simulating cyber attacks at the hardware and application level. In addition, I have defined an automated assessment system for practical training in a simulation environment. The effectiveness and applicability of the developed system was tested with participants matching the target group of the public cyber security training.

RECOMMENDATIONS AND THE PRACTICAL APPLICABILITY OF RESEARCH RESULTS

In my research, I have defined in detail a training programme aimed at improving cybersecurity in the public service, which provides an opportunity to acquire relevant cybersecurity skills for public service professionals with no prior IT training. Consequently, I recommend the practical use of my thesis:

(a) for the professionals responsible for the development of a public service training system for the implementation of cybersecurity training or some of its elements in the public service;
(b) for professionals working in the public service in order to develop their skills and knowledge based on the knowledge to be acquired;
(c) for managers of public service organisations to prepare their employees for cyber security;
(d) for higher education institutions, when planning the revision and design of related higher education training courses, to implement the elements of the training programme presented in this thesis;
(e) for the decision-makers of the Voluntary Reserve System in the design of training for the development of the cyber defence capabilities of the Voluntary Reserve personnel.

In order to ensure the long-term practical application and usability of the results of my research, it is advisable to determine the possible options for the continuation of the research presented in this thesis.

One of the main objectives of the research was to develop a practical training course to develop and improve civil servants' cyber defence skills. Further development of the research is essential to ensure that the practical application of this training programme is effective and of international value. A key component is **creating a platform or forum for national and international universities providing cybersecurity training to share their experiences and best practices.** Knowledge and experience sharing aim to continuously improve related training, identify gaps and adapt relevant "good practices" into their training. With the help of this platform, higher education institutions can identify how their own training can be improved and what changes and modifications are needed to improve the quality of training by using a method to measure the effectiveness of knowledge transfer and by carrying out continuous assessments and analyses.

LIST OF PUBLICATIONS PREPARED BY THE PHD CANDIDATE

Book chapter in Hungarian

[1] Angyal I, Arató Gy, Bakos B, Baranya Zs, Bocsok V, Bogáncs T, Bonnyai T, Buttyán L, Csatár J, Danyek M, **Deák Veronika**, Görgey P, Gyebnár G, Illés G, Krasznay Cs, Molnár F, Pongrácz P, Szabó-Nyakas Zs, Szádeczky T, Szent-Királyi B, Winter G: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve – www.seconsys.eu (2021).

[2] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés tervezése tudományos alapokon* – Hausner Gábor (szerk): Szemelvények a katonai műszaki tudományok eredményeiből II., Ludovika Egyetemi Kiadó, 2020. Budapest, 63-82.

[3] **Deák Veronika**: Hírszerzés a kibertérben – Krasznay Csaba (szerk): Taktikák és stratégiák a kiberhadviselésben Ludovika Egyetemi Kiadó, 2023. Budapest, 87-114.

Peer-reviewed international foreign language journal paper

[4] **Deák Veronika**: *Simulation Framework for Practical Cyber Security Training in the Public Service* – Security and Defense Quarterly: Non-military aspects of security in the changing international order, 33. évfolyam, 1. szám (2021), 87-104.

Peer reviewed national foreign-language journal paper

[5] **Deák Veronika**: *Finding differences on cyber security between public and private sectors* – National Security Review, 1. szám (2021), 169-180.

Peer reviewed Hungarian-language journal paper

[6] Krasznay Csaba, **Deák Veronika**: *Adatbiztonsági informatikai alapismeretek átadásának vizsgálata egy szakirányú továbbképzés keretében* – Hadmérnök, XVI. évfolyam 4. szám (2021), 112-132

[7] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban* – Hadmérnök, XV. évfolyam 4. szám (2020), 157-178

[8] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon* – Hadmérnök, XV. évfolyam 3. szám (2020), 157-178.

[9] **Deák Veronika**: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* – Hadmérnök, XIII. évfolyam 3. szám (2018), 391-402

[10] **Deák Veronika**: *Biztonságtudatosság az információs környezetben* – Szakmai Szemle, XV. évfolyam, 3. szám, 2017. november, 59-77.

[11] **Deák Veronika**: *Kártékony programok terjedése social engineering technikákon keresztül* – Hadmérnök, XIV. Évfolyam 2. szám (2019), 256-271

[12] **Deák Veronika**: *Prototípus implementáció kibervédelmi technikák gyakorlati oktatására* – (Elbírálás alatt)

[13] **Deák Veronika**: *Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során* – Hadmérnök, XIV. Évfolyam 12. szám (2019), 95-111

[14] **Debrecenine Deák Veronika**, Hegyi Henrietta, Koczka Ferenc: *Felhőszolgáltatások műszaki és jogi szempontú attitűdvizsgálata* – Felderítő Szemle, XXI. évfolyam 1. szám (2022), 67-89.

Abstract/Posters published in Hungarian national conference proceedings

[15] Beláz Annamária, **Deák Veronika***: Kiber gyakorlatok és szerepük (poszter),* A biztonság sokszínű arca konferencia, 2018. november 1. DOI:10.13140/RG.2.2.26756.37767

[16] **Deák Veronika**: *Social engineering és biztonságtudatosság*, XXIII. Tavaszi Szél konferencia Absztraktkötet, 2018., 140., ISBN: 978-615-5586-26-2

[17] **Deák Veronika**: *Social engineering felhasználása a lélektani műveletek során*, XXII. Tavaszi Szél konferencia Absztraktkötet, 2019., 240., ISBN: 978-615-5586-42-2

[18] **Deák Veronika**: *A közszolgálati kibervédelmi képesség gyakorlati képzésének technikai és technológiai alapjai*, XXIII. Tavaszi Szél konferencia Absztraktkötet, 2020., 188., ISBN:978-615-5586-70-5

PROFESSIONAL-SCIENTIFIC BIOGRAPHY OF THE DOCTORAL CANDIDATE

Name: Dr. Veronika Debreceniné Deák

Studies:

2011-2015 University of Public Service, Faculty of Public Administration - Bachelor of Public Administration

2015-2017 University of Public Service, Faculty of Public Administration - Expert of Public Administration with Specialisation in Public Management

2016-2018 Eötvös Loránd University, Institute for Continuing Legal Education - Data Protection and Data Security Law

2017- National University of Public Service, Doctoral School of Military Engineering - PhD training

2021-2022 National University of Public Service - Institute for Advanced Training in Public Administration - Electronic Information Security Manager postgraduate specialist training course

Professional career:

From 2019, she was a security expert at Login Autonom Kft for one and a half years. Since the same year, she has been the privacy and data security expert for the IT security awareness channel "IT Security Angels" on the Probono public training portal. From 1 September 2020, she continued her work as Data Protection Officer at the National University of Public Service and from 2022, she will continue in this position as Head of the Data Protection Office. Since 2017, she has also been involved in several national and international research and curriculum development projects.

Language skills:

She holds an intermediate complex language certificate in English and German.

Memberships:

Between 2018 and 2022 she was a member of the NKE University Doctoral Council and since 2018 she is a member of the Hungarian Society of Military Science, Section of Electronics, Informatics and Robotics.

Awards and recognitions:

In 2017, she was awarded 1st place in the Cybersecurity Section of the XXXIII OTDK, Military and Law Enforcement Sciences Section.