гл. ас. д-р Недко Георгиев Тагарев

Резюмета на публикациите във връзка с участие в конкурс:

за заемане на академична длъжност „доцент“ по професионално направление 3.8. Икономика, научна специалност „Икономически анализ и управление на киберсигурността“, публикуван в Д.В., бр.3 от 10.01.2025 г., съгласно решение на АС № 6/11.12.2024 г.,

Съдържание

I.В.3. Тагарев, Н. (2021) Съвременни подходи при управлението на киберсигурността, Част I. Теоретични и методически основи, Изд: Авангард прима, С., ISBN – 978-61-239-546-9 (монография); ISBN – 978-619-239-547-6 (pdf), общо стр. 206.

Монографията "Съвременни подходи при управлението на киберсигурността" на Недко Тагарев разглежда ключовите аспекти на информационната и компютърната сигурност, като акцентира върху тяхната връзка с киберсигурността. В нея се анализират основните елементи на информационната сигурност – цялостност, наличност и поверителност на информацията, както и значението на критичните информационни активи и обектите от критичната инфраструктура. Представени са примери от реални инциденти, като атаките над Световния търговски център през 2001 г. и аварията в АЕЦ Фукушима през 2011 г.

Монографията също така изяснява връзката между информационната и компютърната сигурност, като разглежда ролята на ИТ сигурността при изграждането на архитектурата на информационната система. Направена е класификация на мерките и инструментите за сигурност, свързани с различните професионални направления в киберсигурността. Освен това, представена е оценката на зрелостта на системите за киберсигурност и въвеждането на интегрирани системи за управление на киберсигурността (ИСУК) базирани на ERP модели.

Допълнително, монографията разглежда контрола на достъпа, криптографията и архитектурата на киберсигурността, базирана на концепцията за защита в дълбочина. Анализирани са мрежовата сигурност, управлението на промените в информационната инфраструктура и системата за възстановяване при бедствия. Накрая, разгледани са

интернет безопасността и интернет сигурността, като са представени заплахите и инструментите за противодействие.

The monograph "Modern Approaches to Cybersecurity Management" by Nedko Tagarev examines the key aspects of information and computer security, emphasizing their relationship with cybersecurity. It analyzes the core elements of information security – integrity, availability, and confidentiality of information, as well as the significance of critical information assets and critical infrastructure objects. Real-world incidents, such as the attacks on the World Trade Center in 2001 and the Fukushima nuclear disaster in 2011, are presented as examples.

The monograph also clarifies the connection between information and computer security, exploring the role of IT security in building the architecture of information systems. A classification of security measures and tools related to various professional fields in cybersecurity is provided. Additionally, the assessment of the maturity of cybersecurity systems and the implementation of integrated cybersecurity management systems (ICMS) based on ERP models are discussed.

Furthermore, the monograph delves into access control, cryptography, and the architecture of cybersecurity, based on the concept of defense in depth. Network security, change management in information infrastructure, and disaster recovery systems are analyzed. Finally, internet safety and internet security are explored, with a focus on threats and countermeasures.

I.Г.4.Тагарев, Н. и Колектив, (2021) Икономически аспекти на модели за оценка на киберсигурност в умни градове, Издателски комплекс- УНСС, С., ISBN – 978-619-232-566-4, общо стр. 221
Глава „1.1. Общ базов модел на проекта ” стр. 18-20; Глава „ЧАСТ II МОДЕЛ ЗА СИГУРНОСТ В УМНИТЕ ГРАДОВЕ, БАЗИРАН НА РАЗШИРЕН МОДЕЛ НА УМНИ ГРАДОВЕ И ОСНОВНИ УЯЗВИМОСТИ В МОДУЛИТЕ ” стр. 43-72; Глава „ЧАСТ III КРИТИЧЕН ПОГЛЕД ВЪРХУ МЕТРИКИТЕ ЗА АНАЛИЗ НА КИБЕРСИГУРНОСТТА ”, Въведение , 3.1. „Добра“ срещу „лоша“ метрика , 3.2. Модел на метрика чрез „Пет показателя за сигурност, които трябва да се вземат предвид“ стр. 74-92; Глава „ЧАСТ IV ДИНАМИЧЕН БИЗНЕС МОДЕЛ НА СИГУРНОСТТА (BUSINESS MODEL FOR INFORMATION SECURITY (BMIS)) ЗА ИЗГРАЖДАНЕ НА СИГУРНОСТТА В УМНИТЕ ГРАДОВЕ. МОДЕЛ НА СИГУРНОСТТА IOACTIVE. МОДЕЛ ЗА ВРЪЗКА МЕЖДУ МОДУЛИТЕ НА УМНИЯ ГРАД И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ ”, Въведение , 4.1. Динамичен бизнес модел на сигурността, 4.2. Модел на сигурността IOActive, стр. 105-122; Глава „ЧАСТ V PRAGMATIC SECURITY – ПРАГМАТИЧЕН МОДЕЛ ЗА ОЦЕНКА НА КИБЕРСИГУРНОСТТА ” стр. 129-157; Глава „.ПРИЛОЖЕНИЕ 1 НАРЪЧНИК ЗА СОБСТВЕНИКА НА ИНФОРМАЦИОННИ АКТИВИ В УМНИЯ ГРАД ” стр. 187-202; Глава „ПРИЛОЖЕНИЕ 5 ОПРОСТЕН МОДЕЛ НА УМНИЯ ГРАД И ОСНОВНИ ЕЛЕМЕНТИ ” стр. 209-212, общо стр. 112

Публикацията разглежда дигитализацията на процесите на управление и прехода към умни градове, като подчертава необходимостта от модерни политики за сигурност и защита на данните. Той акцентира върху предизвикателствата за осигуряване на киберсигурност в умните градове, предвид експоненциалния растеж на устройствата, свързани с интернет, и нарастващата урбанизация. Текстът представя основен модел за умни градове, включващ модули като цифрова инфраструктура, киберсигурност, управление на града и икономически аспекти. Също така се разглеждат уязвимостите в различни модули на умните градове, като ИКТ инфраструктура, енергетика, управление на водите, управление на отпадъците, транспорт и здравеопазване. Документът предлага динамичен бизнес модел за информационна сигурност (BMIS) и модел за сигурност от IOActive, фокусирайки се върху жизнения цикъл на технологиите и важността на сигурността на доставчиците. Освен това се представя рамката за метрики за сигурност PRAGMATIC за оценка на ефективността на киберсигурността, като се подчертава необходимостта от точно събиране и докладване на данни за подобряване на мерките за сигурност. Заключението подчертава важността на непрекъснатия мониторинг,

редовните одити и интегрирането на мерките за сигурност в проектирането и експлоатацията на технологиите за умни градове.

The publication discusses the digitalization of management processes and the transition to smart cities, emphasizing the need for modern security policies and data protection. It highlights the challenges of ensuring cybersecurity in smart cities, given the exponential growth of internet-connected devices and the increasing urbanization. The text outlines a basic model for smart cities, including modules like digital infrastructure, cybersecurity, city management, and economic aspects. It also explores vulnerabilities in various smart city modules, such as ICT infrastructure, energy, water management, waste management, transportation, and healthcare. The document proposes a dynamic business model for information security (BMIS) and a security model by IOActive, focusing on the lifecycle of technology and the importance of vendor security. Additionally, it introduces the PRAGMATIC security metrics framework for evaluating cybersecurity effectiveness, emphasizing the need for accurate data collection and reporting to improve security measures. The conclusion stresses the importance of continuous monitoring, regular audits, and the integration of security measures into the design and operation of smart city technologies.

I.Г.6.1. Tagarev, N. (2019) "Role of Case Study Analyses in Education of Cybersecurity Management", The 13th International Multi-Conference on Society, Cybernetics and Informatics: IMSCI 2019, IInternational Institute of Informatics and Systemics, SBN: 978-1-950492-12-1 (Volume I), pp 61-64 (Scopus Indexed)

The problem that this article describes is the application of the knowledge that the trainees gain on case study analyses. This article discusses two approaches in the case study – by the algorithm and by heuristic analyses. The algorithm analyses allow a proactive approach to cybersecurity. The heuristic analyses allow on time proactive analyses of cyber-attacks. To make cybersecurity analyses it requires basic knowledge. The main sphere of knowledge for successful analyses is the knowledge of – Physical security, Information security, Computer security, IT security, Network security. We can provide this knowledge to the students through the cybersecurity course. To make a successful case study analyses course provides additional information for threats and risks, sources of the attack, the path of the attack and security measures and defence mechanisms. The article discusses cybersecurity problems related to management. This article relates to the scientific project “Economic aspects of models for the assessment of cybersecurity in smart cities” in the University of National and World Economy, Bulgaria.

Проблемът, който тази статия описва, е прилагането на знания, които обучаемите придобиват от анализи на казуси. Тази статията разглежда два подхода при анализа чрез казуси – от алгоритъм и чрез евристични анализи. Алгоритмичният анал позволява проактивен подход към киберсигурността. Евристиката позволява навременни проактивни анализи на кибератаки. За извършване на анализи на киберсигурността се изискват основни познания. Основната сфера на познание за успешни анализи са познания по – физическа сигурност, информационна сигурност, компютърна сигурност, ИТ сигурност, мрежова сигурност. Ние можем предоставим тези знания на учащите се чрез курсове по киберсигурност. За да се направи успешен анализ на казус, се анализира допълнителна информация за заплахи и рискове, източници на атаката, пътя на атаката и мерките за сигурност, и защита механизми. Статията разглежда проблемите на киберсигурността свързани с управлението. Тази статия е свързана с научен проект “Икономически аспекти на модели за оценка на киберсигурност в умните градове” в УНСС, България.

I.Г.6.2. Tagarev, N. (2019) Education in Management of Cybersecurity, 9th International Conference The Future of Education, (Florence, Italy, 27-28 June 2019); Filodiritto Publisher, ISBN 978-88-85813-45-8, ISSN 2384-9509, ISPN 939-1-00801418-4, DOI 10.26352/D627_2384-9509_2019, pp. 49-54 (Web of Science Indexed)

The problem presented in this article is the growing need for adequate and relevant cybersecurity education. Current trends placed cybersecurity and the upward trend in the use of smart technologies as the backbone of any business and management education. The education program and training have to cover the specific needs for management of cybersecurity. The program includes – computer security, network security, information technologies (IT) security, physical security, Internet security, security policy, management and business continuity. For training and analyses, we use cyber-attacks examples and real-life cases. As a milestone, the author, use the cybersecurity in objects of critical infrastructure. These objects require specific cybersecurity measures and defence mechanisms. This education of management of cybersecurity provides the often forgotten "horizontal approach" in cybersecurity. On the other side, in general, there is a need for adequate analyses – methods and methodology. The most frequently used, training methods are risk analyses, case studies and scenario analyses. Information security (IS) is part of cybersecurity education. Education in IS is based on most popular international standards such as ISO and NIST. Education relies on Information security management system (ISMS), cryptography, authentication methods and process analyses.

Проблемът, представен в тази статия, е нарастващата нужда от адекватно и подходящо образование по киберсигурност. Настоящите тенденции поставят киберсигурността и възходящата тенденция в използването на интелигентни технологии като гръбнака на всяко бизнес и управленско образование. Образователната програма и обучението трябва да покриват специфичните нужди за управление на киберсигурността. Програмата включва – компютърна сигурност, мрежова сигурност, сигурност на информационните технологии (ИТ), физическа сигурност, интернет сигурност, политика за сигурност, управление и непрекъснатост на бизнеса. За обучение и анализи използваме примери за кибератаки и случаи от реалния живот. Като крайъгълен камък авторът използва киберсигурността в обекти на критична инфраструктура. Тези обекти изискват специфични мерки за киберсигурност и защитни механизми. Това обучение по управление на киберсигурността осигурява често забравяния „хоризонтален подход" в киберсигурността. От друга страна, като цяло има нужда от адекватни анализи – методи и методология. Най-често използваните методи за обучение са анализи на риска, казуси

и анализи на сценарии. Информационната сигурност (ИС) е част от обучението по киберсигурност. Обучението по IS се основава на най-популярните международни стандарти като ISO и NIST. Обучението разчита на система за управление на информационната сигурност (ISMS), криптография, методи за удостоверяване и анализи на процеси.

I.Г.7.1. Tagarev, N. (2019) Defence Resource Planning in the Environment of Internet of Things, Research Papers Vol. 1/2019, Publishing Complex - UNWE, ISSN 0861-9344, pp. 169 – 197, Indexed: RePec,Google Scholar,ROAD,SIS,J-Gate, CEEOL

The problem of this article concern the lack of Defence Resource Planning (DRP) for the future environment of the Internet of Things(IoT). This paper shows the aspect in the DRP in Bulgaria and the probable change in the environment of IoT. The article provides data, cases and examples for comparison. The author shows DRP in Bulgaria in some details, that concerns the analyzed object. Study explains the connection between IoT and DRP. There are some basics about ERP. In this article finds a place the main difference between DRP and ERP. The paper acknowledges the threats and the change of the threats in the IoT. In this article are used several methods for quality analyses that include documentary, process, system case study and analogy methods. This article is one of the first with economic and management approach on this topic – smart devices (that communicate independently through IoT) and their significance for DRP. According to the hypotheses, the main author's conclusion is that the implementation of IoT in DRP will have a major impact on the US-centric military oriented states. Key words: Defence resource planning, Internet of Things, Threats, ERP.

Проблемът на тази статия се отнася до липсата на планиране на ресурсите за отбрана (DRP) за бъдещата среда на Интернет на нещата (IoT). Тази публикация показва аспекта на DRP в България и вероятната промяна в средата на IoT. Статията предоставя данни, случаи и примери за сравнение. Авторът показва ДРП в България в някои детайли, касаещи анализирания обект. Проучване обяснява връзката между IoT и DRP. Има някои основни неща за ERP. В тази статия намира място основната разлика между DRP и ERP. Документът признава заплахите и промяната на заплахите в IoT. В тази статия са използвани няколко метода за анализ на качеството, които включват документални, процесни, системни казуси и методи за аналогия. Тази статия е една от първите с икономически и управленски подход по тази тема – смарт устройства (които комуникират независимо чрез IoT) и тяхното значение за DRP. Според хипотезите основното заключение на автора е, че внедряването на IoT в DRP ще има голямо въздействие върху военно ориентираните към САЩ държави.

I.Г.7.2. Tagarev, N. (2019) Contraband and Counterfeit of Tobacco Products in Digital Age, Research Papers, Vol.4 2019, UNWE, Publishing complex – UNWE, Sofia, ISNN: (print) - 0861-9344, (online) – 2534-8957, pp. 243-251Indexed: RePec,Google Scholar,ROAD,SIS,J-Gate, CEEOL

CONTRABAND AND COUNTERFEIT of tobacco products results in a huge losses of revenue for government.Implementation of cyber/digital technologies in these activities is the problem ofthis article. These technologies change the scope of counteracting illegal activities.Object in this paper is Contraband & Counterfeit(C&C) of tobacco productsas the subject is implementation of digital technologies in these illegal activities. Methodology uses some cases as document analyses, comparative analyses and analyses of strong and week points. Results show the opportunities and the new reality of C&C of tobacco products.The scope of paper is limited to the basics of C&C of tobacco products. The material does not claim exhaustiveness. It lists factors and views that are often ignored in other researches.

КОНТРАБАНДАТА И ФАЛШИФИКАЦИЯТА на тютюневи изделия води до огромни загуби на приходи за правителството. Внедряването на кибер/цифрови технологии в тези дейности е проблемът разглеждан в тази статия. Тези технологии променят обхвата на противодействието на незаконните дейности. Обектът в тази статия е контрабанда и фалшифициране (C&C) на тютюневи изделия, като предметът е внедряването на цифрови технологии в тези незаконни дейности. Методологията използва някои случаи като анализи на документи, сравнителни анализи и анализи на силни и слаби страни. Резултатите показват възможностите и новата реалност на C&C на тютюневи изделия. Обхватът на статията е ограничен до основите на C&C на тютюневи изделия. Материалът не претендира за изчерпателност. Той изброява фактори и възгледи, които често се пренебрегват в други изследвания.

I.Г.7.3. Tagarev, N. (2016) Basics of management for cloud computing security, Inernational Conference on Application of Information and Communication Technology and Statistics in Economy and Education(ICAICTSEE), University of National and World Economy, Sofia, 2015, Publishing Complex - UNWE, AUGUST 15TH 2016, ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), стр. 457-462, Индексирано в: ProQuest

The main problem of this paper is acknowledgement of multiple level conflicts in security management in the clouds. The secondary problem that is observed is access and management of access in cloud environment. This article indicates connections between law, standards and policy. The main threats and defence mechanisms in cyber security related to the clouds are described. Thus this article represents a review of basics, which contains some analyses, and models for cloud security.

Основният проблем на тази статия е установяването на конфликти на множество нива в управлението на сигурността в облаците. Вторичният проблем, който се наблюдава, е достъпът и управлението на достъпа в облачна среда. Тази статия посочва връзките между закон, стандарти и политика. Описани са основните заплахи и защитни механизми в киберсигурността, свързани с облаците. Така тази статия представлява преглед на основите, който съдържа някои анализи и модели за сигурност в облака.

I.Г.7.4. Tagarev N. (2016) Basics of management for cloud computing security (part 2 physical security) , Inernational Conference on Application of Information and Communication Technology and Statistics in Economy and Education(ICAICTSEE), University of National and World Economy, Sofia, 2016, Publishing Complex – UNWE, Sofia, FEBRUARY 19TH 2019 , ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), pp. 285-294

This article is continuation of series of such for management of cyber security. The problem that is observed is management of physical security in cloud environment. This article indicates connections between law, standards and policy for physical security. The main threats and defence mechanisms in cyber security (physical aspects) related to the clouds are described. Thus this article represents a review of basics, which contains some analyses, and models for physical security.

Тази статия е продължение на серия от такива за управление на киберсигурността. Проблемът, който се наблюдава е управление на физическата сигурност в облачна среда. Тази статия посочва връзките между закона, стандартите и политиката за физическа сигурност. Описани са основните заплахи и защитни механизми в киберсигурността (физически аспекти), свързани с облаците. Така тази статия представлява преглед на основите на киберсигурността, които се представят чрез анализи и модели за физическа сигурност.

I.Г.7.5. Tagarev, N (2017) Cyber security – Seven basic principles for self-control in work environment Inernational Conference on Application of Information and Communication Technology and Statistics in Economy and Education(ICAICTSEE), University of National and World Economy, Publishing Complex – UNWE, Sofia, MAY 29TH 2020, ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), pp. 432 -439

This article is continuation of series of such for management of cyber security. The problem that is observed is management of behavior of the personal in his work environment. This article indicates connections between human attitude, standards and policy for self control in work environment. The main threats and defence mechanisms are indicated. Practical examples are given to show the fluent problems in different organizations. Thus this article represents a review of top basics priorities concerning the problems with the personal.

Тази статия е продължение на серия от такива за управление на киберсигурността. Проблемът, който се наблюдава е управление на поведението на личността в работната му среда. Тази статия посочва връзките между човешкото отношение, стандартите и политиката за самоконтрол в работната среда. Посочени са основните заплахи и защитни механизми. Дадени са практически примери, за да се покажат „размитите“ проблеми в различни организации. По този начин, тази статия представлява преглед на основните базови приоритети относно проблемите с личността.

I.Г.7.6. Nedko Tagarev, (2019). "Cyber Security Training Model (Nuclear Security)," Ikonomiceski i Sotsialni Alternativi, University of National and World Economy, Sofia, Bulgaria, issue 2, pages 46-55, June.

The problem addressed in this publication is the growing need for adequate and relevant cyber security training. Emphasis is placed on current trends in nuclear security and the upward trend in the use of nuclear technology. Specific examples of cyber-attacks over nuclear objects are mentioned. The Master's degree program "Economics of Defense and Security" with specialization "Nuclear Security" is briefly presented. It is important to note that currently the program quoted is the only one in the world. Specific examples of the areas where masters who have successfully completed the training program can also be found in the publication.

Проблемът, разгледан в тази публикация, е нарастващата нужда от адекватно и подходящо обучение по киберсигурност. Акцентът е поставен върху съвременните тенденции в ядрената сигурност и възходящата тенденция в използването на ядрени технологии. Посочват се конкретни примери за кибератаки срещу ядрени обекти. Накратко е представена магистърската програма „Икономика на отбраната и сигурността" със специализация „Ядрена сигурност". Важно е да се отбележи, че в момента цитираната програма е единствената в света. В публикацията могат да бъдат намерени и конкретни примери за областите, в които магистри, завършили успешно програмата за обучение.

I.Г.7.7. Тагарев, Н. (2018) Значение на ядрената сигурност през 21 век, Националната научна конференция на тема „ЕВРОПЕЙСКИЯТ СЪЮЗ, БЪЛГАРИЯ И ВОЙНИТЕ НА 21 ВЕК – ПОДЦЕНЕНИТЕ ЗАПЛАХИ" 18 декември 2017 г. София, Нова конферентна зала на СУ „Св. Кл. Охридски", Балкански институт за Стратегически прогнози и управление на риска София, 2018, ISBN- 9786199075722 стр.78-91

The problem addressed in this publication is the current issues of nuclear security. Often these problems are scratched at the expense of more popular, artificially created and popularized issues. The violation of nuclear security can affect everybody in society. The publication also shows how the Department of National and Regional Security at the University of National and World Economy is approached to solve these problems.

Проблемът, засегнат в тази публикация, е актуалната проблематика на ядрената сигурност. Често тези проблеми се задрасват за сметка на по-популярни, изкуствено създадени и популяризирани проблеми. Нарушаването на ядрената сигурност може да засегне всички в обществото. Изданието показва и как към катедра „Национална и регионална сигурност" в УНСС се подхожда към решаването на тези проблеми.

I.Г.7.8. Tagarev, N. (2019) Economic & Investment Perspectives in the Digital Society, Joint Research & Industrial Expert Forum "Future Digital Society Resilience in the New Digital Age“, 30.03-02.04.2018 Bulgarian Academy of Sciences, Softrade, Sofia, 2019,ISBN 978-954-334-221-1, pp. 35 – 52

This article observed the problem of future investments in digital society for the period 2018-2028. As some of the investments are pretty sure, others are discussible. This article considers several areas – warfare, big companies, smarttechnologies, cloud technologies, smartcities and education. Also the study provides some statistics, cases, examples, assumptions and predictions.. There are also list of military technologies of the future decade, future technologies of the big companies, alternative products for the mass usage and more.

Тази статия разглежда проблема с бъдещите инвестиции в цифровото общество за периода 2018-2028 г. Тъй като някои от инвестициите са доста сигурни, други подлежат на обсъждане. Тази статия разглежда няколко области – война, големи компании, интелигентни технологии, облачни технологии, умни градове и образование. Също така проучването предоставя някои статистики, казуси, примери, предположения и прогнози. Има и списък с военни технологии на бъдещото десетилетие, бъдещи технологии на големите компании, алтернативни продукти за масова употреба и др.

I.Г.7.9. Тагарев, Н. (2019) Обучение в областта на киберсигурността, сборник с доклади от Юбилейна научна конференция 25 години катедра ”Национална и регионална сигурност” на тема ”Обучението и изследванията по икономика на отбраната и сигурността – настояще и бъдеще”, Издателски комплекс- УНСС, ISBN 978-954-644-897-2, стр. 102-107.

Проблемът разглеждан в този доклад е процесът на обучение в областта на киберсигурността. За да се стигне до този процес на обучение се преминава през няколко дисциплини свързани с информационните технологии, които подготвят обучавания за адекватно и рационално възприятие на процеса на управление на сигурността на информацията. Без познаване на информационните технологии е невъзможно управлението на процеса на защита на информацията.

The problem addressed in this report is the process of training in the field of cybersecurity. To achieve this training process, several disciplines related to information technology are passed, which prepare the trainees for an adequate and rational perception of the process of information security management. Without knowledge of information technology, it is impossible to manage the process of information protection.

I.Г.7.10. Tagarev, N. (2019) Role of case study analyses in counteracting Contraband & Counterfeit of tobacco products, INTERNATIONAL CONFERENCE ON COMBATTING ILLICIT TOBACCO TRADE AND RELATED CRIMES, October 29-31th, 2018, UNWE, SOFIA, BULGARIA, Publishing Complex - UNWE, ISBN 978-619-232-220-5, pp.120-135

The problem of this article is the underestimation of using of a logical method for analyses as case studies in counteracting Contraband & Counterfeit of tobacco products. Generally, a case study is an incident that has happened regarding the problem. In Contraband & Counterfeit of tobacco products, there are thousands of such incidents per year. Such kind of cases can be found in every country across the world without exception. The case studies help the analyses to stay close to reality.

Проблемът на тази статия е подценяването на използването на логически метод за анализи като казуси в противодействието на контрабандата и фалшифицирането на тютюневи изделия. Като цяло казусът е инцидент, който се е случил по отношение на проблема. При контрабандата и фалшифицирането на тютюневи изделия има хиляди подобни инциденти годишно. Такива случаи могат да бъдат намерени във всяка страна по света без изключение. Казусите помагат анализите да останат близо до реалността.

I.Г.7.11. Tagarev, N. (2019) A Critical Look at the Metrics for Measuring the Effectiveness of a Cybersecurity System, 9 TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION ICAICTSEE – 2019 October 24 – 26th, University of National and World Economy Sofia, Bulgaria, PUBLISHING COMPLEX – UNWE, SOFIA, AUGUST 24TH, 2020, ISSN 2367-7635 (PRINT) ISSN 2367-7643 (ONLINE), pp 183-191, Индексирано в: ProQuest

This publication is part of the material of science project "Economical aspects of security in smart settlements", a University of National and World Economy №15/2018. In this publication are discussed the theoretical aspects of metrics and data that is collected for improving the effectiveness of cybersecurity system. The following text is based on the principle that the security goals have to be in line with business objectives. There are explained the requirements for good metrics, and the usefulness of other ones. There are shown some popular metrics that are not used very often for strengthening security.

Тази публикация е част от материала на научен проект „Икономически аспекти на сигурността в интелигентните селища", УНСС №15/2018. В тази публикация се обсъждат теоретичните аспекти на метриките и данните, които се събират за подобряване на ефективността на системата за киберсигурност. Текстът се основава на принципа, че целите за сигурност трябва да са в съответствие с бизнес целите. Там са обяснени изискванията за добри метрики и полезността на други. Показани са някои популярни показатели, които не се използват много често за укрепване на сигурността.

I.Г.7.12. Tagarev, N. (2020) Smart Cities in Japan, 8TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION (ICAICTSEE – 2018 OCTOBER 18 – 20TH, 2018, UNWE, SOFIA, BULGARIA, PUBLISHING COMPLEX – UNWE, SOFIA, ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), ISSUED FOR PUBLICATION: JUNE 30TH, 2020, pp. 267-275, Индексирано в: ProQuest

This publication is part of the material of science project "Economical aspects of security in smart settlements", a University of National and World Economy №15/2018. It concerns the smart cities in Japan. The goal of this study is to observe and gain knowledge about best practices in this country. In addition, there are examples of smart cities in Japan, their role and purposes. There are also explained the problem and the reasons for implementation of the smart technologies.

Тази публикация е част от материала на научен проект „Икономически аспекти на сигурността в интелигентните селища", УНСС №15/2018. Става въпрос за умните градове в Япония. Целта на това проучване е да се наблюдават и придобият знания за най-добрите практики в тази страна. Освен това има примери за интелигентни градове в Япония, тяхната роля и цели. Разясняват се проблема и причините за внедряването на смарт технологиите.

I.Г.7.13. Tagarev,N. (2020) Role of Cybersecurity Management Explained by a Single Case Study, XIII International & Interdisciplinary Scientific Conference VANGUARD SCIENTIFIC, INSTRUMENTS IN MANAGEMENT '2020, 29 July - 03 August 2020, ONLINE Sessions, UNWE, SOFIA, BULGARIA, Vol 16 (2020): Vanguard Scientiffic Instruments in Management ISSN-1314-0582

In this article is discussed the misunderstanding of the need of cybersecurity managers. The main role of managers is to align the security goals to business goals of the organisation. We can see this role by the change of assets of the information security and the assets of the organisation by a case study through the process analyses. This article proposes a solution with the implementation of project management. We have to look to the cybersecurity as a project, with its programs and packages. The products provided by this approach are management and technological products.

В тази статия се дискутира неразбирането на необходимостта от мениджъри по киберсигурност. Основната роля на мениджърите е да съгласуват целите за сигурност с бизнес целите на организацията. Можем да видим тази роля чрез промяната на активите на информационната сигурност и активите на организацията, чрез анализ чрез казуси и чрез анализ на процеси. Тази статия предлага решение с внедряване на управление на проекти. Трябва да гледаме на киберсигурността като на проект, с неговите програми и пакети. Продуктите, предоставени от този подход, са управленски и технологични продукти.

I.Г.7.14. Tagarev, N. (2020) Minimum Requirements for IDS Based on “Cost-Benefit” Approach, 10 TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION ICAICTSEE – 2020 November 27 – 28th, 2020, PUBLISHING COMPLEX – UNWE, SOFIA, AUGUST 21ST, 2021 BULGARIA ISSN 2367-7635 (PRINT) ISSN 2367-7643 (ONLINE), pp 363-375

The problem addressed in this article is maximizing the effect of the Intrusion Detection System (IDS) with limited resources allocated by the cybersecurity organization. The object of the article is the IDS models, and the subject is the minimum requirements for the system. The methodology used to assess these requirements is "costbenefit" analyses. The analysis compared IDS models, and case studies were applied to achieve an economic justification for the significance of the problem. The minimum requirements, i.e. the benefits are seen as "technical or technological" features that provide a sustainable product - cybersecurity. Concerning costs, different approaches have been proposed for their evaluation. The publication indirectly affects the return on investment in cybersecurity.

Проблемът, разгледан в тази статия, е максимизирането на ефекта от системата за откриване на проникване (IDS) с ограничени ресурси, разпределени от организацията за киберсигурност. Обект на статията са IDS моделите, а предмет минималните изисквания към системата. Методологията, използвана за оценка на тези изисквания, е анализ на "разходи-ползи". Анализът сравнява IDS модели и са приложени казуси, за да се постигне икономическа обосновка за значимостта на проблема. Минималните изисквания, т.е. ползите, се разглеждат като „технически или технологични“ характеристики, които осигуряват устойчив продукт – киберсигурност. По отношение на разходите са предложени различни подходи за тяхната оценка. Публикацията косвено влияе върху възвръщаемостта на инвестициите в киберсигурност.

I.Г.7.15. Tagarev, N. (2021) Manageable Mature Maturity Model(M-MMM) for Evaluation of Cybersecurity, 11 TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION ICAICTSEE – 2021 November 27 – 28th, 2020, PUBLISHING COMPLEX – UNWE, SOFIA, BULGARIA, SEPTEMBER 15TH, 2023 , ISSN 2367-7635 (PRINT) IS SN 2367-7643 (ONLINE) стр. 344-362

The problem addressed in this article is maximizing the effect of the cybersecurity management in organizations. The object of the article is the models for Mature Maturity Model (MMM). The methodology is based on implementation and analyses in the Mature Maturity Model (MMM) that is used in project management. According to this, we can look at cybersecurity as a project with its economic and technical aspects(soft and hard). In this article will be found previous applications and theoretical principles of MMM. Proposed Manageable Mature Maturity Model (M-MMM) is based on data, evaluation and quantity metrics. The M-MMM can provide method for distribution/allocation of the resources for cybersecurity with measurable results. In addition, we will try to provide some experiments on the application of the methodology and without it. These examples are based on problems that we can met in management of cybersecurity.

Проблемът, разгледан в тази статия, е максимизирането на ефекта от управлението на киберсигурността в организациите. Обект на статията са моделите за модел на зрялост (MMM). Методологията се основава на внедряване и анализи в модела за зрялост (MMM), който се използва в управлението на проекти. Според това можем да разглеждаме киберсигурността като проект с неговите икономически и технически аспекти (меки и твърди). В тази статия ще намерите предишни приложения и теоретични принципи на MMM. Предложеният управляем зрял модел (M-MMM) се основава на данни, оценка и количествени показатели. M-MMM може да осигури метод за разпределение/разпределение на ресурсите за киберсигурност с измерими резултати. Освен това ще се опитаме да предоставим някои експерименти за прилагането на методологията и без нея. Тези примери се основават на проблеми, които можем да срещнем при управлението на киберсигурността.

I.Г.7.16. Tagarev, N. (2024) Application of Regression Analyses and Marginal Analyses for Assessing the Effectiveness of COVID-19 Pandemic Mitigation Measures in Bulgaria, International Journal of Science and Research (IJSR), Volume 13 Issue 1, January 2024p ISSN (Online): 2319-7064 pp. 1521-1527

Regression analysis is a popular method for determining multiple variables' relationships. We can use it to quantify this dependence between economic measures and the harmful effects of the COVID-19 pandemic. In addition, we can predict change in future periods. The problem with applying the method is the development of hypotheses about the dependence and accuracy of the data. This problem is discussed in this study, as one of the examples we have given is the "real" level of unemployment and the fastened digitalisation of society. On the other hand, we have the definition of the positive and negative effects of dependent variables on measures that are independent variables. We apply marginal analysis to measure the positive effect and determine when a measure is ineffective. The aim and logic of this study are to reduce the "falsification" of the scientific product so that it is based on objective facts and events and not on the feelings and interpretations of the researcher.

Регресионният анализ е популярен метод за определяне на връзките между множество променливи. Можем да го използваме, за да определим количествено тази зависимост между икономическите мерки и вредните ефекти от пандемията COVID-19. Освен това можем да предвидим промяна в бъдещи периоди. Проблемът при прилагането на метода е разработването на хипотези за зависимостта и точността на данните. Този проблем се обсъжда в това изследване, като един от примерите, които дадохме, е „реалното“ ниво на безработица и ускоряващата се дигитализация на обществото. От друга страна, имаме определението за положителните и отрицателните ефекти на зависимите променливи върху мерките, които са независими променливи. Ние прилагаме маргинален анализ, за да измерим положителния ефект и да определим кога дадена мярка е неефективна. Целта и логиката на това изследване е да се намали "фалшификацията" на научния продукт, така че той да се основава на обективни факти и събития, а не на чувствата и интерпретациите на изследователя.

I.Г.7.17. Tagarev, N. (2024) Implementation of Blockchain in ERP for Cybersecurity In pp.ternational Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 pp. 1737-1741

Blockchain technology has a role beyond cryptocurrency. The ERP also has a role beyond financial and accounting analyses. Blockchain is a key technology of the Fourth Industrial Revolution, removing the boundaries between physical and digital spaces. It creates new innovative opportunities and disrupts existing businesses by enabling decentralized digital transformation. This article examines ERP and blockchain technologies, as well as their combination. The added value that both technologies bring to cyber security and the possibility to increase this value by adding an additional effect is discussed. Considered as an example of contributing to the effect, the process of checking for vulnerabilities.

Блокчейн технологията има роля отвъд криптовалутата. ERP също има роля извън финансовите и счетоводни анализи. Блокчейн е ключова технология на Четвъртата индустриална революция, премахваща границите между физическите и цифровите пространства. Той създава нови иновативни възможности и „нарушава“ съществуващите бизнес практики, като позволява децентрализирана цифрова трансформация. Тази статия разглежда ERP и блокчейн технологиите, както и тяхната комбинация. Обсъжда се добавената стойност, която двете технологии носят към киберсигурността и възможността тази стойност да се увеличи чрез добавяне на допълнителен ефект. Разглеждан като пример за принос към ефекта, процесът на проверка за уязвимости.

I.Г.7.18. Georgi Pavlov, Nedko Tagarev, (2024) Enhansing Cybersecurity trough the Integration of Geographic Information System Technologies Iternational Journal of Science and Research (IJSR) Volume 13 Issue 8, August 2024 ISSN (Online): 2319-7064 pp.591-599

This article explores the integration of Geographic Information Systems GIS with cybersecurity to enhance threat analysis, incident response, and overall network security. Cybersecurity systems can achieve higher efficiency and effectiveness by leveraging GIS data for spatial analysis and real - time monitoring. Integrating SCADA systems further enables comprehensive monitoring and management of external and internal environments. This study also discusses the application of machine learning in automating data analysis for cybersecurity, providing a cyclical improvement in security processes. The article analyses the effect of cybersecurity through GIS technologies.

Тази статия изследва интегрирането на GIS на географските информационни системи с киберсигурността за подобряване на анализа на заплахите, реакцията при инциденти и цялостната мрежова сигурност. Системите за киберсигурност могат да постигнат по-висока ефективност и ефективност чрез използване на ГИС данни за пространствен анализ и наблюдение в реално време. Интегрирането на SCADA системи допълнително позволява цялостен мониторинг и управление на външната и вътрешната среда. Това проучване също така обсъжда приложението на машинното обучение при автоматизиране на анализа на данни за киберсигурността, осигурявайки циклично подобрение в процесите на сигурност. Статията анализира ефекта от киберсигурността чрез ГИС технологиите.

I.Г.7.19. Tagarev, N. (2024), APPLICATION OF CYBER INTELLIGENCE FOR SECURITY OPERATION CENTER, 13TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION (ICAICTSEE – 2023), DECEMBER 15-16TH, 2023, UNWE, SOFIA, BULGARIA ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE) PUBLISHING COMPLEX – UNWE, SOFIA, BULGARIA, ISSUED FOR PUBLICATION: OCTOBER 1ST, 2024 pp. 57-65

Ensuring practical cyber intelligence for a Security Operation Center (SOC) involves collecting, analyzing, and utilizing information about cyber threats to enhance the organization's security posture. This encompasses the gathering and analysis of data on potential and active cyber threats, including Indicators of Compromise (IoCs)" which refer to signs that a security breach may have occurred, while "Tactics, Techniques, and Procedures (TTPs)" refer to the methods and behaviours used by an attacker to carry out a cyber attack and utilized by threat actors. Additionally, it entails the use of advanced tools to monitor networks, systems, and applications for suspicious activities, such as the utilization of Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). Furthermore, it involves developing and implementing plans to respond to security incidents, including identifying, containing, eradicating, and recovering from cyber-attacks. Regularly scanning systems for vulnerabilities and applying patches or mitigations to reduce the attack surface are also crucial components of cyber intelligence in the SOC. Lastly, monitoring and analyzing user and entity behaviour to detect anomalies that could indicate insider threats or compromised accounts is another significant aspect of effectively integrating cyber intelligence into SOC operations.

Осигуряването на практическо киберразузнаване за Център за операции по сигурността (SOC) включва събиране, анализиране и използване на информация за кибернетични заплахи за подобряване на състоянието на сигурността на организацията. Това включва събиране и анализ на данни за потенциални и активни кибернетични заплахи, включително Индикатори за компрометиране (IoCs), които се отнасят до признаци, че може да е настъпил пробив в сигурността, докато "Тактики, техники и процедури (TTP)" се отнасят до методите и поведенията, използвани от нападателя за извършване на кибернетична атака и използвани от участниците в заплахата. Освен това, това включва използването на усъвършенствани инструменти за наблюдение на мрежи, системи и приложения за подозрителни дейности, като използването на системи за сигурност и управление на събития (SIEM), системи за откриване на проникванията (IDS) и системи за предотвратяване на проникване (IPS), освен това включва разработване и прилагане на планове за реагиране на инциденти със сигурността, включително идентифициране,

ограничаване, изкореняване и възстановяване от кибератаки и прилагането на „пачове“ или смекчаващи мерки за намаляване на повърхността на атаката, които също са ключови компоненти на киберразузнаването в SOC. И накрая, наблюдението и анализирането на поведението на потребителите и субектите за откриване на аномалии, които биха могли да показват вътрешни заплахи или компрометирани акаунти, е друг важен аспект на ефективното интегриране на киберразузнаването в операциите на SOC.

I.Г.7.20. Tagarev, N. (2024), GAP ANALYSES IN CYBERSECURITY, APPLICATION OF CYBER INTELLIGENCE FOR SECURITY OPERATION CENTER, 13TH INTERNATIONAL CONFERENCE ON APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY AND STATISTICS IN ECONOMY AND EDUCATION (ICAICTSEE – 2023), DECEMBER 15-16TH, 2023, UNWE, SOFIA, BULGARIA ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), PUBLISHING COMPLEX – UNWE, SOFIA, BULGARIA, ISSUED FOR PUBLICATION: OCTOBER 1ST, 2024 pp. 66-72

This article, part of a series on cybersecurity management, addresses the challenge of managing Cybersecurity as a process and a product. It explores the connections between the current situation, standards, and policies for self-control in the cybersecurity work environment while also highlighting the concept of GAP analyses for managing the main threats and defence mechanisms. The article provides practical example that demonstrate the real-world application of these concepts in different organizations, thereby assuring readers of the practicality of the solutions presented. GAP analysis is a commonly employed methodology across diverse fields including business, education, and project management. It plays a crucial role in assessing the disparity between the present state of affairs and the intended objectives. The acronym "GAP" encompasses "Goal, Achievement, and Performance," representing the fundamental elements involved in the analysis process.

Тази статия, част от поредица за управление на киберсигурността, разглежда предизвикателството на управлението на киберсигурността като процес и продукт. Тя изследва връзките между текущата ситуация, стандартите и политиките за самоконтрол в работната среда за киберсигурност, като същевременно подчертава концепцията за GAP анализи за управление на основните заплахи и защитни механизми. Статията предоставя практически пример, който демонстрира реалното приложение на тези концепции в различни организации, като по този начин уверява читателите в практичността на представените решения. GAP анализът е често използвана методология в различни области, включително бизнес, образование и управление на проекти. Той играе решаваща роля при оценката на несъответствието между настоящото състояние на нещата и планираните цели. Акронимът "GAP" обхваща "цел, постижение и представяне", представляващи основните елементи, включени в процеса на анализ.

I.Г.10.1. Н. Тагарев (2017) ”Съвременен инструментариум за измерване на сигурността” - УНСС 2013-2015г.НИД НП 1-9/2014, колективна монография, Издателски комплекс-УНСС, С., ISBN 978-954-644-945-0
Глава „Съвременни модел за оценка на системата за кибер сигурност”, стр. 92 – 108

ценката на информационната сигурност и киберсигурността се прави върху основата на стандарти, които дават процеси, информацията и източниците на информация, необходими за определянето й. Съществуват две основни групи стандарти ISO 27000 и NIST Special report 800:... ISO 27000 задава процедурите и процеса, както и процедурата за извършване на анализ на риска. NIST 800:... задава конкретни технически параметри за информационната и киберсигурността. Основната методика за оценяване на информационните системи се задава от модела на COBIT. За да може да се оцени киберсигурността, е необходимо модификация и комбинация от споменатите модели, както и добавяне на методики за управление и икономически анализ. В областта на киберсигурността основната цел е предотвратяването на загубата на въведената информация и наличието на "поддържаща система" (back-up).

The assessment of information security and cybersecurity is made on the basis of standards that provide processes, information and sources of information necessary for its determination. There are two main groups of standards ISO 27000 and NIST Special report 800:... ISO 27000 sets the procedures and process, as well as the procedure for performing risk analysis. NIST 800:... sets specific technical parameters for information and cybersecurity. The main methodology for assessing information systems is set by the COBIT model. In order to assess cybersecurity, it is necessary to modify and combine the mentioned models, as well as add management and economic analysis methodologies. In the field of cybersecurity, the main goal is to prevent the loss of the entered information and the presence of a "back-up system".

I.Г.10.2 Н. Тагарев, Глава „Свлачища”, параграф: „Географски физически модели на бедствия с възможности за използване на ГИС технологии” стр.74-84; глава Димитров, Д., Н. Тагарев,Е. Богомилова, „Подходи за определяне на икономическата оценка при бедствия и аварии” стр. стр.113-144 (2019) Икономическа оценка на защитата при бедствия и аварии, Издателски комплекс- УНСС, , ISBN 978-619-232-173-4

Четвъртата глава на Публикацията "Географски физически модели на бедствия с възможности за използване на ГИС технологии" разглежда различни природни бедствия, като свлачища, земетресения и горски пожари, и възможностите за тяхното картографиране и икономическа оценка с помощта на географски информационни системи (ГИС). Параграфът описва процесите на свлачищата, причините за тяхното възникване и методите за тяхното изследване и класификация. Също така се разглеждат гравитационните процеси, които водят до срутвания и преместване на скални и земни маси. В частта, посветена на горските пожари, се анализират причините за тяхното възникване, икономическите последици и възможностите за моделиране на разпространението на пожарите с помощта на ГИС. Документът подчертава важността на ГИС технологиите за прогнозиране и оценка на щетите от природни бедствия, което може да помогне за по-ефективно управление на рисковете и намаляване на икономическите загуби.

The fourth chapter of the publication "Geographical Physical Models of Disasters with Opportunities for Using GIS Technologies" examines various natural disasters, such as landslides, earthquakes, and forest fires, and the possibilities for their mapping and economic assessment using Geographic Information Systems (GIS). The document describes the processes of landslides, the causes of their occurrence, and the methods for their study and classification. Gravitational processes leading to rockfalls and the displacement of rock and soil masses are also discussed. In the section dedicated to forest fires, the causes of their occurrence, economic consequences, and the possibilities for modeling fire spread using GIS are analyzed. The document emphasizes the importance of GIS technologies for predicting and assessing the damage caused by natural disasters, which can help in more effective risk management and reduction of economic losses.

В пети раздел е представен модел за разходен анализ, внедрен в софтуера GRASS GIS, който се използва в рамките на проекта. Моделът включва основните методи за анализ, като параметричен метод, инженерен разходен анализ и ABC анализ, които позволяват стандартизиране, сравнение и позоваване на исторически опит от други проекти.

Разходите по жизнения цикъл на проекта са разделени на шест основни фази: планиране, превенция, смекчаване, готовност, реакция и възстановяване.
Моделът включва и алтернативни елементи на разходите, базирани на процесен анализ и исторически данни, като разходите са категоризирани според вида на щетите – физически, екологични, социални и икономически. Представен е и модел на пълните разходи за различни алтернативи за период от 15 години, като разходите са разпределени по етапите на жизнения цикъл.
Освен това, разгледани са разходите по елементи, като планиране, превенция, смекчаване, готовност, реакция и възстановяване, с детайлно описание на всяка категория. Моделът включва и класификация на земните класове според номенклатурата на „Корина“, която се използва за автоматично изчисление на щетите и разходите върху засегнатите територии.

Fifth section presents a cost analysis model implemented in the GRASS GIS software, used within the project. The model includes key analysis methods such as parametric analysis, engineering cost analysis, and ABC analysis, which allow for standardization, comparison, and reference to historical experience from other projects. The costs over the project's lifecycle are divided into six main phases: planning, prevention, mitigation, preparedness, response, and recovery.
The model also includes alternative cost elements based on process analysis and historical data, with costs categorized according to the type of damage – physical, environmental, social, and economic. A model of total costs for various alternatives over a 15-year period is presented, with costs distributed across the lifecycle phases.
Additionally, the costs by elements are examined, including planning, prevention, mitigation, preparedness, response, and recovery, with a detailed description of each category. The model also incorporates a classification of land cover types according to the CORINE nomenclature, used for automatic calculation of damages and costs on affected areas.

I.Г.10.3. Н. Тагарев,(2022)”Моделиране, анализ и оптимизиране на Социално-икономическите мерки за намаляване на негативните последствия от пандемията Covid-19” Глава: Мерки свързани с дигиталната икономика стр. 27-42 Издателски комплекс-УНСС, С., ISBN978-619-239-875-0

Документът разглежда дигиталните мерки в България, ускорени от COVID-19, и бъдещите планове за цифрова трансформация. Създадена е Национална електронна библиотека за учители, а държавата е финансирала закупуването на лаптопи за ученици и учители. Въведена е електронна рецепта, но с ограничено приложение, и разработена платформа за регистрация за ваксинация. В рамките на Плана за възстановяване и устойчивост са предвидени 1,6 млрд. евро за цифровизация в сектори като енергетика, здравеопазване и транспорт. Въпреки инвестициите, България изостава по DESI индекса спрямо ЕС, особено в свързаността, човешкия капитал и индустриалната цифровизация. Основният проблем е фокусът върху администрацията, а не върху бизнеса и производството. Швеция предлага добри примери с използването на ГИС технологии за анализ на веригите за доставки и онлайн платформи за бизнес развитие. Докладът критикува методологията на ЕС за измерване на дигиталния напредък, която не отчита производствени технологии. Предлага се използване на размити модели (Fuzzy Cognitive Maps) за по-прецизен анализ. Ключови индикатори са скоростта на дигитализация, автоматизацията, енергийното потребление и устойчивостта на технологиите. Ефективността на мерките ще може да се оцени по-реалистично след 2025 г. Пандемията ускори някои процеси, но дигитализацията остава предизвикателство. Инвестициите трябва да бъдат насочени не само към администрацията, но и към бизнеса и индустрията. Без промяна в подхода България рискува да остане изоставаща в цифровата икономика.

The document examines digital measures in Bulgaria, accelerated by COVID-19, and future plans for digital transformation. A National Electronic Library for teachers was created, and the government funded the purchase of laptops for students and teachers. An electronic prescription system was introduced, though with limited application, and a vaccination registration platform was developed. Under the Recovery and Resilience Plan, €1.6 billion is allocated for digitalization in sectors such as energy, healthcare, and transport. Despite investments, Bulgaria lags behind the EU in the DESI index, particularly in connectivity, human capital, and industrial digitalization. The main issue is the focus on administration rather than business and production. Sweden offers good examples, such as using GIS technologies for supply chain analysis and online platforms for business development. The report criticizes the EU methodology for measuring digital progress, which does not account for production technologies. It suggests using fuzzy models (Fuzzy Cognitive Maps) for a more precise

analysis. Key indicators include digitalization speed, automation, energy consumption, and technology sustainability. The effectiveness of these measures can be realistically assessed only after 2025. While the pandemic accelerated some processes, digitalization remains a challenge. Investments should target not only administration but also business and industry. Without a change in approach, Bulgaria risks remaining behind in the digital economy.

I.Г.10.4. Н. Тагарев (2021) Глава „Мрежова и информационна сигурност в електронното управление (обща част)” стр. 283-340; Цакова, И., М. Хубенова, К. Георгиева, Т. Тимева, Н. Тагарев (2021) „Всичко за електронното управление в едно практическо ръководство“ Изд: Парадигма, София, ISBN 9789543264544 Глава „Мрежова и информационна сигурност в електронното управление (обща част)” стр. 283-340;

Киберсигурността е от съществено значение за критичните обекти, тъй като повечето контролиращи активи са цифрови. Проблемът, който е определен по този начин, се състои в огромния обхват на управлението на киберсигурността, който често се пренебрегва за сметка на инструментите за сигурност, които могат да бъдат софтуерно или хардуерно решение за някакъв проблем.

Предметът на тази част от материала е киберсигурността (компютърна и мрежова) в сферата на публичните обекти. Киберсигурността е съществена част от административните обекти, тъй като цифровата инфраструктура за управлението на държавата е критична инфраструктура. Основната тема е политиката за киберсигурност, която включва всички изисквания за функциониране на тази инфраструктура, като третира и защитните механизми като софтуер и хардуер.

Cybersecurity is essential for critical facilities, as most controlling assets are digital. The problem, as defined in this context, lies in the vast scope of cybersecurity management, which is often overlooked in favor of security tools that may be software or hardware solutions to specific issues.

This section of the material focuses on cybersecurity (both computer and network security) in the field of public facilities. Cybersecurity is a crucial aspect of administrative entities since the digital infrastructure used for state governance is considered critical infrastructure. The main topic is cybersecurity policy, which encompasses all requirements for the functioning of this infrastructure while also addressing protective mechanisms such as software and hardware solutions.

I.Г.10.5. Н. Тагарев (2021) Глава „Осигуряване на информационна и мрежова сигурност съгласно Наредба за минималните изисквания за информационна и мрежова сигурност" стр. 622-656 Цакова, И., М. Хубенова, К. Георгиева, Т. Тимева, Н. Тагарев (2021) „Всичко за електронното управление в едно практическо ръководство" Изд: Парадигма, София, ISBN 9789543264544

Компютърната и информационната сигурност са скъпо и трудоемко начинание, с което администрацията се сблъска след сериозни проблеми в областта на киберсигурността през последните две години. Киберсигурността изисква финансови инвестиции, които зависят от размера и структурата на организацията. За изграждането на защитните инструменти в организацията се изискват задълбочени технически познания по отношение на архитектурата на компютърните мрежи. Проблемът с внедряването на минималните изисквания за компютърна и мрежова сигурност се състои обикновено в отсъствието на финансови средства или наличие на подготвени служители, които да са добре запознати с особеностите и рисковете в киберсигурността.

Целта на настоящата част е да подпомогне процеса на внедряване и изпълнение на изискванията на Наредбата за минимални изисквания за информационната и мрежовата сигурност, приета с ПМС № 186 от 19.07.2019 г., в сила от 26.07.2019 г. (Наредбата)1 . Този процес е изключително комплексен поради неговата мултидисциплинарност.

Материалът е структуриран в съответствие със структурата на разглеждания нормативен акт, като нормативните текстове са разяснени накратко с оглед на тяхното разбиране и прилагане.

Computer and information security are expensive and labor-intensive endeavors that the administration has faced following serious cybersecurity issues over the past two years. Cybersecurity requires financial investments, which depend on the size and structure of the organization. Building protective tools within an organization requires in-depth technical knowledge of computer network architecture. The challenge in implementing the minimum requirements for computer and network security often stems from a lack of financial resources or the absence of adequately trained personnel familiar with cybersecurity risks and specifics.

The aim of this section is to support the process of implementing and complying with the requirements of the Regulation on Minimum Requirements for Information and Network Security, adopted by Council of Ministers Decree No. 186 of July 19, 2019, in force since July 26, 2019. This process is highly complex due to its multidisciplinary nature.

The material is structured in accordance with the structure of the regulatory act under review, with the legal provisions briefly explained to facilitate their understanding and application.

II.Ж.26. Nedko Tagarev, (2022). "Economic Aspects of Models for Assessing Cybersecurity in Smart Cities," Ikonomiceski i Sotsialni Alternativi, University of National and World Economy, Sofia, Bulgaria, issue 2, pages 44-61, June.

Тази публикация е резултат от УНИВЕРСИТЕТКИ ПРОЕКТ ЗА ИЗСЛЕДВАНИЯ №NID NI-15/2018 „Икономически аспекти на модели за оценка на киберсигурността в интелигентните градове“. Изследването представя е анализира моделите на интелигентните градове, подходите към строителството и ги анализира и сравнява. Показан е модел за киберсигурност на интелигентните градове. Този модел е изграден върху удължен модел на интелигентни градове. Подходът към модела се основава на специфичните уязвимости и заплахи за всеки от модулите. На този етап от изследването започва изграждането на връзката на икономическите ефекти върху киберсигурността. Тази връзка показва, че инвестирането в киберсигурност ускорява дигитализацията. Следващата стъпка от изследването прилага критичен анализ на показателите, традиционно използвани за оценка на киберсигурността. Предлагат се критерии за избор на „добри показатели“. Моделите за изграждане на киберсигурност са сравнени и са показани техните силни и слаби страни. Тези модели могат да се прилагат в комбинация с управление на проекти за модел на киберсигурност или методология за създаване на модел за икономическа оценка на киберсигурността. В подкрепа на модела на икономическа оценка се прилага прагматичната методология за оценка на сигурността. Информацията от различни случаи беше използвана в подкрепа на проекта и беше проведено проучване с потребителите на продукта за киберсигурност.

This publication is the result of UNIVERSITY RESEARCH PROJECT N–NID NI-15/2018 „Economic aspects of models for assessing cybersecurity in smart cities“. The study presents, analyzes and compares the models of smart cities and the approaches to construction. A model for cybersecurity of smart cities is also shown. This model is built on an extended model of smart cities. The approach to the model is based on the specific vulnerabilities and threats for each of the modules. At this stage of the study, the link between the economic effects on cybersecurity begins. This link shows that investing in cybersecurity is accelerating digitalization. The next step of the study applies a critical analysis of the indicators traditionally used to assess cybersecurity. Criteria for selecting â€œgood indicatorsâ€ are proposed. The models for building cybersecurity are compared and their strengths and weaknesses are shown. These models can be applied in combination with project management for a cybersecurity model or a methodology for creating a model for economic assessment of cybersecurity. In support of the economic assessment model, the pragmatic security

assessment methodology is applied. Information from various cases was used to support the project and a survey was conducted with users of the cybersecurity product.

II.3.26. Тагарев, Н. Учебнопомагало за изработване на курсова работа по методът «Разходи-Ползи» и анализ на казус по събитие по дисциплините «Икономически анализ в отбраната и сигурността» и «Икономически анализ във вътрешния ред и сигурност», Авангард Прима, София, 2024 г, ISBN 978-619-279-018-9 мека корица, ISBN 978-619-279-019-6 pdf

Актуалността на метода „разходи-ползи“ произтича от функцията му на инструмент за вземане на решения, използван в различни области, като отбрана и сигурност, икономика, бизнес, публична политика и управление на проекти. Той включва сравняване на разходите за различни алтернативи решение или проект с очакваните ползи. Методът на разходите и ползите е много уместен, тъй като осигурява систематична и количествена рамка за вземане на решения.

Анализът на разходите и ползите е широко използван метод в организации, правителства и предприятия за вземане на информирани решения. Той помага за ефективното разпределяне на ресурсите чрез идентифициране на проекти или дейности, които предлагат най-висока нетна полза. Този метод е от решаващо значение за субекти с ограничени ресурси, за да се гарантира, че инвестициите са насочени към инициативи, които доставят най-значимата обща стойност.

Анализът на разходите и ползите се използва и за оценка на проекта, където лицата, вземащи решения, претеглят очакваните ползи спрямо прогнозираните разходи, за да оценят жизнеспособността на проекта. Правителствата използват този метод, за да оценят въздействието на предложените политики, като вземат предвид краткосрочните и дългосрочните разходи и ползи.

Този метод може също да помогне при идентифицирането и оценката на рисковете, свързани с решение или проект, чрез количествено определяне на разходите и ползите. Той осигурява прозрачен и систематичен подход към вземането на решения, позволявайки на заинтересованите страни да разберат обосновката зад дадено решение и да приоритизират множество проекти или инициативи въз основа на общия им принос към целите на организацията.

Освен това анализът на разходите и ползите подобрява отчетността, като предоставя основа за оценка на успеха или неуспеха на решение, или проект. Внедряването позволява на организациите да сравняват действителните резултати с първоначалните прогнози, улеснявайки непрекъснатото подобрение.

Вземащите решения могат също така да разширят метода разходи-ползи, за да включат екологични и социални фактори извън финансовите съображения, допринасяйки за по-всеобхватно вземане на решения.

Въпреки определени ограничения, като например предизвикателства при количественото определяне на определени нематериални фактори, субективни оценки и потенциални отклонения, методът на разходите и ползите остава незаменим инструмент за насочване на решения и разпределение на ресурси в широк диапазон.

Целта на учебното помагало по икономически анализ(„разходи-ползи“) е предоставянето на инструмент и ресурс, предназначен да помогне на студентите да научат, разберат и запомнят информацията, която е свързана с приложението на методиката. По този начин може да се подобрят ефективността на учебните сесии(лекции и упражнения) и цялостното академично представяне на студентите.

Задачите, които си поставя учебното помагало по отношение на учебния процес:

1. Улесняване на разбирането на методиката за икономически анализ в отбраната и сигурността. Това се постига чрез опростяване на сложни концепции, за да се раздели информацията на по-малки части и да осигури визуални представяния за подпомагане на разбирането.

2. Организиране на информацията като се спомага за организирането на данните и информацията по структуриран начин, което улеснява учащите да схванат връзките между различни теми и да идентифицират ключови елементи.

3. Насърчаване на активното разбиране и използване на материала, чрез водене на бележки, планове за приложение на методите и интерактивни упражнения, които насърчават обучаемите да участват активно в учебния процес, засилвайки разбирането чрез активно ангажиране.

4. Учебното помагало може да помогне при управлението на времето, като подпомогне учащите да приоритизират задачите, да си поставят цели и да разпределят времето ефективно по време на учебния процес, по отношение на подготовката за изпити и подготовката на самостоятелни работи.

5. По отношение на подготовката за тестовете, учебното помагало предоставя ресурси за полагането на практически изпити, примерни въпроси. По този начин се повишава увереността и представянето на обучаемите по време на изпитите.

6. Помагалото позволява адаптиране към стиловете на учене, като се отчитат различните индивидуални стилове на учене (визуални, слухови, кинестетични). Учебното помагало отчита тези различни предпочитания за учене, предоставяйки опции, които са в съответствие с предпочитания от индивида начин на учене.

7. Учебното помагало допринася за намаляване на стреса, като осигурят структуриран подход към ученето(разбиране, използване и пресъздаване), разбивайки огромни количества информация на управляеми части.

8. Учебното помагало позволява на обучаемите да преценят своето разбиране на материала, да идентифицират областите на слабости и съответно да коригират своя подход на обучение.

В аспекта на преподаваните дисциплини трябва да се уточни, че в бакалавърска степен се работи в детерминирана(определена) среда на използваните методи, вероятности, заплахи, уязвимости и нужди. При преподаването в магистърска степен се отчита неопределеността на средата, като в помагалото са добавени спомагателни методи за анализ на вероятностния характер на средата.

В текста ще забележите, че на места не се използват специфичните термини или наименования на конкретен обект, а популярното му название. Това е направено, за да се „олекоти“ текста, както и целевата аудитория да възприеме по-лесно методиката, без да се задълбочава в теоретични концепции. Също така ще забележите наличието на много термини в английския език, които на практика обозначават един и същ елемент или процес. В рамките на това учебно помагало сме се опитали да оптимизираме терминологията във възможните рамки на българския език(чрез алегории), така че всички аналитични методи да са разбираеми и приложими. От друга страна някои от използваните данни не са реалните(истинските). Това се дължи на факта, че по-голямата част от информацията за обектите е класифицирана, както и информацията от производителите, договорите и брошурите са специфични за конкретния обект. Прозата в изложението може да не е детайлна и описателна(дескриптивна), но е необходимо „активно четене“, за да се разберат и приложат елементите на анализа. Всички елементи, детайли и модели са свързани по между си.(бел. авт.)

От друга страна, поради наличието на много изчисления и вероятността да се допусне грешка, призовавам за използването на електронни таблици и автоматизирани инструменти особено за статистическите изчисление. Тези инструменти ни позволяват много по-бързото верифициране на моделите и тестване на повече модели. През последните две години поради онлайн обучението, това беше демонстрирано от мен и използвано от студентите с голяма лекота и успех.

The relevance of the cost-benefit method stems from its function as a decision-making tool used in various fields, such as defense and security, economics, business, public policy, and project management. It involves comparing the costs of different alternative solutions or projects with the expected benefits. The cost-benefit method is highly relevant as it provides a systematic and quantitative framework for decision-making.

Cost-benefit analysis is a widely used method in organizations, governments, and businesses for making informed decisions. It helps in the efficient allocation of resources by identifying projects or activities that offer the highest net benefit. This method is crucial for entities with limited resources to ensure that investments are directed toward initiatives that deliver the most significant overall value.

Cost-benefit analysis is also used for project evaluation, where decision-makers weigh the expected benefits against the projected costs to assess the viability of a project. Governments use this method to evaluate the impact of proposed policies, taking into account both short-term and long-term costs and benefits.

This method can also help in identifying and assessing the risks associated with a decision or project by quantifying the costs and benefits. It provides a transparent and systematic approach to decision-making, allowing stakeholders to understand the rationale behind a decision and prioritize multiple projects or initiatives based on their overall contribution to the organization's goals.

Furthermore, cost-benefit analysis enhances accountability by providing a basis for evaluating the success or failure of a decision or project. Its implementation allows organizations to compare actual results with initial forecasts, facilitating continuous improvement.

Decision-makers can also expand the cost-benefit method to include environmental and social factors beyond financial considerations, contributing to more comprehensive decision-making. Despite certain limitations, such as challenges in quantifying certain intangible factors, subjective assessments, and potential biases, the cost-benefit method remains an indispensable tool for guiding decisions and allocating resources across a wide range of fields.

The goal of the educational guide on economic analysis (cost-benefit) is to provide a tool and resource designed to help students learn, understand, and retain information related to the application of the methodology. This can improve the effectiveness of learning sessions (lectures and exercises) and the overall academic performance of students.

The tasks that the educational guide sets for the learning process are:

Facilitating the understanding of economic analysis methodology in defense and security. This is achieved by simplifying complex concepts, breaking down information into smaller parts, and providing visual representations to aid comprehension.

Organizing information by helping to structure data and information in a way that makes it easier for learners to grasp the connections between different topics and identify key elements.

Encouraging active understanding and use of the material through note-taking, application plans, and interactive exercises that encourage learners to engage actively in the learning process, enhancing understanding through active participation.

Time management by helping learners prioritize tasks, set goals, and allocate time effectively during the learning process, particularly in preparing for exams and independent work.

Exam preparation by providing resources for practice tests, sample questions, and other materials that boost learners' confidence and performance during exams.

Adapting to learning styles by accommodating different individual learning styles (visual, auditory, kinesthetic). The educational guide takes these preferences into account, offering options that align with each learner's preferred style.

Reducing stress by providing a structured approach to learning (understanding, applying, and reproducing), breaking down large amounts of information into manageable parts.

Self-assessment by allowing learners to evaluate their understanding of the material, identify areas of weakness, and adjust their learning approach accordingly.

In the context of the taught disciplines, it should be clarified that at the undergraduate level, the focus is on a deterministic (defined) environment of the methods used, probabilities, threats, vulnerabilities, and needs. In teaching at the master's level, the uncertainty of the environment is taken into account, and supplementary methods for analyzing the probabilistic nature of the environment are added to the guide.

In the text, you will notice that specific terms or names of particular objects are sometimes replaced with more popular terms. This is done to "lighten" the text and make it easier for the target audience to grasp the methodology without delving too deeply into theoretical concepts. Additionally, you will notice the presence of many terms in English, which in practice denote the same element or process. Within this educational guide, we have attempted to optimize the terminology within the possible limits of the Bulgarian language (through allegories), so that all analytical methods are understandable and applicable. On the other hand, some of the data used are not real (true). This is due to the fact that most of the information about the objects is classified, as well as the information from manufacturers, contracts, and brochures, which is specific to the particular object. The prose in the exposition may not be detailed and descriptive,

but "active reading" is necessary to understand and apply the elements of the analysis. All elements, details, and models are interconnected. (Note by the author.)

On the other hand, due to the presence of many calculations and the possibility of errors, I advocate for the use of spreadsheets and automated tools, especially for statistical calculations. These tools allow us to verify models much faster and test more models. Over the past two years, due to online learning, this was demonstrated by me and used by students with great ease and success.