Анотация на публикации по група показатели В.

Редът и номерацията са идентични с другите справки (номерата са от вида Bxx, както и имената на файловете в съответните фолдъри).

Номер	Публикация	Annotation	Анотация
B4. Хабилитационен труд – научни публикации (не по-малко от 10) в издания, които са реферирани и индексирани			
B01	George Sharkov. 2016. *From Cybersecurity to Collaborative Resiliency*. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig' 16). ACM, New York, NY, USA, 3-9. ISBN: 978-1-4503-4566-8. https://doi.org/10.1145/2994475.2994484 (in SCOPUS, WoS)	This paper presents the holistic approach to cyber resilience as a means of preparing for the "unknown unknowns" in cyberspace. Principles of augmented cyber risks management and resilience management model at national level are presented, with elaboration on multistakeholder engagement and partnership for the implementation of national cyber resilience collaborative framework. A system-of-systems (SoS) approach to national cybersecurity system is presented with mechanisms for threat intelligence and coordinated risk management and response. The model is implemented for defining the cyber maturity levels and operational network in the National Cybersecurity Strategy of Bulgaria "Cyber resilient Bulgaria 2020" (2016).	Този доклад представя цялостен „холистичен" подход към кибер устойчивостта на национално ниво за посрещане на „неизвестните неизвестни" в кибер пространството. Принципи за разширено управление на кибер рисковете и модел за управление на кибер устойчивост на национално ниво са представени, с акцент върху ангажиране на всички заинтересовани лица и партньорство за реализиране на национална (оперативна) мрежа за взаимодействие. Подходът на системи-от-системи (CoC) е развит за целите на национална система за кибер-устойчивост, както и механизми за откриване на заплахи и координирано управление на кибер рисковете и отговорите на атаки. Моделът е внедрен при изготвяне на Национална стратегия за киберсигурност „Кибер устойчива България 2020" (2016).
B02	Sharkov, G., Todorova, C., Koykov, G., Zahariev, G. *Hybrid exercising for cyber-resilient healthcare and cross-sector crisis response operability* (2021), CEUR Workshop Proceedings, Vol. 2933, pp. 329-351. ISSN: 1613-0073. (in SCOPUS). Online at: http://ceur-ws.org/Vol-2933/paper32.pdf	In this paper, the authors present an approach for the creation of a complex generic cyber range containing a variety of exercise polygons simulating and propagating vertical escalations related to the healthcare sector, its logistics, and supply chains within the context of COVID-19. The conceptual model for cross-sector crisis response presented is based on "system-of-intelligent-systems" concept, proposed by the authors. A special focus is put on the organizational aspects for the creation of a complex intersection of technical, tabletop, communications, and operational exercise environment and experience. The application of AI/ML methods and tools for simulation of cyber-attacks (red-teaming) and exercise facilitation is	Тази статия разглежда подход за създаване на комплексен и генеричен кибер полигон (cyber range) съдържащ широка гама установки, симулиращи вертикални ескалации в сектора на здравеопазването, логистиката и веригите за доставки в контекста на COVID-19. Представеният концептуален модел за отговор на крос-секторни кризи е базиран на концепцията „системи от интелигентни системи", разработен от авторите. Специален акцент е поставен върху организационните аспекти и пресечните точки между технически, tabletop и комуникационни/оперативни кибер учения. Изследването представя и преглед на приложенията на AI/ML методи за симулиране на

		overviewed. Lessons learned from three types of pilot exercises “Cyber Shockwave” in critical infrastructures are discussed.	кибер атаки (red team) и създаването, и управлението на хибридни кибер учения. Обобщен е и опитът с кибер полигони, базиран на провеждането на три мащабни кибер учения от типа „Cyber Shockwave”.
B03	Sharkov, G. (2020) *Assessing the Maturity of National Cybersecurity and Resilience*, December 2020, Connections:The Quarterly Journal 19(4):5-24, ISSN 1812-1098, e-ISSN 1812-2973, https://doi.org/10.11610/Connections.19.4.01 (in SCOPUS)	This paper presents a critical overview of existing standards and methods for assessing the cybersecurity and resilience maturity at national level. An approach towards defining and applying the enterprise resilience requirements and indicators at the level of critical sectors and entire countries is presented. Cyber maturity levels of large interoperable complex systems are defined and used to map indexes and assessment results. These levels are applied to determine cyber readiness and maturity of nations. A success story of implementing such assessment in Bulgaria is given.	Този доклад представя критичен преглед на известните стандарти и методи за оценка на състоянието и зрелостта на киберсигурността и кибер устойчивостта на национално ниво. Предложен е подход за дефинирането и прилагане на индустриални и организационни изисквания и индикатори към цели критични сектори и държави. Дефинирани са нива на „кибер зрялост“ на големи и сложни взаимодействащи си системи за целите на съпоставяне на индексите и резултати от одити. Пример с успешно прилагане в България е представен.
B04	Todor Tagarev, Nikolai Stoianov, and George Sharkov, *“Integrative Approach to Understand Vulnerabilities and Enhance the Security of Cyber-Bio-Cognitive-Physical Systems”* in Proceedings of the 18th European Conference on Cyberwarfare and Security (ECCWS19), edited by Tiago Cruz and Paulo Simoes, University of Coimbra, Portugal, 4-5 July 2019, pp. 492-500, ISBN: 9781510890091, http://www.proceedings.com/49816.html (in SCOPUS, WoS)	This paper presents an integrative approach to the exploration of ‘systems of systems’ (SoS) concept in five domains: communications and information systems and networks; cyber-physical system; bio-integrated systems; cognitive processes, i.e. the processes of shaping perceptions, assessing a certain situation and options and making decisions; and drones, remotely controlled or autonomous. The latter case is particularly reliant on advances in artificial intelligence. It outlines the problem of vulnerability of each of the five domains to influences from cyber space and gives criteria for cross-domain dependencies and risks based on SoS model..	Докладът представя интегриран подход към изследването на концепцията за „системи от системи“ (CoC) в пет области: комуникационни и информационни системи и мрежи; киберфизическа система; биоинтегрирани системи; когнитивни процеси, т.е. процеси на формиране на възприятия, оценка на определена ситуация и възможности и вземане на решения; и дронове, дистанционно управлявани или автономни, като последният случай е особено зависим от напредъка в областта на изкуствения интелект. Той очертава проблема с уязвимостта на всеки от петте домейна под въздействия от кибер пространството и дава критерии за между-секторни зависимости и рискове на базата на CoC модел.
B05	Todor Tagarev, George Sharkov: *Computationally Intensive Functions in Designing and*	This paper outlines six high-level, computationally demanding functions. The first three relate to the formulation and implementation of cybersecurity	Този доклад очертава шест функции на високо ниво, изискващи значителна изчислителна мощност. Първите три са свързани с

	Operating Distributed Cyber Secure and Resilient Systems. CompSysTech '19: Proceedings of the 20th International Conference on Computer Systems and Technologies June 2019 Pages 8–18 https://doi.org/10.1145/3345252.3345255 (in SCOPUS, WoS)	policy: understanding risk; planning and implementing cybersecurity measures; and continuous adaptation to the changing technological, threat and policy landscape. The other three functions are operational: situational awareness, including detection of cyberattacks and hybrid malicious activities; operational decision making, e.g. selecting a course of action under attack; and cyber forensics. A system-of-systems view to analyze and mitigate the risks at different levels is described.	формулирането и прилагането на политиката за киберсигурност: разбиране на риска; планиране и прилагане на мерки за киберсигурност; и непрекъснато адаптиране към променящия се технологичен, кибер-застрашен терен. Останалите три функции са оперативни: ситуационна осведоменост, включително откриване на кибератаки и хибридни злонамерени дейности; оперативно вземане на решения, напр. избор на курс на действие при атака; и кибер криминалистика. Предложен е подход на „система от системи" (CoC) за анализиране и смекчаване на рисковете.
B06	Yavor Papazov, George Sharkov, Georgi Koykov, Christina Todorova (2021/3) *Managing Cyber-Education Environments with Serverless Computing*, In: "Digital Transformation, Cyber Security and Resilience of Modern Societies", pp. 49-60, Springer Nature. ISBN 978-3-030-65721-5, ISSN 21976503, https://doi.org/10.1007/978-3-030-65722-2_4 (in SCOPUS)	This article is an experience report about the authors' efforts in applying the "serverless" computation paradigm for managing cyber education environments through the Course Manager platform developed by the authors' team. This paper further provides an in-depth overview of an innovative architecture and frontend of a cyber-education environment management framework, designed to work in a serverless environment. It analyses the lessons learnt from using said framework in providing cyber trainings to students and IT professionals for more than a year to shrink the skills and competences gap within the Bulgarian cybersecurity sector.	Тази статия представлява доклад за опита на авторите в прилагането на безсървърната изчислителна парадигмата за управлението на среди и полигони за обучения по киберсигурност чрез платформата Course Manager, разработена от екипа на авторите. Статията предоставя задълбочен преглед на иновативна архитектурата и фронтенд на платформата, проектирана да работи в „безсървърна" среда. Анализират се научените уроци от използването на посочената рамка при провеждането на киберобучения за студенти и ИТ специалисти в продължение на повече от година с цел намаляване на недостига на умения и компетентности в сектора на киберсигурността в България.
B07	Sharkov, G., Todorova, C., Varbanov, P. (2022) *Harnessing the Power of Responsible Innovation: The Shift Towards Human-Centered Skills and Competences in AI Engineering*, CEUR Workshop Proceedings ISGT'22, Vol. 3191, ISSN 1613-0073, pp. 1-17 http://ceur-ws.org/Vol-3191/paper01.pdf	This paper will investigate the shift of demands from AI specialists in the context of the rising body of legal, regulatory, and compliance frameworks, using current research and empirical data from a needs and market study. Based on a series of focus group interviews and quantitative studies, this paper presents results from representatives from European companies in three major groups - research and academia, small and medium-sized enterprises, and large enterprises. The study reveals	Това изследване разглежда промяната в изискванията към професионалисти в сферата на ИИ, в контекста на нарастващия брой правни и регулаторни рамки, на базата на емпирични данни от проучване на нуждите и пазара, направено от авторите. Въз основа на поредица от интервюта с фокус групи, комбинирани с количествени проучвания, този документ представя резултати, получени от анализ на отговори на представители на европейски

	(in SCOPUS)	a critical shift in skills and competencies required from AI professionals, a growing talent gap that needs to be filled by relevant educational initiatives and interdisciplinary, hands-on exercises.	компании в три основни групи - изследователски и академични организации, малки и средни предприятия и големи предприятия. Проучването разкрива критична промяна в изискванията към уменията и компетентностите на ИИ специалисти и техният нарастващ недостиг, който трябва да следва да бъде компенсиран чрез образователни инициативи, съчетани с интердисциплинарни и практически упражнения.
B08	Sharkov, G., Stoeva, M. (2022) *Multi-disciplinary approach to industry standards in the IT higher education programs*, CEUR Workshop Proceedings ISGT'2022, Vol. 3191, ISSN 1613-0073, pp. 51-62, http://ceur-ws.org/Vol-3191/paper05.pdf (in SCOPUS)	This paper descries a methodology and theoretical background to reshape the content and the way of training IT and cybersecurity professionals: informatics, software engineering, software technology and design, and business information technologies. It is based on the combination of structured knowledge, theoretical models for designing complex systems, secure coding requirements and designing cyber-resilient systems. Industry de-facto standards such as Capability Maturity Model Integration (CMMI), CMMI with Scrum, Test Maturity Model integration (TMMi), CERT Resilience Management Model (CERT-RMM) are "translated" to be applicable in small organizations with practical tasks and project implemented in teams. DevOps concept is extended to meet security requirements, namely DevSecOps. This methodology has been applied in two pilot courses at Plovdiv University (FMI) for 4 years.	Този доклад описва методология и теоретична основа за промяна на съдържанието и начина на обучение на специалисти по ИТ и киберсигурност: информатика, софтуерно инженерство, софтуерни технологии и дизайн и бизнес информационни технологии. Базира се на прилагането на комбинация от структурирани знания, теоретични модели за проектиране на сложни системи, изисквания за сигурно кодиране и проектиране на кибер-устойчиви системи. Индустриални де факто стандарти като Capability Maturity Model Integration (CMMI), CMMI със Scrum, Test Maturity Model Integration (TMMi), CERT Resilience Management Model (CERT-RMM) са „преведени", за да бъдат приложими в малки организации с практически задачи и проект, реализиран в екипи. Концепцията DevOps е разширена, за да отговори на изискванията за сигурност, а именно DevSecOps. Тази методология е приложена в два пилотни курса в Пловдивски университет (ФМИ).
B09	Ivaylo Gueorguiev, Christina Todorova, Pavel Varbanov, Petar Sharkov, George Sharkov, Carina Girvan, Nikoleta Yiannoutsou and Marianthi Grizioti: *Educational Robotics for Communication, Collaboration and Digital Fluency*. In: Lepuschitz W., Merdan M., Koppensteiner G., Balogh R.,	This contribution outlines the findings of an empirical investigation into the conception, execution, and outcomes of an educational robotics workshop in Bulgaria. A methodology for exploiting robots and automated devices to facilitate "learning-by-discovery" is presented with a focus on STEM and collaborative problem-solving. Initial steps towards complex interoperable systems are conducted, including features like reliability, safety,	В този материал са описани резултатите от емпирично изследване на концепцията, изпълнението и анализът от серия работилници по образователна роботика в България. Методология за използване на роботи и автоматизирани устройства за постигане на „учене чрез откриване" е представена с акцент върху STEM и колаборативното решаване на проблеми. Начални стъпки към сложни взаимодействащи си

	Obdržálek D. (eds) Robotics in Education. RiE 2017. Advances in Intelligent Systems and Computing, vol 630, pp. 113-125. Springer, Cham, ISBN 978-3-319-62874-5. DOI: https://doi.org/10.1007/978-3-319-62875-2_10. (in SCOPUS, WoS)	security. The workshops designed and piloted aim to build educational robotics activities for the cultivation of hard and soft skills and competences. The study was conducted with 312 in 2016.	системи са изпълнени, включително и аспекти като надеждност, безопасност, сигурност. Семинарите имат за цел да изградят образователни дейности по роботика за развиване на твърди и меки умения и компетентности. Изследването е проведено с 312 ученици през 2016 г.
B10	Vanderstraeten D, Chaerle L, Sharkov G, Lambers H, Van Montagu M (1995): *"Salicylic-acid enhances the activity of the alternative pathway of respiration in tobacco-leaves and induces thermogenicity"*. Planta 196 (SPRINGER VERLAG), ISSN: 00320935, Pp.412–419, https://doi.org/10.1007/BF00203637 (in SCOPUS, WoS)	The article presents a completely new concept and model to monitor and study the behavior of complex biological systems, such as plants, under stress and infection. It is based on infrared thermography methods and tools, and a development of specific new methods to automatically measure and analyze the surface temperature of leaves with infrared thermography and map to biochemical processes. New AI-based methods and tools have been elaborated to match the complex theoretical models and detect the correlations. This work is part of my post-doc in University of Gent, Laboratory of Genetics. Based on these results and the development and introduction of new model-based and AI-empowered methods for thermal imaging, a revolutionary new line of research was created which is still global leader. Citations of this paper and work are still growing (more than 45 in Scopus).	Статията представя напълно нова концепция и модел за наблюдение и изследване на поведението на сложни биологични системи, каквито са растенията, при стрес и инфекция. Базира се на методи и средства за инфрачервена термография, както и на разработените от мен специфични нови методи за автоматично измерване и анализ на повърхностната температура на листата с инфрачервена термография и съпоставянето с биохимичните процеси. Нови, базирани на ИИ методи и инструменти бяха създадени за съпоставяне на тези сложни теоретични модели и откриване на корелациите. Тази работа е част от моята пост-докторантура в Университета в Гент, в Лаборатория по генетика. На базата на тези резултати и разработените нови методи за обработка на термични изображения с помощта на ИИ, беше развита нова революционна линия на изследванията , която е световен лидер. Цитатите на този доклад и работата все още расте (над 45 цитата само в Scopus).

Таблица с анотации за публикациите от група показатели Г

Редът и номерацията са идентични с другите справки (номерата са от вида Gxx за целия раздел Г, както и имената на файловете в съответните фолдъри).

Номер	Публикация	Annotation	Анотация
Г7. Научни публикации в издания, които са реферирани и индексирани в световноизвестни бази данни с научна информация			
G01	Sharkov, G., Stoeva, M. (2021) *Introducing software quality maturity models in software engineering education and small organisations*, CEUR Workshop Proceedings, Vol. 2933, pp. 97-113. ISSN: 1613-0073 http://ceur-ws.org/Vol-2933/paper10.pdf (in SCOPUS)	This paper descries a methodology for applying industry-defined "maturity models" and up-to-date requirements to software and IT systems, including their reliability, robustness, safety, and cybersecurity. This research was performed both at the university (form small studio course team projects) and some small companies. It is based on the combination of structured knowledge, theoretical models for designing complex systems, secure coding requirements and designing cyber-resilient systems. Industry de-facto standards such as CMMI, tests-model TMMi, CERT Resilience Management Model (CERT-RMM) and others. This methodology has been applied in two pilot courses at Plovdiv University (FMI) for 4 years.	Този документ описва методология за прилагане на дефинирани от индустрията „модели на зрялост" и актуални изисквания към софтуера и ИТ системите, включително тяхната надеждност, устойчивост, безопасност и киберсигурност. Това изследване е извършено както в университета (от малки студийни екипни проекти), така и в няколко малки компании. Базира се на комбинацията от структурирани знания, теоретични модели за проектиране на сложни системи, изисквания за сигурно кодиране и проектиране на кибер-устойчиви системи. Индустриални де факто стандарти като CMMI, тестов модел TMMi, CERT Resilience Management Model (CERT-RMM) и други са включени. Тази методология сме приложили в два пилотни курса в Пловдивския университет (ФМИ) в продължение на 4 години.
G02	Boiko M. Balev, George I. Sharkov (1990): "Knowledge-Based Interpretation of Biophysical Images". In: Philippe Jorrand, Vasil Sgurev (Eds.): Artificial Intelligence IV: Methodology, Systems, Applications - Proceedings of the Fourth International Conference AIMSA '90, North-Holland, 1990, ISBN 0-444-88771-7. Pp. 405-414 (in WoS, WOS:A1990BT97Z00040)	This paper presents a knowledge-representation methods and tools dedicated to modeling biophysical objects and processes and their use for analysis and interpretation of biophysical images and video sequences. The multi-level knowledge representation structure follows the organization of knowledge already formalized in referenced expert systems for planning biophysical experiments. The reasoning of the system is based on abstract models of objects investigated and the physicochemical processes observed. The system ISIA can process and analyze 2-d static and dynamic images, and applies heuristic rules as formulated by experts for recognizing the objects and measuring their parameters. An	Тази статия представя методи и инструменти за представяне на знания, посветени на моделирането на биофизични обекти и процеси и тяхното използване за анализ и интерпретация на биофизични изображения и видео последователности. Многослойната структура на представяне на знания следва организацията на знанията, вече формализирани в референтни експертни системи за планиране на биофизични експерименти. Разсъжденията на системата се основават на абстрактни модели на изследваните обекти и наблюдаваните физикохимични процеси. Системата ISIA може да обработва и анализира двумерни статични и динамични

		innovative, behavior driven and predictive approach to image recognition, tracing and measurements was presented for microscopic and other image sequences from biological experiments. It is generic and has been applied for the next thermographic research performed as post-doc in University of Gent.	изображения и прилага евристични правила, формулирани от експерти за разпознаване на обекти и измерване на техните параметри. Демонстриран е разработеният иновативен, поведенчески подход за разпознаване с предсказание, проследяване и измервания на изображения за микроскопични и други последователности от изображения от биологични експерименти. Той е генеричен и беше впоследствие приложен за следващото изследване с термографски изображения, извършено като пост-доктор в Университета на Гент.
Г8. Научни публикации в нереферирани списания с научно рецензиране или в редактирани колективни томове			
G03	Posea, Vlad, George Sharkov, Adrian Baumann, and Georgios Chatzichristos. "Towards Unified European Cyber Incident and Crisis Management Ontology." *Information & Security: An International Journal* 53, no. 1 (2022): 33-44. https://doi.org/10.11610/isij.5303	ENISA (the European Cybersecurity Agency) highlighted the need for a common reporting taxonomy for cybersecurity incidents to be used by cybersecurity analysts across Europe. The analysis of the domain revealed a large number of taxonomies for different areas of the cybersecurity domain (types of attacks, vulnerabilities, sectors, harm), but those needed to be linked together in a model that allows a cybersecurity officer to report and track an incident fast and accurately. The taxonomy should also treat the cybersecurity domain not only from the technical point of view but also from the socio-economical aspect. This document describes the theoretical ontology model, composed by different established taxonomies, and the methodology used to develop it and define the use for information sharing, crisis management and response.	ENISA (Европейската агенция за киберсигурност) подчерта необходимостта от обща таксономия за докладване на инциденти в киберсигурността, която да се използва от анализаторите на киберсигурността в цяла Европа. Анализът на домейна разкри голям брой таксономии за различни области на домейна на киберсигурността (видове атаки, уязвимости, сектори, щети), но тези трябваше да бъдат свързани заедно в модел, който позволява на служител по киберсигурността да докладва и проследява инцидент бързо и точно. Таксономията трябва също така да третира областта на киберсигурността не само от техническа гледна точка, но и от социално-икономически аспект. Този документ описва теоретичния онтологичен модел, съставен от различни установени таксономии, и методологията, използвана за разработването му и определяне на използването за споделяне на информация, управление на кризи и реакция.
G04	Sharkov, G., Todorova, C., Koykov, G., Nikolov, I. (2022) *Towards a Robust and Scalable Cyber Range Federation for Sectoral Cyber/Hybrid Exercising: The*	The current contribution describes the authors' experience designing the Red Ranger, a Composite Cyber Range. The authors detail the design and development to facilitate the agility required to support a working multi-faceted	Статията описва опита на авторите при проектирането на Red Ranger – композитен кибер полигон (cyber range). Подробно е описано проектирането, разработването и практиките, използвани за

	Red Ranger and ECHO Collaborative Experience, Information & Security: An International Journal 53, no. 2 (2022): 287-302. https://doi.org/10.11610/isij.5319	federation with the ECHO Cyber Range to allow for an "exercise-as-a-service" model to provide adequate and accessible cyber-hybrid mechanisms for crisis response training and preparation. The federation at system level is based on advanced and elastic architecture and cloud resources management. At the application level it is based on the system-of-systems model, developed by the author, to simulate the interoperable real systems in critical infrastructure, study the dependencies and identify weaknesses, and used them for blue-team response.	подобряване на гъвкавостта на системата, необходима за поддържане на работеща многостранна федерация с кибер полигона ECHO. Статията описва и подходът при федерирането, с крайна цел да се създаде възможност за провеждането на "кибер-учение като услуга", който да осигури адекватни и достъпни киберхибридни механизми за обучение и подготовка за реакция при кризи. Федерацията на системно ниво се основава на усъвършенствана и еластична архитектура и управление на облачни ресурси. На ниво приложение той се основава на модела система-от-системи, разработен от автора, за да симулира оперативно съвместими реални системи в критична инфраструктура, да проучи зависимостите и да идентифицира слабостите и да ги използва за отговор на „синия екип".
G05	Sharkov, G., Stoeva, M. (2022) *Bringing Industrial International Standards to ICT Higher University Education*, EDULEARN22 Proceedings, ISSN: 2340-1117, pp. 6131-6138, Vol. 2933, pp. 97-113. ISSN: 1613-0073, https://dx.doi.org/10.21125/edulearn.2022.1446 (to appear in WoS)	A selection of international defined software quality standards, covering the software development lifecycle (SDL), including the Secure SDL, have been analyzed for their applicability for the training of ICT professionals and software engineers. Standards such as CMMI, tests-model TMMi, CERT Resilience Management Model (CERT-RMM), and "agile" implementations (like Scrum, DevOps, DevSecOps) have been reviewed and mapped towards the e-competences EU standards (e-CF, ICT job profiles). Some specific process as defined by these standards and other contextual requirements (like technical robustness, security and resilience of systems) have been applied to define maturity levels and design the courses and exercises with university students.	Подбрани международни дефинирани стандарти за качество на софтуера, обхващащи жизнения цикъл на разработката на софтуер (SDL), включително Secure SDL, бяха анализирани за тяхната приложимост за обучение на ИКТ специалисти и софтуерни инженери. Стандарти като CMMI, модел за организиране на тестването - TMMi, CERT Resilience Management Model (CERT-RMM) и „гъвкави" реализации (като Scrum, DevOps, DevSecOps) бяха прегледани и съпоставени със стандартите на ЕС за е-компетенции (e-CF, работни профили в ИКТ). Някои специфични процеси, определени от тези стандарти и други контекстуални изисквания (като техническа устойчивост, сигурност и устойчивост на системите), са приложени за определяне на нивата на зрялост и проектиране на курсове и упражнения със студенти.
G06	Sharkov, George, Christina Todorova, and Pavel Varbanov. *"Strategies, Policies, and Standards in the EU Towards a Roadmap for Robust and Trustworthy AI Certification."*	Within recent years, governments in the EU member states have put increasing efforts into managing the scope and speed of socio-technical transformations due to rapid advances in Artificial Intelligence (AI). Guaranteeing and providing access to reliable AI is a prerequisite for the proper	През последните години ЕС полага все по-големи усилия за управление на обхвата и скоростта на социо-техническите трансформации, дължащи се на бързия напредък в областта на изкуствения интелект (ИИ). Гарантирането и осигуряването на достъп до надежден

	Information & Security: An International Journal 50, no. 1 (2021): 11-22. https://doi.org/10.11610/isij.5030	development of the sector. One way to approach this challenge is through governance and certification. This article discusses initiatives supporting a better understanding of AI adoption's magnitude and depth. Given the numerous ethical concerns posed by "unstandardised AI", it further explains why certification and governance of AI are a milestone for the reliability, security, robustness, trustworthiness and competitiveness of technological solutions.	ИИ е предпоставка за развитието на сектора. Един от начините да се подходи към това предизвикателство е чрез стандартизация и сертифициране. В тази статия са разгледани инициативи, подпомагащи по-доброто разбиране на мащаба и дълбочината на внедряването на ИИ. Предвид многобройните етични проблеми, породени от нестандартизирания ИИ, в нея се обяснява още защо сертифицирането и стандартизацията на ИИ са императивни за надеждността, сигурността, устойчивостта и конкурентоспособността на технологичните решения.
G07	Sharkov, George, Christina Todorova, Georgi Koykov, and Georgi Zahariev. *"A System-of-Systems Approach for the Creation of a Composite Cyber Range for Cyber/Hybrid Exercising."* Information & Security: An International Journal 50, no. 2 (2021): 129-148. https://doi.org/10.11610/isij.5029	Complex cyber-hybrid scenarios, exercising effective collaboration at the technical, operational, and higher decision-making levels, are increasingly employed to prepare to face emerging hybrid threats. The current contribution presents the authors' experience in designing a Composite Cyber Range, following a System-of-Systems (SoS) approach for the dynamic activation or incorporation of playgrounds and on-the-run integration of custom-made emulation or overlay ranges to support an exercise-as-a-service model for the provision of adequate and accessible cyber-hybrid mechanisms for crisis response training and preparation.	Сложните киберхибридни сценарии, при които се упражнява колаборация на техническо, оперативно и високо ниво на вземане на решения, все по-често се използват за подготовка за посрещане на нововъзникващи хибридни заплахи. Тази статия представя опита на авторите в проектирането на композитен кибер полигон (cyber range), следвайки подхода за сигурност на системи от системи за динамичното активиране и интегриране на кибер-полигони, включително и емулационни и "overlay" кибер полигони по модела на " кибер-учение като услуга" за осигуряване на адекватни и достъпни киберхибридни механизми за обучение и подготовка за реакция при кризи.
G08	George Sharkov (2021) *Harnessing the Potential of AI Against COVID-19 Through the Lens of Cybersecurity: Challenges, Tools, and Techniques.* Information & Security: An International Journal, Vol. 49 (2021):49-69. https://isij.eu/node/22973/	In this paper, the author analyses and discusses recent AI applications for the fight against the COVID-19 pandemic through the prism of cybersecurity and data privacy. The article discusses system-of-systems propositions for companies and SMEs concerning the ethical and safe use of AI means, methods, and tools. Furthermore, the paper provides an overview of recent developments and applications of AI methods and tools in terms of AI against COVID-19, AI for Cybersecurity, Cybersecurity for AI, and Misusing AI. A special focus is given on the AI-specific supply chains (like training data) and other interdependencies are analyzed in view of the coming certification schemes (under Cyber Act, AI Act, Cyber Resilience act, etc.)	В тази статия авторът анализира и обсъжда последните приложения на изкуствения интелект за борба с пандемията COVID-19 през призмата на киберсигурността и неприкосновеността на личните данни. В статията се обсъждат и някои предложения за прилагане на подхода за сигурност на системи от системир насочени към компаниите и МСП за етичното и безопасно използване на средствата, методите и инструментите на ИИ. Освен това статията прави преглед на последните разработки и приложения на методите и инструментите на ИИ по отношение на ИИ срещу COVID-19, ИИ за киберсигурност, киберсигурност за ИИ и злоупотреба с ИИ. Обръща се специален акцент върху специфичните за AI вериги за доставки (като данни за обучение) и се анализират други взаимозависимости с оглед на предстоящите схеми за сертифициране (съгласно Cyber Act, AI Act, Cyber Resilience Act и др.)

G09	Sharkov, G., Papazov, Y., Todorova, C., Koykov, Zahariev, G., *MonSys: A Scalable Platform for Monitoring Digital Services Availability, Threat Intelligence and Cyber Resilience Situational Awareness,* Information & Security An International Journal 46-2 (2020):155-167 https://doi.org/10.11610/isij.4611	This article presents a design and architecture of a flexible, robust, and scalable monitoring platform implemented as a cloud-based service and an on-premise solution specifically designed to address the need for ensuring service availability at an individual level. This new platform MonSys offers a variety of standardised service availability checks, including web-based services from multiple geographical locations and a flexible platform and tools for defining customised complex services. Particular attention is paid to the processes of metrics collection, processing, storage, and querying. The end goal of creating this platform is for its results to produce guidelines for improving relevant skills and competences, security architecture hardening, and identification of training needs.	В тази статия е представена MonSys - гъвкава, надеждна и мащабируема мониторинг платформа, реализирана като облачна услуга и локално решение. MonSys предлага разнообразни стандартизирани проверки на наличността на услугите, включително на уеб-базирани услуги от различни географски местоположения, както и гъвкава платформа и инструменти за дефиниране на персонализирани комплексни услуги. Особено внимание е обърнато на процесите на събиране, обработка, съхранение и търсене на метрики. Крайната цел на създаването на тази платформа е резултатите от нея да доведат до изготвянето на насоки за подобряване на уменията и компетентностите на персонала, укрепване на архитектурата за сигурност и определяне на нуждите от обучение.
G10	Sharkov, G., Todorova, C., Papazov, Y., Koykov, G., Zahariev, G. (2021) *Chapter One: Cybersecurity Tools for Threat Intelligence and Vulnerability Monitoring for National and Sectoral Analysis. In book: Information Security in Education and Practice*, ed. Kalinka Kaloyanova, Cambridge Scholars Publishing. ISBN-10 : 152756066X. Pp. 1-18 https://www.cambridgescholars.com/product/978-1-5275-6066-6	This paper provides insights into the findings from the pilot implementation of Cyber Map Bulgaria, revealing chronic vulnerabilities in the IT infrastructure of different industries in Bulgaria. The authors discuss how the implications of this study could be used to provide guidelines for developing training programs to supplement critical gaps in the security skills and competences in the Bulgarian context. The paper further provides a brief overview of the architectural underpinnings of Cyber Map Bulgaria, a technical tool developed by the authors to provide an aggregated picture of the technical profile and the vulnerabilities of a large number of systems of systems, focusing first on Bulgarian cyberspace and also, at a larger scale, on specific sectors or interconnected digital businesses (clusters).	Тази статия представя резултатите от пилотното прилагане на Кибер картата на България, която разкрива хронични уязвимости в ИТ инфраструктурата на различни индустрии в България. Авторите обсъждат как резултатите от това проучване могат да се използват за предоставяне на насоки за разработване на учебни програми за попълване на критичните пропуски в уменията и компетенциите в областта на киберсигурността в българския контекст. В статията се прави и кратък преглед на архитектурните основи на Кибер карта на България - технически инструмент, разработен от авторите с цел да се предостави обобщена картина на техническия профил и уязвимостите на голям брой системи от системи, като се акцентира първо върху българското киберпространство, а също така и в по-голям мащаб, за конкретни сектори или взаимосвързани дигитални бизнеси (клъстери).
G11	Gkamas V., Rigou M., Paraskevas M., Zarouchas T., Perikos I., Vassiliou V., Gueorguiev .I, Varbanov P., Sharkov G., Todorova C., Sotiropoulou A., *Bridging the skills gap in the Data Science and Internet of Things domains: A Vocational Education and Training Curriculum.* In: Brown, M., Nic Giolla Mhichil, M., Beirne, E., & Costello, E. (eds.) (2020). Proceedings of the 2019	In this work, the authors present the macro-level design of knowledge model, skills and competences, training objectives and the learning outcomes of a multi-disciplinary VET program for data science and the Internet of Things. Data Science and Internet of Things are currently among the key drivers of skills and competences required by the IT market. As a skills' gap is projected in the Data Science and Internet of Things domains, substantial effort is required by training providers to upskill the IT workforce, including	В тази работа авторите представят дизайна на учебните цели и структурирането на уменията и компетентностите при създаването на мултидисциплинарна програма за ПОО в областите на науката за данните и интернет на нещата. Понастоящем науката за данните и интернет на нещата са сред ключовите фактори, влияещи върху еволюцията в изискванията за уменията и компетенциите на ИТ пазара. Тъй като се прогнозира недостиг на умения в тези две области, са необходими значителни усилия от

	ICDE World Conference on Online Learning, Volume 1, Dublin City University, Dublin. ISBN: 978-1-911669-10-4 http://dx.doi.org/10.5281/zenodo.3804014	security architectures and trustworthiness. This article details an approach towards this end goal.	страна на доставчиците на обучение за повишаване на квалификацията на ИТ работната сила, включително по отношение на архитектурите за сигурност и надеждност. Тази статия описва подход, свързан с тази крайна цел.
G12	Sharkov, G., Papazov, Y., Todorova, C., Koykov, G., Georgiev, M., Zahariev, G., "Cyber Threat Map for National and Sectoral Analysis", *Computer and Communications Engineering,* Vol. 13, No. 2/2019. Workshop on Information Security 2019, 9th Balkan Conference in Informatics. ISSN 1314-2291	This paper presents Cyber Map Bulgaria, a technical tool developed by the authors to provide an aggregated picture of the technical profile and the vulnerabilities of a large number of systems of systems, focusing first on Bulgarian cyberspace and also, at a larger scale, on specific sectors or interconnected digital businesses (clusters). This paper further summarizes the work and some of the findings from the pilot run of "Cyber Map Bulgaria," such as chronic vulnerabilities per domain or groups of domains or identifying critical points within the public and private IT infrastructure.	В настоящата статия е представена Кибер карта на България - технически инструмент, разработен от авторите с цел да се предостави обобщена картина на техническия профил и уязвимостите на голям брой системи от системи, като се акцентира първо върху българското киберпространство, а също така и в по-голям мащаб, за конкретни сектори или взаимосвързани дигитални бизнеси (клъстери). В този документ е представено и обобщение на работата и някои от изводите от пилотното пускане на "Киберкарта България", като например хронични уязвимости по домейни или групи от домейни или идентифициране на критични точки в публичната и частната ИТ инфраструктура.
G13	Christina Todorova, Carina Girvan, Nikoleta Yiannoutsou, Marianthi Grizioti, Ivaylo Gueorguiev, Pavel Varbanov, George Sharkov. *Visualising mathematics with the MathBot: a constructionist activity to explore mathematical concepts through robotics* Proceedings Int. Conference Constructionism 2018, Vilnius, Lithuania, pp. 656-663, ISBN 978-609-95760-1-5 http://www.constructionism2018.fsf.vu.lt/file/repository/Proceeding_2018_Constructionism.pdf	In this practice paper, we aim to share our experience with the design and implementation of constructionist educational robotics activities tailored to primary school students (4th grade, age 9-11 years) implemented in a series of robotics workshops, which took place within a real school setting in Sofia, Bulgaria. Through this contribution, we will further present an activity plan involving student engagement with mathematical concepts (angle measuring and properties of the circle) to program the behavior of a robot to teach critical STEM concepts, skills, and competences, such as collaborative problem-solving.	В тази статия от практиката целим да споделим опита си в проектирането и изпълнението на конструктивистки образователни дейности по роботика, пригодени за ученици от началното училище (4 клас, 9-11 години), реализирани в поредица от работилници по роботика, които се проведоха в реална училищна среда в София, България. Чрез този принос ще представим допълнително план за дейност, включващ ангажиране на учениците с математически понятия (измерване на ъгъл и свойства на окръжност) за програмиране на поведението на робот с цел преподаване на критични STEM концепции, умения и компетентности, като например колаборативно решаване на проблеми.
G14	Ivaylo Gueorguiev, Christina Todorova, Nikoleta Yiannoutsou, Xristina Greka, Pavel Varbanov, George Sharkov, Carina Girvan, Julian M. Angel-Fernandez, Lisa Vittori, Annalise Duca, *Towards a Generic Curriculum for Educational Robotics in STEM: From Scientific Concepts to Technologies and*	This paper and its corresponding poster present a "work in progress" concept for visualising 19 educational activity plans into a generic curriculum map for teaching critical STEM concepts, skills, and competences, such as collaborative problem-solving through constructionist robotics activities. Six educational paths represent potential use cases, and these have been validated through 148	Този доклад и съответният му постер представят концепция за визуализиране на 19 учебни плана в обща учебна програма за преподаване на критични STEM концепции, умения и компетентности, като например колаборативно решаване на проблеми чрез конструкционистки дейности по роботика. Шест учебни направления са обсъдени в потенциалните им приложения и са валидирани чрез 148 образователни

	Powerful Ideas. Proceedings Int. Conference Constructionism 2018, Vilnius, Lithuania, pp. 697-700, ISBN 978-609-95760-1-5 http://www.constructionism2018.fsf.vu.lt/file/repository/Proceeding_2018_Constructionism.pdf	educational robotics workshops implemented with children between the ages of 7 and 18 in six European countries.	семинара по роботика, реализирани с деца на възраст между 7 и 18 години в шест европейски държави.
G15	Todor Tagarev, George Sharkov, and Nikolai Stoianov, "Cyber Security and Resilience of Modern Societies: A Research Management Architecture," Information & Security: An International Journal, Volume 38 (2017), p.93-108, DOI: https://dx.doi.org/10.11610/isij.3807 . ISSN 0861-5160, e-ISSN 1314-2119	Advanced information and communications technologies (ICT) facilitate the increase of effectiveness and efficiency of defense and security organizations, governmental services, the economy, and quality of life, while at the same time providing opportunities for malicious actors to cause significant damage without exercising physical coercion. Policies for security and resilience of modern societies to threats and risks from the cyberspace account for foreseen cyber threats, their immediate impact on ICT infrastructure, consequent effects on critical services, as well as cascading effects across systems and infrastructures. This paper presents the architecture used to plan and, consequently, manage cybersecurity research in Bulgaria. It follows five application areas (information management systems; industrial control systems; unmanned and remotely piloted vehicles; bio-integrated systems; and cognitive processes and decision-making), the study of systems of systems, and support to the formulation and implementation of cybersecurity policy.	Усъвършенстваните информационни и комуникационни технологии (ИКТ) улесняват повишаването на ефективността и ефикасността на организациите за отбрана и сигурност, правителствените служби, икономиката и качеството на живот, като в същото време предоставят възможности на злонамерените участници да причинят значителни щети, без да упражняват физическа принуда . Политиките за сигурност и устойчивост на съвременните общества на заплахи и рискове от киберпространството отчитат предвидените киберзаплахи, тяхното непосредствено въздействие върху ИКТ инфраструктурата, последващите ефекти върху критичните услуги, както и каскадните ефекти в системите и инфраструктурите. Тази статия представя архитектурата, използвана за планиране и, следователно, управление на изследванията в областта на киберсигурността в България. Той следва пет области на приложение (системи за управление на информация; системи за промишлен контрол; безпилотни и дистанционно пилотирани превозни средства; биоинтегрирани системи; и когнитивни процеси и вземане на решения), изследване на системи от системи и подкрепа за формулиране и прилагане на киберсигурност политика.
G16	George Sharkov (2017), "A Systems-of-Systems Approach to Cybersecurity and Resilience", Information & Security: An International Journal, Volume 37 (2017), pp. 69-94, ISSN 0861-5160, e-ISSN 1314-2119, https://isij.eu/node/22974	To address the cybersecurity, safety, and reliability aspects of the entire digitalized ecosystems, we need first to understand and possibly model how the respective computer systems of different participating entities interoperate and collaborate. Modern computer systems and emerging applications are not just largescale and complex in the digitally connected world. We categorize them also as decentralized, distributed, networked, interoperable compositions of heterogeneous and (semi)autonomous systems and/or elements. These new types of composite systems with emergent behavior have	За да разгледаме аспектите на киберсигурността, безопасността и надеждността на цялата цифровизирана екосистема, първо трябва да разберем и евентуално да моделираме как съответните компютърни системи на различни участващи субекти взаимодействат и си сътрудничат. Съвременните компютърни системи и нововъзникващите приложения не са просто мащабни и сложни в дигитално свързания свят. Ние ги категоризираме също като децентрализирани, разпределени, мрежови, оперативно съвместими композиции от хетерогенни и

		been defined as “Systems of Systems” (SoS). This paper explores different types of SoS and analyzes the interdependencies to manage cybersecurity threats and risks and achieve cyber resilience. It describes a new theoretical approach towards achieving cyber resilience of SoS, suitable for threat intelligence, composite risk management, and “layered” view on different types of SoS, namely: functional SoS, safety monitoring and supervisory SoS, and cybersecurity layer. An AI-empowered overlay (or SoS-ring) is also discussed, in support to decision-making, and coordinated response and prevention in real time. An SoS view on managing the supply/value chain cyber risks is also outlined, including the “hidden” risks. This new theoretical model and some of the practical implementations have been presented as invited talks at various conferences (ACM, IEEE, ITU, ENISA, AFCEA), and also implemented partially in the National Cybersecurity Strategy for the operational collaborative network definition and specification.	(полу)автономни системи и/или елементи. Тези нови типове съставни системи с възникващо поведение са определени като „Системи от системи“ (SoS). Този документ изследва различни видове SoS и анализира взаимозависимостите за управление на заплахите и рисковете за киберсигурността и постигане на кибер устойчивост. Той предлага нов теоретичен подход за постигане на кибер устойчивост на SoS, подходящ за търсене на заплахи, комбинирано управление на риска и „слоест“ поглед върху различни видове SoS, а именно: функционални SoS, мониторинг на безопасността и надзорен SoS, както и слой от SoS за киберсигурност. Обсъжда се също специален покриващ слой (пръстен), подпомаган от ИИ решения, в подкрепа на вземането на решения и координиран отговор и превенция в реално време. Очертава се също и едно SoS виждане за управление на киберрисковете по веригата за доставки/стойност, включително „скритите“ рискове. Този нов теоретичен модел и някои от практическите реализации бяха представени като лекции покана на различни конференции (ACM, IEEE, ITU, ENISA, AFCEA) и също така частично внедрени в Националната стратегия за киберсигурност за дефиниране и спецификация на оперативна мрежа за сътрудничество.
G17	George Sharkov and Christina Todorova. "Capture the Flag for Cyber-Resilience Exercising through Cryptographic Puzzles and Collaborative Problem-Solving." Information & Security: An International Journal (2017): 95-102. https://isij.eu/node/22975	This paper provides an overview of the possibilities of Capture the Flag (CTF) exercises to test cybersecurity capabilities into a complex system-of-systems setting using collaborative methodologies and cryptographic challenges. It also discusses the bridge from theory to practice and combining theoretical cryptographic knowledge with practical tools and attack scenarios. It presents the experience and lessons learned from four summer schools “CryptoBG”.	Тази статия прави обзор на възможностите и приложенията на "Capture the Flag" (CTF) кибер учения за тестване на способностите за киберсигурност в сложна среда на системи от системи, като се използват колаборативни методологии и криптографски задачи. Той също така обсъжда моста от теория към практика и комбинирането на теоретични криптографски знания с практически инструменти и сценарии за атака. Представен е опитът и поуките от четири летни школи CryptoBG.
G18	Sharkov G., Stoeva M., *Software Engineering Management Education – Bringing Industry Standards to the University Program*, Tenth Jubilee International Conference Information systems and grid technologies – ISGT’16, September 30 - October 1,	This paper presents and early stage of implementing a new style and methodology for teaching software engineers, information security specialists Some de-facto software standards (CMMI, TMMi, RMM) have been discussed and introduced to enrich the university education with practical knowledge and competences. Results from students’ course	Този документ представя ранен етап на внедряване на нов стил и методология за обучение на софтуерни инженери, специалисти по информационна сигурност Някои де факто софтуерни стандарти (CMMI, TMMi, RMM) бяха обсъдени и въведени, за да обогатят университетското образование с практически знания и компетенции. Резултатите от курсовата работа на

	2016., Sofia, Bulgaria, pp. 184-198, ISSN 1314-4855	work (competitive team projects) are presented and discussed.	студентите (състезателни екипни проекти) се представят и обсъждат.
G19	Tagarev, Todor and George Sharkov. "Multi-stakeholder Approach to Cybersecurity and Resilience." *Information & Security: An International Journal* 34, no. 1 (2016): 59-68. https://doi.org/10.11610/isij.3404	Identifying and involving all relevant stakeholders in national cybersecurity strategy (NCSS) development is key for defining the scope, setting the goals and approaches, and the roadmap to achieve targeted maturity levels. It is more than involving the three groups (government, private sector, academia) and requires a holistic approach towards security and resilience of all interconnected segments of national and international cyberspace. The paper presents the approach to making the Bulgarian NCSS (BG-NCSS). Different aspects of stakeholders' involvement and engagements are considered: for identifying the scope and developing the strategy, defining the responsibilities and engaging with the development of a national collaboration operational network, strategy implementation and the roadmap to a resilient society, and collaboration to achieve operational cyber resiliency. As a collaboration mechanism, applications of public-private partnerships at different levels are envisaged.	Идентифицирането и включването на всички съответни заинтересовани страни в разработването на национална стратегия за киберсигурност (NCSS) е ключово за определяне на обхвата, определяне на целите и подходите и пътната карта за постигане на целеви нива на зрялост. Той включва повече от трите групи (правителство, частен сектор, академични среди) и изисква холистичен подход към сигурността и устойчивостта на всички взаимосвързани сегменти на националното и международното киберпространство. В статията е представен подходът за създаване на Българската НКСС (BG-NCSS). Разглеждат се различни аспекти на участието и ангажиментите на заинтересованите страни: за идентифициране на обхвата и разработване на стратегията, определяне на отговорностите и ангажиране с разработването на национална оперативна мрежа за сътрудничество, изпълнение на стратегията и пътна карта за устойчиво общество и сътрудничество за постигане на оперативно киберустойчивост. Като механизъм за сътрудничество се предвиждат приложения на публично-частни партньорства на различни нива.
G20	George Sharkov, Petya Asenova, Valentina Ivanova, Ivaylo Gueorguiev, Pavel Varbanov: “Evaluation of ICT Curricula using European e-Competence Framework”, In: Proceedings of the 10th Annual International Conference on Computer Science and Education in Computer Science 2014 (CSECS2014); ISSN 1313-8624 pp. 275-294	This paper presents a method for evaluation of e-competences (knowledge, skills and attitudes/proficiency levels) as outputs of university ICT bachelor and master programs. The benchmarking is based on the European e-Competence Framework (e-CF) - a set of 40 competences derived from IT job profiles, which became an EU standard by CEN in 2015. The method and e-CF framework can be used by ICT business, policy makers and public authorities, HR organizations, education and VET, as well as in cross-industries. The mapping method is bidirectional starting with courses/modules assessment of the learning outcomes towards e-CF, then aggregate to a target ICT jobs profiles. The analysis of the mappings allows updates and improvements at the program level to meet industry demands, but also a fine tuning of the courses to gradually build competences and have a coherent theoretical and practical learning path. The paper presents the method and results of the approach, analyses its applicability for	Този документ представя метод за оценка на е-компетенции (знания, умения и нагласи/нива на владеене) като резултати от бакалавърски и магистърски програми по ИКТ в университета. Сравнителният анализ се основава на Европейската рамка за електронни компетенции (e-CF) - набор от 40 компетенции, извлечени от профили на работа в ИТ, които станаха стандарт на ЕС от CEN през 2015 г. Методът и рамката за е-компетенции могат да се използват от ИКТ бизнес, политици и публични органи, организации за човешки ресурси, образование, както и в различни индустрии. Методът на картографиране е двупосочен, като се започва с оценка на курсове и модули на резултатите от обучението към e-CF, след което се агрегира към целеви профили на работа в ИКТ. Анализът на съпоставянията позволява актуализации и подобрения на ниво програма, за да се отговори на изискванията на индустрията, но също така и фина

		continual improvements of curricula and the teaching approach in order to create long-term ICT competences which meet better industry needs, European and global trends.	настройка на курсовете за постепенно изграждат компетенции и имат съгласувана теоретична и практическа пътека на обучение. Статията представя метода и резултатите от подхода, анализира приложимостта му за непрекъснати подобрения на учебните програми и подхода на преподаване с цел създаване на дългосрочни ИКТ компетенции, които отговарят на по-добрите нужди на индустрията, европейските и световните тенденции.
G21	Valentina Ivanova, Latchezar Tomov, George Sharkov, Ivaylo Gueorguiev: "Towards e-Leadership M.Sc. Program Curricula". In: Proceedings of the 10th Annual International Conference on Computer Science and Education in Computer Science 2014 (CSECS2014); ISSN 1313-8624 pp. 315-325	The paper presents analysis of existing information about NBU M.Sc., IT PM Program. Individual courses, modules and the program are mapped to e-CF competences. The e-CF profile of the program is compared to CEN ICT profiles and to e-Leadership profiles. The content and the teaching methods are adapted to the recommendations, and curricula improvement opportunities are identified and discussed.	Статията представя анализ на съществуваща информация за магистърската програма на НБУ, IT PM. Индивидуалните курсове, модули и програмата са свързани с компетенциите за e-CF. e-CF профилът на програмата се сравнява със CEN ICT профилите, както и с e-Leadership профилите. Съдържанието и методите на преподаване са адаптирани към препоръките, а възможностите за подобряване на учебните програми са идентифицирани и обсъдени.
G22	Peter Weiss, John O'Sullivan, George Sharkov, "ICT Certification in Action: Positioning Methodology of e-Certs against e-CF". In: eChallenges e-2011 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), IIMC International Information Management Corporation (2011) ISBN: 978-1-905824-27-4, http://www.echallenges.org/e2011/	The paper presents research concerning positioning of ICT Certifications against the European e-Competence Framework (e-CF). The research aims at evaluation and trial of possibilities and options to implement a methodology for positioning ICT certifications onto the e-CF and the European Qualifications Framework (EQF). Results of analysis of the CompTIA Roadmap are presented including 74 of some of most prominent certifications offered on the market. The roadmap intends to offer guidance to learners through offering career paths for typical IT professions such as e.g. Security Specialist or Network Administrator. The paper explains background and details of applied methodology for the analysis and presents some results.	Статията представя изследване относно позиционирането на ИКТ сертификатите спрямо Европейската рамка за електронна компетентност (e-CF). Изследването има за цел да оцени и изпробва възможностите и опциите за прилагане на методология за позициониране на ИКТ сертификати в e-CF и Европейската квалификационна рамка (EQF). Резултатите от анализа на пътната карта на CompTIA са представени, включително 74 от някои от най-известните сертификати, предлагани на пазара. Пътната карта има за цел да предложи насоки на учащите чрез предлагане на кариерни пътеки за типични ИТ професии, като напр. Специалист по сигурността или мрежов администратор. Статията обяснява основата и подробностите на приложената методология за анализа и представя някои резултати.
G23	George Sharkov and Dimitar Birov, "Challenging the IT University Education and Innovations in Bulgaria: Introducing management Aspects of Software for IT Graduates", in Proc. Euroean Computer Science Summit ECSS 2011, pp. 61-64	This paper presents a new model and methodology to designing the university education in ICT and software engineering. It is based on introducing management aspects of software and IT services development, and synergy in three areas: Technical focus areas (enabling technology", Management Focus Area, Business and Organizational Control Focus Area. Industry driven knowledge and skills	Тази статия представя нов модел и методология за проектиране на университетското образование по ИКТ и софтуерно инженерство. Базира се на въвеждане на управленски аспекти на разработването на софтуер и ИТ услуги и синергия в три области: Технически фокусирани области; Област на управленски фокус, Област на бизнеса и организационния контрол.

		areas have been defined, and a special new inter-university program SEMP (Software Engineering Management Program) as launched in partnership with Carnegie Mellon University, involving 4 Bulgarian universities.	Дефинирани са области на знания и умения, ориентирани към индустрията, и специална нова междууниверситетска програма SEMP (Програма за управление на софтуерното инженерство), стартирана в партньорство с университета Карнеги Мелън, включваща 4 български университета.
G24	Van Der Straeten, Dominique, George Sharkov, and Marc Van Montagu, "Fever in Plants: Thermogenic Responses of Tobacco to Exogenous Salicylate." Journal Thermologie Osterreich 4 (1): pp. 10–17 (1994), ISSN: 1021-4356	A novel approach to study the thermogenic responses in living organisms is presented. It is based on theoretical models of the behavior of complex biological systems, combined with the latest technologies to monitor and register the thermal patterns in living objects. From the technology aspect, the infrared thermography methods and tools are used to automatically measure and analyze the surface temperature of leaves. AI-based methods and programs have been developed to perform an advanced quantitative/qualitative analysis of the behavior and correlate to physico-chemical processes. A discovery of a phenomenon was achieved, namely the mechanism of the response to exogenous salicylate. This work is part of my post-doc in University of Gent, Laboratory of Genetics, and application of my knowledge-based "expert systems" work in the field of biophysics.	Представен е нов подход за изследване на термогенните реакции в живите организми. Базира се на теоретични модели на поведението на сложни биологични системи, съчетани с най-новите технологии за наблюдение и регистриране на топлинните модели в живите обекти. От гледна точка на технологията, методите и инструментите за инфрачервена термография се използват за автоматично измерване и анализ на повърхностната температура на листата. Базирани на AI методи и програми са разработени за извършване на усъвършенстван количествен/качествен анализ на поведението и корелация с физико-химични процеси. Беше постигнато откритие на един феномен, а именно механизма на отговора към екзогенния салицилат. Тази работа е част от моята пост-докторантура в Университета на Гент, Лаборатория по генетика, и прилагането на моята базирана на знания работа по „експертни системи" в областта на биофизиката.
G25	B. Balev, G. Sharkov, "Knowledge representation in intelligent system for image analysis". In: Computer Analysis of Images and Patterns, Proceedings of the IV International Conference CAIP'91 (Dresden, September 17-19, 1991), edited by Reinhard Klette, ISBN 3-05-501299-2 DM118. Akademie Verlag GmbH, Berlin, Germany. Pp. 239-247	This paper presents developed by our team knowledge-representation methods and tools dedicated to modeling biophysical objects and processes and their use for analysis and interpretation of biophysical images and video sequences. The multi-level knowledge representation structure follows the organization of knowledge already formalized in referenced expert systems for planning biophysical experiments. The reasoning of the system is based on abstract models of objects investigated and the physicochemical processes observed. The system ISIA can process and analyze 2-d static and dynamic images, and applies heuristic rules as formulated by experts for recognizing the objects and measuring their parameters. Promising results from applying to support two expert systems for experimental data extraction and analysis are presented.	Този доклад представя разработени от нас методи и инструменти за представяне на знания, посветени на моделирането на биофизични обекти и процеси и тяхното използване за анализ и интерпретация на биофизични изображения и видео последователности. Многостепенната структура на представяне на знания следва организацията на знанията, вече формализирани в разработени експертни системи за планиране на биофизични експерименти. Разсъжденията на системата се основават на абстрактни модели на изследваните обекти и наблюдаваните физикохимични процеси. Системата ISIA може да обработва и анализира двумерни статични и динамични изображения и прилага евристични правила, формулирани от експерти за разпознаване на обекти и измерване на техните параметри. Представени са обещаващи резултати от прилагането

			за поддръжка на две експертни системи за извличане и анализ на експериментални данни.
G26	Sharkov, G., and D. S. Dimitrov, “AI Approach to research in membrane biophysics”, in. Proc. Int. Seminar “AI Methods in Biological Research”, Prague (1989), pp. 84-91, ISBN 80-02-99441	A generic knowledge-based approach to modeling the biological objects with their complex structure, processes and mechanisms for their interaction, and response to external fields is presented. The experimental application in the field of biophysics is described, and the specialized Knowledge Representation Environment for Biological Systems (KREBS) is outlined. Two main components of the environment are detailed – the “descriptive” language (frame-based) and the “reasoning module” (implemented by production rules, fuzzy logic and temporal logic).	Представен е генеричен, базиран на знания подход за моделиране на биологични обекти с тяхната сложна структура, процеси и механизми за тяхното взаимодействие и реакция на външни полета. Описано е експерименталното приложение в областта на биофизиката и е очертана специализираната среда за представяне на знания за биологични системи (KREBS). Подробно са описани два основни компонента на средата – „описателният“ език (базиран на рамка) и „разсъждаващият модул“ (имплементиран от производствени правила, размита логика и времева логика).

Номер	Публикация	Annotation	Анотация
Г9. Публикувана глава от колективна монография			
G901	Д. Полимирова, В. Шаламанов, Н. Стоянов, Т. Тагарев, Я. Янакиев, Г. Шарков, Я. Папазов, В. Ризов, К. Иванова, *Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България* (София: ИПА, 2019 г.). ISBN 978-619-7262-14-8 https://www.ipa.government.bg/sites/default/files/01_ipa_study_v10.0._final_ed.pdf Глава: Приложение на иновативни технологии в работата на държавната администрация: Анализ на възможностите за използване на изкуствен интелект и чатботове при предоставяне на услуги и	In this chapter of the collective monograph systematizes the current state of research in the field of AI and the practical possibilities, good practices and prospects for using AI methods and means for providing services and servicing users, mainly for the public administrative services sector. Aspects of using AI systems in cyber security, security and defense are also discussed. The three main aspects of the use of AI are presented - ethical, legal and technological, in relation to the author's participation in the European High Level Expert Group on "Trustworthy AI" and the guidelines adopted by the EC. A number of examples and recommendations are given for the use of AI systems in various fields of services and activities, including those for managing critical resources and "essential services" (as defined by the EC).	В тази глава от колективната монография систематизира съвременното състояние на изследванията в областта на ИИ и практическите възможности, добрите практики и перспективите за използване на методите и средствата на ИИ за предоставяне на услуги и обслужване на потребители, основно за сектора на публичните административни услуги. Разгледани са и аспектите на използване на системи с ИИ в областта на киберсигурността, на сигурността и отбраната. Представени са трите основни аспекта за използването на ИИ – етични, правни и технологични, във връзка с участието на автора в Европейската група на високо ниво за „Надежден ИИ“ (Trustworthy AI) и приетите насоки от ЕК. Дадени са редица примери и препоръки за използване на системи с ИИ в различни сфери услуги и дейности, включително и такива за управление на критични ресурси и „съществени услуги“ (според дефиницията на ЕК).

	комуникация с потребителите, както и за поддържане на кибер сигурността (стр. 142-172)		
G902	Глава: Среда за кибер сигурност в България: Основни рискове и заплахи за кибер сигурността в НАТО и ЕС със специфични измерения за България (стр. 174 – 191)	This chapter describes and analyzes the cyber security environment in Bulgaria in the context of NATO and EU membership and development trends in several directions - development and implementation of standards, interoperability, development of information sharing systems, as well as coordinated rapid response of large-scale incidents and crises. Described are: - The main risks and threats for cyber security in NATO and the EU, and the specific dimensions for Bulgaria; - The standards for interoperability and cyber security and resilience in Bulgaria and NATO, EU; - Information sharing and joint rapid response systems in Bulgaria and within NATO and the EU; - Types and types of cyber exercises, public and private sector exercises, cyber resilience exercises. The taxonomy developed by the author for sharing information on large-scale cyber incidents and crises, which has been adopted by ENISA, is presented.	В тази глава е описана и анализирана средата за киберсигурност в България в контекста на членството в НАТО и ЕС и тенденциите за развитие в няколко посоки – развитие и прилагане на стандарти, оперативна съвместимост, развитие на системи за споделяне на информация, както и координирано бързо реагиране на инциденти от голям мащаб и кризи. Описани са: - Основните рискове и ззплахи за киберсигурността в НАТО и ЕС, и специфичните измерения за България; - Стандартите за оперативна съвместимост и киберсигурност и устойчивост в България и НАТО, ЕС; - Системи за споделяне на информация и съвместна бърза реакция в България и в рамките на НАТО и ЕС; - Видовете и типове кибер учения, участие на публичния и частен сектор, учения за кибер устойчивост. Представена е разработената от автора таксономия за споделяне на информация за кибер инциденти от голям мащаб и кризи, която е възприета от ENISA.