МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

университет информатики и радиоэлектроники, Республика Беларусь)	
THE STATE OF CYBER SECURITY DEVELOPMENT FOR CERTAIN CRITICAL DOMAINS IN THE REPUBLIC OF MOLDOVA. ***AURELIAN BUZDUGAN*** (Moldova State University, Republic of Moldova)	38
АНАЛІЗ ШИФРІВ У БЕЗДРОТОВИХ МЕРЕЖАХ. ***КУЛЯ Ю.Е.*** (Харківський національний університет радіоелектроніки), ***ГАВРИЛОВА А.А.*** (Харківський національний економічний університет імені Семена Кузнеця)	40
ВИКОРИСТАННЯ СИСТЕМИ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ В АНТИ-ФОРЕНЗИЦІ. ***МАКАРЕНКО А.О.*** (Харківський національний економічний університет імені Семена Кузнеця)	42
DDOS-АТАКИ НА ОСВІТНІ ВЕБ-РЕСУРСИ. ***КОРОЛЕВИЧ Є.М., ПЛОТНІКОВ В.М., ЗІНЧЕНКО І.І.*** (Одеська національна академія харчових технологій)	44
ОЦІНКА ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФРАСТРУКТУРІ "РОЗУМНИЙ БУДИНОК". ***ЄРЕЩЕНКО О.Д.,*** (Харківський національний університет імені Семена Кузнеця)	46
ПРО ВРАХУВАННЯ СТАВЛЕННЯ ДО РИЗИКУ В ПРОСТОРОВИХ СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ. ***КЛЕПАТСЬКА В.В., БУЧИНСЬКА І.В., КУЗНІЧЕНКО С.Д. (***Одеський державний екологічний університет)	47
КЛАСИФІКАЦІЯ ЗАГРОЗ ВЕБ-ЗАСТОСУНКІВ. ***ЛАВРЄНОВ В.А., СІРЕНКО О.І.,*** (Одеська національна академія харчових технологій)	49
PROOF OF ZERO-KNOWLEDGE IN THE TASKS OF ANONYMIZATION OF FINANCIAL TRANSACTIONS. ***PROKOPOV E.K.*** (Odessa I.I. Mechnikov National University)	51
РОЗРОБКА ПРОГРАМИ ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ОРИГІНАЛЬНІСТЬ. ***БЕВЗ С.В., БУРБЕЛО С.М., ВОЙТКО В.В., ЗАВАЛЬНЮК Є.К.*** (Вінницький національний технічний університет)	52
АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ. ***КАСІЯНЕНКО Д.В. (***Київський національний університет імені Тараса Шевченка)	54
РОЗРОБКА УНІВЕРСАЛЬНОЇ ІНФОРМАЦІЙНОЇ УПРАВЛЯЮЧОЇ СИСТЕМИ ДЛЯ ОРГАНІЗАЦІЇ РОБОТИ СКЛАДУ. ***КРИВИЙ Є.О., ШВЕЦЬ Н.В.*** (Одеська національна академія харчових технологій)	56
ВИКОРИСТАННЯ ГРАФІЧНОГО ФРЕЙМВОРКУ LIBGDX ДЛЯ РОЗРОБКИ КРОСПЛАТФОРМНИХ ІГОР. ***РОМАНЮК О.Н., ВЕРЕНЬКО А.І., МИРГОРОДСЬКИЙ А. В.*** (Вінницький національний технічний університет)	58
DEVELOPMENT OF MODELS AND ALGORITHMS FOR THREE-FACTOR AUTHENTICATION SYSTEM. ***DONETS O.V.*** (V. N. Karazin Kharkiv National University), ***RADOUTSKA A.K.*** (Kharkiv National University of Radio Electronics)	60
КОМП'ЮТЕРИЗОВАНИЙ ВІДБІР ОПЕРАТОРІВ БПЛА. ***МАРУЩАК А.В., ШМАЛЮХ В.А., РОМАНЮК О.Н., КОВАЛЬ Л.Г.*** (Вінницький національний технічний університет)	61
ПАСИВНИЙ МЕРЕЖЕВИЙ АНАЛІЗ ТА ЗАСОБИ ЙОГО ВДОСКОНАЛЕННЯ. ***ЖОЛНЕР І.Д., МИРУТЕНКО Л.В., ШЕСТАК Я.В. (***Київський національний університет ім. Тараса Шевченка)	63
АНАЛІЗ ХМАРНОЇ ТЕХНОЛОГІЇ GOOGLE DRIVE. ***РОМАНЮК О.Н., БОРИСОВА К.О., КАТЄЛЬНІКОВ Д.І.*** (Вінницький національний технічний університет)	65
АНАЛІЗ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ. ***ТРОЩІЙ А.О.*** (Харківський національний економічний університет імені Семена Кузнеця)	67

THE STATE OF CYBER SECURITY DEVELOPMENT FOR CERTAIN CRITICAL DOMAINS IN THE REPUBLIC OF MOLDOVA

AURELIAN BUZDUGAN, M. Sc, doctoral student
Moldova State University (Republic of Moldova)

In this paper we will update upon the research performed on cyber security program development for specific domains in Republic of Moldova. We will analyze the findings of previous case studies on evaluation of cyber security requirements for healthcare, nuclear and radiological domain, and map the obtained results to the recently developed Model for Cyber Security Maturity Assessment in Critical Infrastructures (herein after as Model) [1]. The proposed model focuses on four primary dimensions (Policies and administration; Education and training; Work environment; Cyber risk management) and was built with the scope to analyze the efficiency of potential information systems used for cyber risk management. The model is multidimensional, as it can also show the actual state of cyber security maturity in an organization, fact which was also proven by external reviews. The results of this analysis will help confirm the applicability of the Model for organizations at different stages of cyber security development, as well as from different domains.

The digitalization and use of computer systems in various domains has offered tremendous growth and development opportunities for critical infrastructure (CI) domains. However, digitalization has also created challenges in identifying and managing cyber risks in the CI domain. In this paper we will review the cyber security developments in the nuclear and radiological (NR) domain.

The cyber security program development for the NR domain is strongly linked to international guidance and recommendations, as well as threat landscape increase level. One of the first analysis performed in 2015 presented the inclusion of cyber security in the safe and security use of nuclear and radiological entities. The NR domain legislation includes cyber security as part of nuclear security, which creates premises for a horizontal cooperation with IT specialized bodies. In addition, the IT security was confirmed as intrinsic part for physical security systems and dictated specific technical requirements such as user access, monitoring and incident reported or data confidentiality. This situation can be interpreted via the proposed model where all dimension would have below average ratings, indicating a need to develop and improve the Policies and Administration section. In a later analysis from 2016 [2], we stressed the strong link between the overall national cyber security maturity, and the developments in certain domains. In addition, the National Cyber Security Program covered aspects as functions, responsibilities and training indicators [3]. Therefore, through the prism of the Model, it is suggested to develop the Education and Training component simultaneously, to raise the overall cyber security level which directly can lead to a better legal framework development. In 2017, we have also analyzed the Decision on Minimum Cyber Security Requirements [4], which is a holistic document focusing on all areas of cyber security. In relation to our Model, we believe the document is requiring the maturity increase for dimension such as technical tools or configuration, user awareness and training, via legislative initiatives. In this case, the model would show different results compares to 2015 where there would be high ratings for the Policies and Administration when it comes to national legislation, and lower ratings for the rest of the domains. We believe this situation is characteristic for many countries in the context of cyber security program development.

Furthermore, we performed an analysis on cyber security in the healthcare domain, which is also part of the CI. The findings at that time (2016, 2019) have shown that while technologies exist, these cannot be enforced without national policies and regulations in this sense [5]. We believe this is also strongly correlated to the mindset and overall security culture, as human dimension has a

strong influence upon the development of the legal framework. Therefore, we see a correlation in the development phase which is confirmed by the first two dimension of the Model, key for triggering overall technical developments. As solutions to this context, a horizontal cooperation has been recommended with domains that are at the same stage, or have went through significant developments in the past years, such as the nuclear and radiological domain. Moreover, this solution is necessary in the context of existence of a large number of ionizing radiation sources in the healthcare domain, as well as the imminent need to ensure cyber security of healthcare devices in the context of Covid-19 pandemic.

One last development in the legal framework of Moldova is the Information Security Strategy for 2020-2024. This document highlights the gap of ensuring cyber security for CI domain, as well as the need for developing policies in this matter. We believe the findings and results of the proposed Model, in light of previous case studies performed in this domain, match the current status.

In conclusion, cyber security program development is a complex process that requires a holistic approach. Various methods to evaluate the gaps and priorities can be applied, such as via external assessments [7] or practical models. The findings in this paper are a valuable input for the interpretation of results given by the proposed Model, such as the prioritization of policy development when all dimensions have a low score, as well as the need to have a general approach covering also education and training, and specifically raising awareness about the need of cyber security improvements.

REFERENCES

[1] A. Buzdugan, Gh. Capatana, (2021) - Cyber Security Maturity Model for Critical Infrastructures [submitted manuscript], 20th International Conference on Informatics in Economy (IE 2021), Bucharest, Romania

[2] Au. Buzdugan, A. Buzdugan - "Cyber Security in the Nuclear and Radiological Domain: Case Study of Republic of Moldova", 3rd International Conference on Nanotechnologies and Biomedical Engineering, IFMBE Proceedings 55, Springer Science+ Business Media Singapore 2016

[3] National Cyber Security Program of Republic of Moldova for 2016-2020, Government Decision 811 from 29.11.2015. Monitorul Oficial, no. 306-310 from 13.11.2015 (in Romanian)

[4] Minimum security requirements for ensuring cyber security of IT systems, hardware and software, Government Decision 201 from 28.03.2017. Monitorul Oficial, no. 109-118 (in Romanian)

[5] Au. Buzdugan, Integration of Cyber Security in Healthcare equipment, p. 153. In: 4-th International Conference on Nanotechnologies and Biomedical Engineering. Program and Abstract Book. Chisinau, Moldova, September 18-21, 2019. Published by Technical University of Moldova, Ed. Prof. Dr. Victor Sontea et al.

[6] Information Security Strategy of Republic of Moldova for 2019-2024, Parliament Decision 257 from 22.11.2018. Monitorul Oficial, no. 13-21 from 18-01-2019 (in Romanian)

[7] I. Bolun, D. Ciorba, A. Zgureanu, R. Bulai,, R. Calin, C. Bodoga. Informatics security assessment in the Republic of Moldova. In: Journal of Engineering Sciences. vol. XXVII, no. 4 (2020), pp. 103-119. ISSN 2587-3474. DOI 10.5281/zenodo.4288297

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.