MATHEMATICAL AND COMPUTER MODELING

DOI 10.20535/2411-1031.2024.12.2.31574
UDC 378.147:004.056.5

SERHII HORLICHENKO,
ANASTASIIA HORLICHENKO

MATHEMATICAL MODEL FOR OPTIMISING THE CONTEMPORARY PROCESS OF TRAINING SPECIALISTS IN THE FIELD OF CYBERSECURITY AND INFORMATION PROTECTION

The article examines current issues of training cybersecurity specialists, which are of particular importance in the context of rapid development of information technology and the growing number of cyber threats. It is noted that in Ukraine, as in many other countries, there are problems related to the organisation and management of the process of training such specialists. Traditional teaching methods do not always correspond to the specifics of the rapidly changing cyber environment, which makes it difficult for graduates to adapt to real working conditions. There is also a lack of uniform methodological approaches to regulating the educational processes in the field of cybersecurity, which leads to different quality of training in different educational institutions. Emphasises the need to develop a mathematical model for optimising the modern educational process of cybersecurity specialists, which would provide an integrated approach to planning and managing the training of cybersecurity specialists. Analyses the latest scientific researches and publications on the education of cybersecurity specialists, which investigated the problems and ways of improving cyber-education both in Ukraine and abroad. The purpose of the article is to develop a mathematical model for optimising the modern educational process of training cybersecurity specialists. This model takes into account the interaction between students, teachers and employers, as well as the dynamic development of students' competences. The authors propose to define the main roles of the participants in the educational process and their strategies. The model allows to take into account the transition probabilities of the development of students' competences and possible risks associated with the choice of certain educational pathways. The proposed mathematical model makes it possible to optimise the process of training specialists, which will help to improve their professional competence and ability to respond to current challenges in the field of cybersecurity. Such an integrated approach makes it possible to ensure effective decision-making at each stage of the educational process, which is extremely important for training qualified personnel in the field of cybersecurity, capable of countering modern cyber threats and ensuring high levels of information security.

Key words: cybersecurity, training of specialists, mathematical model, competencies, information security.

Problem statement. The accelerated evolution of information and communication technology, coupled with the exponential growth of cyber threats, has created an urgent need to develop a cadre of highly qualified cyber security professionals who can effectively address today's challenges in the field of information protection. However, in Ukraine, as in many other countries, there are a number of challenges associated with the planning and management of training programmes for such specialists.

Firstly, traditional teaching methods often fail to take into account the specifics of the dynamically changing cyber environment, which makes it challenging for graduates to adapt to real-world work conditions. Secondly, the lack of consistent methods governing the training process results in a disparity in the quality of training across different educational institutions. Thirdly, there

is a dearth of practice-oriented curricula that would equip students with the requisite skills to work in the face of real cyber threats.

These issues necessitate the formulation of a methodological framework that would facilitate a comprehensive approach to the planning and management of the training process for cybersecurity specialists. This encompasses the introduction of contemporary teaching methodologies tailored to market demands and the establishment of efficacious educational management systems. It is also crucial to integrate the latest technologies and methodologies that will assist students in developing the practical competencies essential for successful professional activities in the context of contemporary cyber threats.

The analysis of recent research and publications in the field of cybersecurity reveals that the issues surrounding the training of qualified personnel and potential avenues for improvement are subjects of investigation by domestic scholars, including Melnyk S. [1], Danik Y. [2], Stashevsky Z. [3], and others.

In his work, Melnyk S. V. presents a rationale for optimising the professional training of future cybersecurity specialists [1]. This is to be achieved on the basis of innovative pedagogy and an integrated approach to the implementation of key security competencies in the context of the information society.

In their work, Danik Y. and Zinchenko A. conducted an analysis of the current state of cyber education, both in Ukraine and globally [2]. They demonstrated that, in the modern context, cybersecurity knowledge should be integrated into the fundamental curriculum of all educational institutions, rather than being confined to specific IT and cybersecurity specialisations.

Stashevskyi Z. P. and Hrytsiuk Y. I. investigated the distinctive characteristics of developing a model for the implementation of the educational process of the higher education institution of the SES of Ukraine based on a competence-based approach [3]. This approach defines the main goals of the project and the project product as the integral competence of the SES personnel for the implementation of IT projects in information security.

The paper [4] puts forth mathematical models of prospective professionals' competencies and, based on these models, delineates the objectives of studying such competencies.

Baofa Sun put forth four mathematical models of learning effectiveness: the model of examination control, the model of talent development, the model of career growth, the model of career development, and the model of quality education [5]. Additionally, the paper identifies key issues that students should prioritize.

In their work [6], a group of scientists proposed the Delphi method, which was employed to develop a model of the learning system. This approach enabled them to gain a comprehensive understanding of the current training requirements and recommendations.

The aim of this work is to develop a mathematical model for optimising the contemporary process of training specialists in the field of cybersecurity and information protection.

The exposition of the main research material. In the context of the global challenges and threats to information security, a growing number of countries, including Ukraine, are enacting legislative measures with the objective of enhancing the protection of information resources. These legal instruments delineate the standards and requirements pertaining to information security, while also delineating the requisite knowledge and skills that professionals engaged in this field should possess.

To illustrate, a comparative table of the competencies required for Bachelor's [7] and Master's [8] degree programmes in Cybersecurity and Information Protection with the competencies outlined in the professional standard for the head of a structural unit for information security and cybersecurity [9] can be used to demonstrate the alignment between the two sets of competencies. (see Table 1).

This table provides a more comprehensive representation of the manner in which the competencies inherent to the educational programmes and the professional standard are divided into key areas of knowledge and skills.

Table 1 – Competency mapping table

Educational programme	Competence code of the educational programme	Competence code by professional standard	Competence category
Bachelor	ІК	А1	Risk Management
Bachelor	ЗК 1	А2	Risk Management
Bachelor	ЗК 2	А3	Risk Management
Bachelor	ЗК 3	Г3	International Standards
Bachelor	ЗК 4	Б1	Risk Management
Bachelor	ЗК 5	В2	Risk Management
Bachelor	ФК 1	Б2	Risk Management
Bachelor	ФК 2	Б3	International Standards
Bachelor	ФК 3	Б4	Legal Knowledge
Bachelor	ФК 4	В1	Risk Management
Bachelor	ВПК 1	В3	Risk Management
Bachelor	ВСК 1	Г1	Risk Management
Bachelor	ВСК 2	Г2	International Standards
Master	КІ	А1	Risk Management
Master	КЗ 1	А2	Risk Management
Master	КЗ 2	Б1	Risk Management
Master	КЗ 3	Г1	Risk Management
Master	КЗ 4	Б4	Legal Knowledge
Master	КФ 1	В2	Technical Skills
Master	КФ 2	Б2	Risk Management
Master	КФ 3	Б3	International Standards
Master	КФ 4	В1	Risk Management
Master	КФ 5	В3	Risk Management
Master	КФ 6	Г2	International Standards

As defined in the study [10], a cybersecurity specialist is a qualified professional who not only ensures secure information activities but also has a comprehensive understanding of all aspects of information security, including legal, social, software and hardware, and psychological. The specialist's work is based on information resources and their infrastructure, and their expertise allows them to effectively perform professional duties and promote their own professional development.

To achieve the definition of a “cybersecurity specialist”, we propose a mathematical model that will help us optimise the process of training cybersecurity specialists, taking into account the interaction between students / cadets, teachers and employers, as well as the dynamic development of students' competencies.

Based on well-known methods [11], let us define the main roles and their strategies:

1. Student: Chooses courses, internships and other educational trajectories.
2. Teacher: Decides which curricula and teaching methods to implement.
3. Employer: Determines the requirements for graduate competences and offers internship opportunities.

Based on Table 1, we define quantitative indicators for each competence, in particular for bachelor's and master's degrees. Each competence has a quantitative assessment on a scale from 0 to 100, where 0 means no competence and 100 means full mastery of the competence.

The following competences have been integrated into the model:

– Risk Management – RM;
– Legal Knowledge – LK;
– Technical Skills – TS;
– International Standards – IS.

It can be reasonably assumed that students will progress at different rates and that their competence will develop in a gradual manner, moving from one state to another:

– S_1 (Low level of competence): This level is characterised by a basic knowledge and initial experience;

– S_2 (Intermediate level of competence): This level is defined by the ability to perform more complex tasks under supervision;

– S_3 (Proficient): This level is defined by the ability to solve complex problems independently.

The transition probabilities can be calculated using the following equation:

$$P(S_{t+1}|S_t, a_t) = f(RM, LK, TS, IS) = w_1 \times RM + w_2 \times LK + w_3 \times TS + w_4 \times IS, \quad (1)$$

where w_i – weighting factors reflecting the importance of each competency.

Using the function of utility and use (1), we obtain:

$$U(S_t) = P(S_{t+1}|S_t, a_t), \quad (2)$$

Furthermore, we are aware that a significant factor in the decision-making process is the inherent risk associated with potential actions. Consequently, participants may adjust their strategies in response to an assessment of the associated risk, resulting in a modified version of formula (2) as follows:

$$U(S_t) = P(S_{t+1}|S_t, a_t) - R_F(a_t), \quad (3)$$

where $R_F(a_t)$ – risk factor associated with the action a_t .

$$R_F(a_t) = P_R(RM, LK, TS, IS) \times I_R$$

where $P_R(RM, LK, TS, IS)$ – probability of risk is contingent upon indicators of competence;

I_R – risk exposure.

Subsequently, the utility functions for each participant will be calculated using equation (3), resulting in the following formulas:

$$U_{student}(S_t) = P(S_{t+1}|S_t, a_t) - R_F(a_t)$$

$$U_{Instructor}(S_t) = P(S_{t+1}|S_t, b_t) - R_F(b_t)$$

$$U_{Employer}(S_t) = P(S_{t+1}|S_t, c_t) - R_F(c_t)$$

It is possible for participants to alter their strategies with the intention of reducing the likelihood of adverse outcomes or to accommodate alterations in circumstances:

$$a_t^* = argmin[R_F(a_t)]$$

1. The student selects courses with a lower risk profile.
2. The teacher modifies their teaching methods to reduce risk.
3. The employer modifies their requirements to avoid risk.

Once all participants have selected the most optimal strategy and no further improvement in outcome can be achieved by modifying their strategy alone, equilibrium will be reached. The resulting state will be as follows:

$$(S^*, a^*, b^*, c^*) = argmax[U_{Student}(S_t) \times U_{Instructor}(S_t) \times U_{Employer}(S_t)]$$

In order to determine the optimal strategy for maximising the usefulness of participants in the educational process, we propose the use of a mathematical model which facilitates the calculation of the optimal strategy. This will be achieved through the utilisation of a code developed based on the Python programming language [12]:

```
...
class Player:
    def init(self, name, strategies):
        self.name = name
        self.strategies = strategies
        self.selected_strategy = strategies[0]

def utility_function(competencies, weights, risk_factor):
    utility = (
        weights["RiskManagement"] * competencies["RiskManagement"] +
        weights["LegalKnowledge"] * competencies["LegalKnowledge"] +
        weights["TechnicalSkills"] * competencies["TechnicalSkills"] +
        weights["InternationalStandards"] * competencies["InternationalStandards"]
    )
    return utility - risk_factor

def evaluate_strategy(player, strategy):
    risk_factor = np.random.uniform(0, 0.5)
    return utility_function(competencies, weights, risk_factor)

def choose_optimal_strategy(player):
    utilities = [evaluate_strategy(player, strategy) for strategy in player.strategies]
    optimal_strategy = player.strategies[np.argmax(utilities)]
    return optimal_strategy

states = ["Low", "Medium", "High"]
transition_matrix = np.array([
    [0.6, 0.3, 0.1],
    [0.2, 0.7, 0.1],
    [0.0, 0.2, 0.8]
])
current_state = 0

def next_state(current_state):
    return np.random.choice([0, 1, 2], p=transition_matrix[current_state])

def simulate_education_process(steps=10):
    state = current_state
    result = []
    for _ in range(steps):
        result.append(state)
        state = next_state(state)
    return result

def risk_assessment(competencies):

    if competencies["RiskManagement"] < 50 or competencies["TechnicalSkills"] < 50:
        probability_risk = 0.6
    else:
        probability_risk = 0.3

    impact_risk = np.random.uniform(0, 1)
    risk = probability_risk * impact_risk
    return risk

def adaptive_risk_management(player):
    risks = [risk_assessment(competencies) for strategy in player.strategies]
    min_risk_strategy = player.strategies[np.argmin(risks)]
    return min_risk_strategy
...
if __name__ == "__main__":
    root = tk.Tk()
    app = CybersecurityTrainingApp(root)
    root.mainloop()
```

The application interface is illustrated in Figure 1.

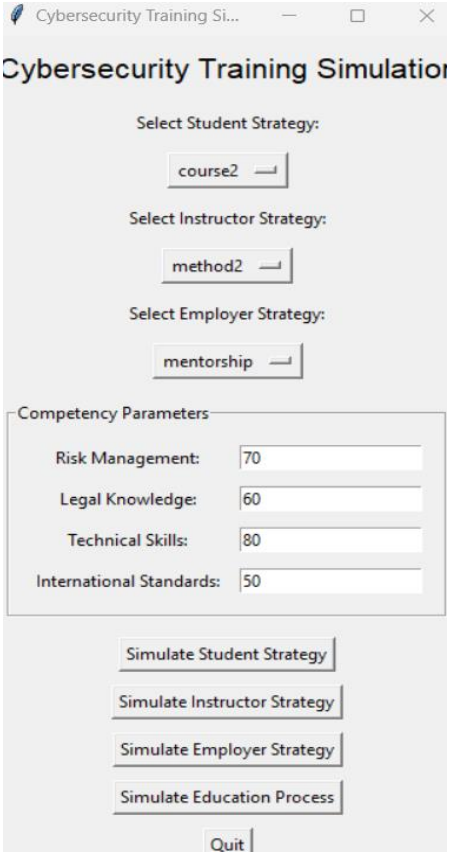

Figure 1 – Application interface

The evolution of the student's/cadet's proficiency, contingent on the selected learning methodologies and the employer's operational parameters, can be observed in the graph that will be accessible subsequent to the simulation (see Figure 2).

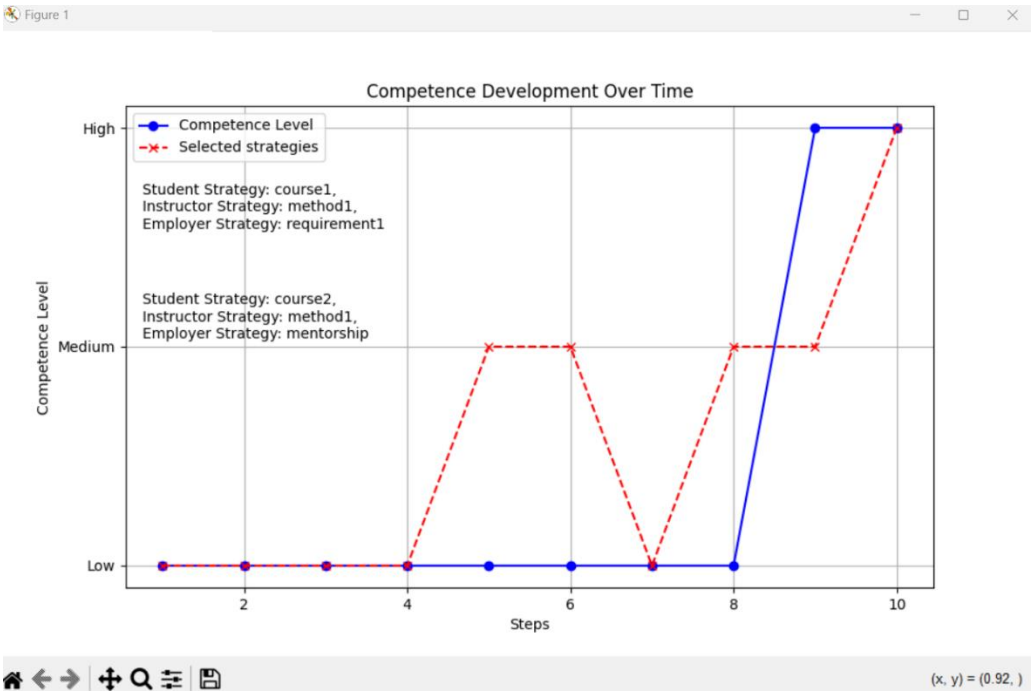

Figure 2 – Competency progression chart.

Conclusions. The proposed mathematical model and the programme that implements it facilitate the exploration of diverse approaches to cybersecurity education and the assessment of their efficacy, thereby enabling the preparation of highly qualified specialists equipped to confront the challenges of contemporary cyberspace..

Further research is recommended in order to improve the optimisation of mathematical models. In addition to students' competencies, external factors such as technological changes and cyber threats should also be considered. The impact of gamification on the learning process in the field of cybersecurity is also worthy of further investigation, with scenarios for educational games that simulate real-life threats and problems in information security being created.

REFERENCES

[1] S. Melnyk, S. Voskoboinikov, and D. Stupak, "Optimisation of professional training of future cybersecurity specialists based on innovative pedagogy and integrated approach in the system of implementation of key security competencies in the information society", *Vtoky pedagogicheskoho mastership*, no. 21, pp. 125-129, 2018. [Online]. Available: http://dspace.pnpu.edu.ua/bitstream/123456789/11641/1/Melnyk.pdf. Accessed on: Aug. 15, 2024.

[2] Y. Danik, and A. Zinchenko, "Cyber education and its features", *Military Education*, no. 2, pp. 67-84, 2018. doi: https://doi.org/10.33099/2617-1783/2018-2/67-84.

[3] Y.I. Hrytsiuk, and Z.P. Stashevskyi, "Model of the process of forming the competence of the SES of Ukraine personnel for the implementation of IT projects on information security", *Scientific Bulletin of the National Technical University of Ukraine*, vol. 25, no. 9, pp. 373-390, 2015. doi: https://doi.org/10.15421/40250958.

[4] D.D. Aistrakhanov, "Mathematical models of professional competence of a future specialist", *Vestnik Vinnytsia Polytechnic Institute*, no. 3, pp. 136-140, 2014. [Online]. Available: https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/945/944. Accessed on: Aug. 9, 2024.

[5] B. Sun, "Mathematical models of learning efficiency", *EURASIA J. Math. Sci. Technol. Educ.*, 13 (7), pp. 4261-4270, 2017. doi: https://doi.org/10.12973/eurasia.2017.00834a.

[6] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study", *Comput. & Secur*., no 113, 15 p., 2022. doi: https://doi.org/10.1016/j.cose.2021.102551.

[7] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (May 13, 2024). *Educational and professional program First (bachelor's) level of higher education, ID 57879, Security of information resources*. [Online]. Available: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppb_bdir_2024.pdf. Accessed on: Aug. 1, 2024.

[8] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (May 13, 2024). *Educational and professional program Second (master's) level of higher education, ID 57881, Security of information resources*. [Online]. Available: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppm_bdir_2024.pdf. Accessed on: Aug. 1, 2024.

[9] 1239 Head of the structural unit for information security and cyber defense, Professional standard. [Online]. Available: https://register.nqa.gov.ua/uploads/0/576-kerivnik_strukturnogo_pidrozdilu_z_pitan_bezpeki_informacii_ta.pdf. Accessed on: Aug. 7, 2024.

[10] S. Horlichenko, "Features of modern conceptual and terminological apparatus in the field of training of cyber security specialists", *Cybersecurity: Education, Science, Technology*, vol. 3, no. 23, pp. 171-181, 2024. doi: https://doi.org/10.28925/2663-4023.2024.23.171181.

[11] V.D. Romanenko, Ed. Game theory: a course of lectures. Kyiv, Ukraine: Igor Sikorsky Kyiv Polytechnic Institute, 2022. [Online]. Available: https://ela.kpi.ua/bitstream/123456789/49092/1/Teoriia_ihor.pdf. Accessed on: Aug. 7, 2024.

[12] The Python tutorial. [Online]. Available: https://docs.python.org/3/tutorial/index.html Accessed on: Aug. 5, 2024.

The article was received 15.08.2024.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] С.В. Мельник, С.О. Воскобойніков, та Д.Є. Ступак, "Оптимізація фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі релізації ключових компетенцій безпеки в інформаційному суспільстві", *Витоки пед. майстерності*, № 21, с. 125-129, 2018. [Електронний ресурс]. Доступно: http://dspace.pnpu.edu.ua/bitstream/123456789/11641/1/Melnyk.pdf. Дата звернення: Серп. 15, 2024.

[2] Ю. Даник, та А. Зінченко, "Кіберосвіта та її особливості", Військ. освіта, № 2, с. 67-84, 2018. doi: https://doi.org/10.33099/2617-1783/2018-2/67-84.

[3] Ю.І. Грицюк, та З.П. Сташевський, "Модель процесу формування компетентності персоналу ДСНС України для реалізації ІТ-проектів з інформаційної безпеки", *Наук. вісн. НЛТУ України*, т. 25, № 9, с. 373-390, 2015. doi: https://doi.org/10.15421/40250958.

[4] Д.Д. Айстраханов, "Математичні моделі професійної компетентності майбутнього фахівця", *Вісн. Вінн. політехн. ін-ту*, № 3, с. 136-140, 2014. [Електронний ресурс]. Доступно: https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/945/944. Дата звернення: Серп. 9, 2024.

[5] B. Sun, "Mathematical models of learning efficiency", *EURASIA J. Math. Sci. Technol. Educ.*, 13 (7), pp. 4261-4270, 2017. doi: https://doi.org/10.12973/eurasia.2017.00834a.

[6] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study", *Comput. & Secur.*, no 113, 15 p., 2022. doi: https://doi.org/10.1016/j.cose.2021.102551.

[7] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" (2024, 13 трав.). *Освітньо-професійна програма Перший (бакалаврський) рівень вищої освіти, ID 57879, Безпека інформаційних ресурсів*. [Електронний ресурс]. Доступно: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppb_bdir_2024.pdf. Дата звернення: Серп. 1, 2024.

[8] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" (2024, 13 трав.). *Освітньо-професійна програма Другий (магістерський) рівень вищої освіти, ID 57881, Безпека інформаційних ресурсів*. [Електронний ресурс]. Доступно: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppm_bdir_2024.pdf. Дата звернення: Серп. 1, 2024.

[9] 1239 Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту, професійний стандарт. [Електронний ресурс]. Доступно: https://register.nqa.gov.ua/uploads/0/576-kerivnik_strukturnogo_pidrozdilu_z_pitan_bezpeki_informacii_ta.pdf. Дата звернення: Серп. 7, 2024.

[10] С. Горліченко, "Особливості сучасного понятійно-термінологічного апарату у сфері підготовки фахівців з кібербезпеки", *Кібербезпека: освіта, наука, техніка*, т. 3, № 23, с. 171-181, 2024. doi: https://doi.org/10.28925/2663-4023.2024.23.171181.

[11] В.Д. Романенко, Ред. *Теорія ігор: Курс лекцій*. Київ, Україна: КПІ ім. Ігоря Сікорського, 2022. [Електронний ресурс]. Доступно: https://ela.kpi.ua/bitstream/123456789/49092/1/Teoriia_ihor.pdf. Дата звернення: Серп. 7, 2024.

[12] The Python tutorial. [Online]. Available: https://docs.python.org/3/tutorial/index.html Accessed on: Aug. 5, 2024.

СЕРГІЙ ГОРЛІЧЕНКО,
АНАСТАСІЯ ГОРЛІЧЕНКО

МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ ОПТИМІЗАЦІЇ СУЧАСНОГО ПРОЦЕСУ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядаються актуальні питання підготовки фахівців з кібербезпеки, що набувають особливого значення в умовах стрімкого розвитку інформаційних технологій і зростання кількості кіберзагроз. Зазначається, що в Україні, як і в багатьох інших країнах, існують проблеми, пов'язані з організацією та управлінням процесом підготовки таких фахівців. Традиційні методи навчання не завжди відповідають специфіці швидкозмінного кіберсередовища, що ускладнює адаптацію випускників до реальних умов роботи. Також існує відсутність єдиних методологічних підходів до регулювання освітніх процесів у сфері кібербезпеки, що призводить до різної якості підготовки в різних навчальних закладах. Наголошується на необхідності розробки математичної моделі для оптимізації сучасного навчального процесу фахівців з кібербезпеки, яка б забезпечили комплексний підхід до планування та управління підготовкою фахівців з кібербезпеки. Проаналізовано останні наукові дослідження та публікації, присвячені питанням підготовки фахівців з кібербезпеки, які досліджували проблеми та шляхи вдосконалення кіберосвіти як в Україні, так і за її межами. Мета статті полягає у розробці математичної моделі для оптимізації сучасного навчального процесу підготовки фахівців з кібербезпеки. Ця модель враховує взаємодію між студентами, викладачами та роботодавцями, а також динамічний розвиток компетенцій студентів. Пропонується визначити основні ролі учасників освітнього процесу та їх стратегії. Модель дозволяє врахувати перехідні ймовірності розвитку компетенцій студентів і можливі ризики, пов'язані з вибором тих чи інших освітніх траєкторій. Запропонована математична модель дозволяє оптимізувати процес підготовки фахівців, що сприятиме підвищенню їх професійної компетентності та здатності реагувати на сучасні виклики у сфері кібербезпеки. Завдяки такому комплексному підходу можливо забезпечити ефективне прийняття рішень на кожному етапі освітнього процесу, що є надзвичайно важливим для підготовки кваліфікованих кадрів у сфері кібербезпеки, здатних протидіяти сучасним кіберзагрозам та забезпечувати інформаційну безпеку на високому рівні.

Ключові слова: кібербезпека, підготовка фахівців, математична модель, компетенції, інформаційна безпека.

Horlichenko Serhii, researcher at the Research centre, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. ORCID 0000-0002-8999-7526, serhii.horlichenko@gmail.com.

Horlichenko Anastasiia, engineer of the first category of the Research centre, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. ORCID 0000-0002-9845-5809, a.poliakova@kpi.ua.

Горліченко Сергій Олександрович, науковий співробітник Науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

Горліченко Анастасія Сергіївна, інженер І категорії Науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.