РЕЗЮМЕТА НА НАУЧНИ ТРУДОВЕ

на гл. ас. д-р инж. Галя Павлова
За участие в конкурс за заемане на академична длъжност „Доцент“,
В област на висше образование: 5. Технически науки, професионално направление: 5.3. Комуникационна и компютърна техника, специалност: „Системи с изкуствен интелект“,
обявен в ДВ брой 94 / 25-11-2022

I. ОБЩА ХАРАКТЕРИСТИКА НА НАУЧНИТЕ ТРУДОВЕ

Гл. ас. д-р инж. Галя Павлова, представя за участие в конкурса 1 монографичен труд (Показател В3) и 39 публикации (Показатели Г7 и Г8). Реферирани и индексирани в Scopus и/или Web of Science са 26 публикации, от които 10 са с SJR. Останалите 13 са публикации в нереферирани списания с научно рецензиране или в съвременни български научни издания с научно рецензиране от Националния референтен списък. От представените публикации 3 са на български език и 36 са на английски. Има и публикувано учебно пособие (показател Ж24).

II. ***ПОКАЗАТЕЛ В3:*** РЕЗЮМЕ НА МОНОГРАФИЧЕН ТРУД

***Галя Павлова**, „Изкуствен интелект и роботика“ Авангард прима, София, 2022,141 с., ISBN: 978-619-239-725-8*

Настоящата монография е посветена на изследването на приложение на методи от изкуствения интелект в роботиката.

В първа глава са разгледани мотивите за използването на елементи на изкуствен интелект в областта на движението и действието на роботите, структурно-функционалната интеграция на ниво технически характеристики и когнитивни способности. Направена е оценка на алгоритмите за машинно обучение по отношение на точност; време за обучени; размер, качество и вид на данните; брой параметри, брой на характеристиките. Разгледани са подходите за проектиране на роботи с подходящо разпределена мобилност и съответстваща интелигентност.

Във втора глава се третират проблемите на приложението на роботи с елементи на изкуствен интелект в Индустрия 4.0. Разгледани са основните принципи за идентифициране на четвъртата индустриална революция, връзките между гъвкавост, интелигентност и производителност, хардуерните и софтуерни изисквания към изкуствения интелект. Посочени са характеристиките на видовете софтуерни приложения, характерни за етапите на хардуерно развитие. Посочени са конкретни възможности за прилагане на ИИ в умните фабрики и подобряване на ефективността на производството като е предложена универсална схема система за управление на умно производство. Изследвани са проблемите

за защита на данните при индустриалния интернет на нещата и комуникацията машина към машина.

В трета глава се третират проблеми на колаборативната работа на хора и роботи в умните фабрики. Изследвана е нормативната база за оценка на риска и безопасна работа при съвместна работа на хора и роботи с елементи на изкуствен интелект. Типизирани са съвместните дейности на хора и роботи. Разгледани са мерки за регулиране на изкуствения интелект в индустрията, като са отчетени възможни интелигентни кибератаки и тяхното влияние върху киберфизичните системи.

III. СПИСЪК С ПУБЛИКАЦИИ и РЕЗЮМЕТА - ***Показател Г7***:

Списък с научни публикации, които са реферирани и индексирани в световноизвестни бази данни научна информация

№	Заглавие на публикация
Г7.1	O. Nakov, R. Trifonov, **G. Pavlova** and P. Nakov, "Comparative Analysis of the Interoperability Assessment Methods and Approaches in the Industry 4.0," *2022 10th International Scientific Conference on Computer Science (COMSCI)*, 2022, pp. 1-4, **ISBN** 978-166549777-0, doi: 10.1109/COMSCI55378.2022.9912606. https://www.scopus.com/record/display.uri?eid=2-s2.0-85141438941&origin=resultslist&sort=plf-f **SCOPUS**
Г7.2	R. Trifonov, S. Manolov, G. Tsochev, **G. Pavlova** and K. Raynova, "Analytical Choice of an Effective Cyber Security Structure with Artificial Intelligence in Industrial Control Systems," *2022 10th International Scientific Conference on Computer Science (COMSCI)*, 2022, pp. 1-6, doi: 10.1109/COMSCI55378.2022.9912608. **ISBN** 978-166549777-0, https://www.scopus.com/record/display.uri?eid=2-s2.0-85141410960&origin=resultslist&sort=plf-f **SCOPUS**
Г7.3	E. Sabev, R. Trifonov, **G. Pavlova** and K. Rainova, "Cybersecurity Analysis of Wind Farm SCADA Systems," 2021 International Conference on Information Technologies (InfoTech), 2021, pp. 1-5, ISBN:978-1-6654-0324-5, doi: 10.1109/InfoTech52438.2021.9548589. Scopushttps://www.scopus.com/record/display.uri?eid=2-s2.0-85116605845&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=0&citeCnt=1&searchTerm= **SCOPUS**
Г7.4	I. Chavdarov, I.Georgiev, L. Miteva, R.Trifonov **and G. Pavlova** Analysis of the kinematic characteristics of a 3D printed finger of robotic humanoid hand, ACM International Conference Proceeding Series, In Proceedings of CompSysTech '20, June 18–19, 2021, Ruse, Bulgaria, pp. 145–150 https://doi.org/10.1145/3472410.3472434 ISBN: 978-1-4503-8982-2 https://www.scopus.com/record/display.uri?eid=2-s2.0-85117580999&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=1&citeCnt=0&searchTerm= **SCOPUS, SJR 0.232**
Г7.5	R. Trifonov, S. Manolov, R. Yoshinov, G. Tsochev and **G. Pavlova** "Applying the Experience of Artificial Intelligence Methods for Information Systems Cyber Protection at

	Industrial Control Systems," *2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, Athens, Greece August 22-24, 2021, **ISBN:**978-1-6654-2749-4, doi: 10.1109/CSCC53858.2021.00012. https://www.scopus.com/record/display.uri?eid=2-s2.0-85125017847&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=2&citeCnt=0&searchTerm= **SCOPUS**
Г7.6	R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov and **G. Pavlova,** "Cyber Trends in Industrial Control Systems," 2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC), 2021, pp. 41-45, ISBN:978-1-6654-2749-4, doi: 10.1109/CSCC53858.2021.00015. https://www.scopus.com/record/display.uri?eid=2-s2.0-85125014263&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=3&citeCnt=0&searchTerm= **SCOPUS**
Г7.7	O. Nakov, R. Trifonov**, G. Pavlova** and P. Nakov, "Analysis of Software Vulnerabilities, Measures for Prevention and Protection and Security Testing," *2021 29th National Conference with International Participation (TELECOM)*, 2021, pp. 73-76, ISBN:978-1-6654-3344-0, doi: 10.1109/TELECOM53156.2021.9659585. https://www.scopus.com/record/display.uri?eid=2-s2.0-85124526561&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=4&citeCnt=0&searchTerm= **SCOPUS**
Г7.8	E. Sabev, R. Trifonov, G.Tsochev, **G. Pavlova** and K.Raynova. Analysis of practical cyberattack scenarios for wind farm SCADA systems, I, IEEE International Conference Automatics and Informatics'2021 (ICAI'21), 30 September – 3 October 2021, pp. 420-424, ISBN:978-1-6654-2661-9, doi: 10.1109/ICAI52893.2021.9639550. https://www.scopus.com/record/display.uri?eid=2-s2.0-85123852960&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=5&citeCnt=0&searchTerm= **SCOPUS**
Г7.9	R. Trifonov, O. Nakov, S. Manolov, G. Tsochev and **G. Pavlova,** "Cyber-Security of Industrial Computer Systems" - Differentiation as a Separate Discipline, IEEE International Conference Automatics and Informatics'2021 (ICAI'21), 30 September– 3 October 2021, pp. 414-419, ISBN:978-1-6654-2661-9, doi: 10.1109/ICAI52893.2021.9639645. https://www.scopus.com/record/display.uri?eid=2-s2.0-85123823070&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=6&citeCnt=0&searchTerm= **SCOPUS**
Г7.10	R. Trifonov, O. Nakov, **G. Pavlova,** S. Manolov, G. Tsochev and P. Nakov, "Analysis of the Principles and Criteria for Secure Software Development," 2020 28th National Conference with International Participation (TELECOM), Sofia, 2020, pp. 125-128, Scopus, doi: 10.1109/TELECOM50385.2020.9299567. https://www.scopus.com/record/display.uri?eid=2-s2.0-85099456666&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=7&citeCnt=2&searchTerm= **SCOPUS**
Г7.11	R. Trifonov, O. Nakov, S. Manolov, G. Tsochev and **G. Pavlova,** "Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods," 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, ISBN:978-1-7281-9308-3, doi: 10.1109/ICAI50593.2020.9311333

	https://www.scopus.com/record/display.uri?eid=2-s2.0-85100097464&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=8&citeCnt=2&searchTerm= **SCOPUS**
Г7.12	G. Tsochev, R. Trifonov, O. Nakov, S. Manolov and **G. Pavlova,** "Cyber security: Threats and Challenges," 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-6, ISBN:978-1-7281-9308-3, doi: 10.1109/ICAI50593.2020.9311369. https://www.scopus.com/record/display.uri?eid=2-s2.0-85100089082&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=9&citeCnt=6&searchTerm= **SCOPUS**
Г7.13	Trifonov, R., Manolov, S., Tsochev, G., **Pavlova, G.,** Recommendations Concerning the Selection of Artificial Intelligence Methods for Increasing of Cyber-Security, CompSysTech '20: Proceedings of the 21st International Conference on Computer Systems and Technologies '20June 2020 Pages 51–55, ISBN:978-1-4503-7768-3 https://www.scopus.com/record/display.uri?eid=2-s2.0-85090566161&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=10&citeCnt=0&searchTerm= **SCOPUS, SJR 0.232**
Г7.14	Miteva, L., Pavlova, G., Trifonov, R., Yovchev, K., Manipulability Analysis of Redundant Robotic Manipulator CompSysTech '20: Proceedings of the 21st International Conference on Computer Systems and Technologies '20June 2020 Pages 135–140, ISBN:978-1-4503-7768-3, https://doi.org/10.1145/3407982.3407987 https://www.scopus.com/record/display.uri?eid=2-s2.0-85090558710&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=11&citeCnt=2&searchTerm= **SCOPUS SJR 0.232**
Г7.15	Chavdarov, I., Krastev, A., Naydenov, B., **Pavlova, G.** Analysis and experiments with a 3D printed walking robot to improve climbing obstacle, International Journal of Advanced Robotic SystemsVolume 17, Issue 3, May-June 2020, pp.1-13, ISSN:1729-8806, https://doi.org/10.1177/1729881420925282, https://www.scopus.com/record/display.uri?eid=2-s2.0-85086182967&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=12&citeCnt=2&searchTerm= **SCOPUS SJR 0.549**
Г7.16	G. Tsochev, R. Trifonov, S. Manolov and **G. Pavlova,** "Investigation of Secure Mobile Agents as a Tool in Intrusion Detection Systems," 2020 International Conference on Mathematics and Computers in Science and Engineering (MACISE), Madrid, Spain, 2020, pp. 114-118, ISBN:978-1-7281-6695-7, doi: 10.1109/MACISE49704.2020.00026, https://www.scopus.com/record/display.uri?eid=2-s2.0-85092733201&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=13&citeCnt=0&searchTerm= **SCOPUS**
Г7.17	Trifonov, R., Nakov, O., Manolov, S., Tsochev, G., **Pavlova, G.,** New approaches to the investigations and classification of cyber threats challenged by the application of artificial intelligence methods, CEUR Workshop Proceedings, 2020, 2656, pp. 82–91, https://www.scopus.com/record/display.uri?eid=2-s2.0-85090878832&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=14&citeCnt=0&searchTerm= **SCOPUS, SJR 0.228**
Г7.18	Trifonov, O Nakov, S Manolov, G Tsochev, **G Pavlova,** One method of network cyber-security, based on artificial intelligence, 27th National Conference with International

	Participation: The Ways to Connect the Future, TELECOM 2019 - Proceedings, 2019, pp. 39-41, doi: 10.1109/TELECOM48729.2019.8994880. https://www.scopus.com/record/display.uri?eid=2-s2.0-85080924720&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=15&citeCnt=2&searchTerm= **SCOPUS**
Г7.19	G.Tsochev, R.Trifonov, R. Yoshinov, S. Manolov, **G. Pavlova,** Improving the Efficiency of IDPS by Using Hybrid Methods from Artificial Intelligence, Proceedings of the International Conference on Information Technologies (InfoTech-2019) 19-20 September 2019, p.1-4, Scopus,ISSN 1314-1023 https://www.scopus.com/record/display.uri?eid=2-s2.0-85074297374&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=16&citeCnt=3&searchTerm= **SCOPUS**
Г7.20	D. Budakova**, G. Pavlova,** R. Trifonov, Chavdarov, I., Obstacle avoidance algorithms for mobile robots, ACM International Conference Proceeding Series, 20-th International Conference on Computer Systems and Technologies. CompSysTech'19, Ruse, Bulgaria — June 21-22, 2019, pp. 78-83 ISBN 978-1-4503-7149-0 https://www.scopus.com/record/display.uri?eid=2-s2.0-85073065922&origin=resultslist&sort=plf-f&src=s&sid=6db6349f6b9d3dd79a6d032218b95d38&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=17&citeCnt=0&searchTerm= **SCOPUS SJR 0.232**
Г7.21	Tsochev, G., Trifonov, R., Manolov, S., Popov, G., **Pavlova, G.,** Some Security Model Based on Multi Agent Systems, International Conference on Control, Artificial Intelligence, Robotics and Optimization, ICCAIRO 2018, 2 July 2018, Prague, pp. 32-36 doi: 10.1109/ICCAIRO.2018.00014 (Scopus), https://www.scopus.com/record/display.uri?eid=2-s2.0-85065168337&origin=resultslist&sort=plf-f&src=s&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=19&citeCnt=3&searchTerm= **SCOPUS**
Г7.22	R. Trifonov, G. Tsochev, G. Pavlova, R. Yoshinov and S. Manolov, "Adaptive Optimization Techniques for Inteligent Network Security," 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2017, pp. 219-223, doi: 10.1109/MCSI.2017.45. scopus.com/record/display.uri?eid=2-s2.0-85050346251&origin=resultslist&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=20&citeCnt=4&searchTerm= **SCOPUS**
Г7.23	R. Trifonov, R. Yoshinov, **G. Pavlova**, G. Tsochev, Artificial neural network intelligent method for prediction, 2017 International Conference on Mathematical Methods & Computational Techniques in Science & Engineering MMCTSE 2017, Cambridge, UK, February 24-26, 2017, AIP Conference Proceedings 1872, 020021 (2017), https://doi.org/10.1063/1.4996678 https://www.scopus.com/record/display.uri?eid=2-s2.0-85029836287&origin=resultslist&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=21&citeCnt=6&searchTerm= **SCOPUS, SJR 0.189**
Г7.24	R. Trifonov, D. Budakova, **G. Pavlova,** Neural network application in financial area, 18-th International Conference on Computer Systems and Technologies CompSysTech'17, 23-24 June 2017, University of Ruse, Bulgaria, ACM Digital Library (2017), p.52-57, doi/10.1145/3134302.3134336

	https://www.scopus.com/record/display.uri?eid=2-s2.0-85038447740&origin=resultslist&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=22&citeCnt=0&searchTerm= **SCOPUS, SJR 0.232**
Г7.25	R. Trifonov, R. Yoshinov, B. Jekov, and **G. Pavlova**, "Open data assessment", AIP Conference Proceedings 1836, 020078 (2017) https://doi.org/10.1063/1.4982018, ISSN:0094-243X https://www.scopus.com/record/display.uri?eid=2-s2.0-85021322037&origin=resultslist&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=23&citeCnt=1&searchTerm= **SCOPUS, SJR 0.189**
Г7.26	R. Trifonov, S. Manolov, Radoslav Yoshinov, G. Tsochev, G. Pavlova, An adequate response to new Cyber Security challenges through Artificial Intelligence methods. Applications in Business and Economics., WSEAS TRANSACTIONS on BUSINESS and ECONOMICS, Volume 14, 2017, E-ISSN: 2224-2899, pp. 272-281, Scopus, https://www.scopus.com/record/display.uri?eid=2-s2.0-85037051141&origin=resultslist&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=8f228dcddf8c459850562e8fbc937e9b&sot=aut&sdt=a&sl=18&s=AU-ID%2857194637773%29&relpos=24&citeCnt=4&searchTerm= **SCOPUS, SJR 0.194**

Г7.1. Сравнителен анализ на методите и подходите за оценка на оперативната съвместимост в Индустрия 4.0

Технологичната основа на съвременната индустрия се състои от интелигентни, когнитивни, свързани, вградени и цифрово интегрирани системи, които до голяма степен подпомагат автоматизацията и по-добрата организация на производствените процеси. В този документ се разглеждат стандарти, които улесняват оперативната съвместимост вътре в предприятието и междуиндустриалното сътрудничество, за да се разберат по-добре проблемите и да се идентифицират бариерите пред оперативната съвместимост. Направен е сравнителен анализ на основните методи и подходи за оценка на оперативната съвместимост по отношение на системите в колаборативно предприятие с цел интелигентните корпоративни системи да работят оперативно и да взаимодействат правилно.

Г7.2. Аналитичен избор на ефективна структура за киберсигурност с изкуствен интелект в индустриални системи за управление

Новата парадигма на индустриалното развитие, наречена Индустрия 4.0, се сблъсква с проблемите на киберсигурността и се фокусира върху използването на инструменти за изкуствен интелект за повишаване на устойчивостта на индустриалните информационни системи срещу кибер заплахи. Определят се индикаторите, които служат за оценка и сравнение на въздействията върху контролираните елементи. Сравнени са основните референтни модели, описващи съответно IS и ICS: референтният модел на приложната информационна архитектура и референтният модел PERA, както и архитектурата ISA-95. Разгледани са сценарии за атаки срещу индустриални компютърни системи. Дефиниран е на алгоритми за откриване на заплахи и аномалии на основата на децентрализиран модел с използване на различни комбинации от методи на изкуствения интелект.

Г7.3. *Анализ на киберсигурността на SCADA системи за вятърни ферми*

Настоящата тенденция за въвеждане на повече възобновяема енергия като основен енергиен източник за човечеството увеличава броя на системите за надзорен контрол и събиране на данни (SCADA) във вятърните паркове по целия свят Сигурността на вятърните

турбини започва с класическия контрол на достъпа и се простира до защита на чувствителни зони с кодови карти. SCADA системите често са уязвими срещу различни видове кибератаки и по този начин позволяват на нарушителите успешно да се намесят и да проникнат в различни SCADA системи на вятърни паркове. Направено е изследване архитектурата и свързаните с нея атаки върху SCADA системите за вятърни паркове и са идентифицирани съществуващите уязвимости в реалния свят за такъв тип системи. Уязвимостите са обособени в четири групи - Вектори на физическа атака; Уязвимости на непрекъснатостта на работата; Вектори на мрежова атака; уязвимости, причинени от човек.

Г7.4. *Анализ на кинематичните характеристики на 3D отпечатан пръст на роботизирана хуманоидна ръка*

В тази статия е представена оригинална идея за отпечатване на пръстите на хуманоидна ръка напълно сглобени. Основните кинематични характеристики на пръста на хуманоидната ръка са изследвани с помощта на концепциите за отворена кинематична верига. Реализиран е алгоритъм за определяне на основните кинематични характеристики на пръста, като работно пространство и манипулативност. Резултатите за всички пръсти, без палеца, са описани и сравнени с помощта на техния среден размер и ставни ограничения.

Г7.5. *Прилагане на опита от методите на изкуствения интелект за киберзащита на информационните системи в индустриални системи за управление”*

На базата на опит в прилагането на инструменти на изкуствения интелект в киберзащитата на информационните системи и по-точно, създавайки и успешно експериментирайки с хибриден модел на система за откриване и предотвратяване на проникване (IDPS) е проучена и експериментирана възможността за прилагане на подобен модел към индустриални системи за управление. Изследвани са критериите за избор на адекватни методи в зависимост от спецификата на заплахите и до каква степен ще бъдат продуктивни при другия тип системи.

Г7.6. Тенденциите за кибератаки в индустриалните системи за управление

Индустриалните системи днес използват интернет и облачни технологии, което ги прави уязвими на модерни атаки. С пандемията от COVID-19 много хора се преместиха да работят от вкъщи, което доведе до увеличаване на кибератаките. Индустриалните решения за киберсигурност са насочени към защита на технологичното оборудване с оглед на нарастващия риск от заплахи в тази област. Тази статия представя изследване на текущите заплахи за индустриалните системи и някои гледни точки към тях. Предлага се изследване на интелигентни методи за анализ на обменяната информация, потоците в мрежите, източниците на заплахи, както и планиране на ефективни мерки за въздействие, вкл. проактивно (т.е. атакуване на основните източници на заплаха, като центрове за контрол на бот-мрежи и т.н.) за индустриални системи за контрол.

Г7.7. *Анализ на софтуерни уязвимости, мерки за превенция и защита и тестване на сигурността*

Направен е анализ на приложения с най-популярни софтуерни уязвимости и са посочени ефективни мерки за предотвратяване на злоупотребата с тези уязвимости от нарушители по време на проектирането на кода. Важна роля играе и тестването на софтуера. В този документ също се разглеждат видове софтуерно тестване и най-популярните инструменти за тестване. Обсъждат се резултатите от проведените тестове за сигурност.

Г7.8. ***Анализ на практически сценарии за кибератака за SCADA системи за вятърни паркове”***

SCADA системите често са уязвим срещу различни видове кибератаки, които позволяват на нападателите успешно да експлоатират и манипулират този тип системи във вятърните паркове. Представени са сценарии за атака, които използват вече съществуващи уязвимости в реалния свят. Сценариите на атаката ще бъдат демонстрирани на специално изработен тестов стенд на SCADA система за вятърна ферма. Едно от основните заключения е, че няма решение или подход „един размер, подходящ за всички“, когато става въпрос за киберсигурност в Индустрия 4.0. Всяка ICS/SCADA система изисква универсални политики и стандарти, разрешаващи IT/OT конвергенцията и затварящи всички съществуващи пропуски в сигурността.

Г7.9. Обособяване на "Киберсигурност на индустриални компютърни системи" като отделна дисциплина

Разработва се методология и учебни програми за обучение по киберсигурност във висшето образование, следвайки основните принципи, изложени в доклада на ACM и IEEE „Computing Curricula 2020“, а именно: преход от дефиниране базирани на знания учебни програми за обучение по компетенции в компютърното обучение и разширяване на обхвата на обучението по компютърни науки. Анализирани са разликите в подхода и интерпретацията на киберзаплахите, киберотбраната и други елементи на киберсигурността между информационните и индустриалните системи. Изследванията, проведени за оптимизиране и интелектуализация на обучението по киберсигурност, ясно показват, че има определени специфики и особености при въздействието на киберзаплахите, както и при адекватното им реагиране в информационните системи.

Г7.10. Анализ на принципите и критериите за сигурна разработка на софтуер

Софтуерните приложения обикновено се разработват с помощта на езици за програмиране от високо ниво, които сами по себе си могат да имат уязвимости в сигурността. В тази статия са представени преглед и анализ на стандартите за развитие на сигурността на софтуера и най-добрите практики, както и е направено сравнение на езиците за програмиране от позицията на сигурността на кода с цел да се гарантират поверителността, целостта и достъпността на информационните системи.

Г7.11. Възможности за подобряване на качеството на обучението по киберсигурност чрез прилагане на методи на изкуствения интелект

|Разгледани са международните изисквания и стандарти в областта на образованието по киберсигурност и опитите за подобряване на образованието чрез въвеждане на динамични принципи и персонализация в учебната програма, реализираща адаптивни системи за обучение, управлявани чрез методите на изкуствения интелект.

Г7.*12. Киберсигурност: заплахи и предизвикателства*

В тази статия са разгледани и обобщени най-популярните и успешни средства за защита, използвани от организации. Предлагат се препоръки и политики за мрежова и информационна сигурност за университети, изследователски институти, училища и публична администрация. Целта е да се получи общ преглед на кибератаките от цял свят, да се разберат начините на действие и потенциалното въздействие върху бизнеса или лицата, както и контрамерките, които трябва да се предприемат за справяне с рисковете. Проучването се основава на атаки, идентифицирани и проследени през последните три до пет години. На базата на многофакторен анализ на заплахите за киберсигурността и възприемането на военната теория в процедурите за киберсигурност е формулирана нова класификация на етапите на киберзащитата и класове задачи, които могат да се решават с помощта на методите на изкуствения интелект.

Г 7.13 Препоръки относно избора на методи за изкуствен интелект за повишаване на киберсигурността

Анализирани са и са сравнени възприема следния подход за анализиране и сравняване на различни методи на изкуствен интелект: комбиниране на основен критерий (или набор от основни критерии) с допълнителни критерии. За тактическия кибер-интелект са избрани: максимална производителност (т.е. ефективност на откриване, комбинирана с ниво на производителност) и минимален процент на фалшиви аларми, а като допълнителни критерии: гъвкавост за използване в различни среди; генерична методология; скоростта на обработка, необходима за анализиране на съдържанието на пакета, за да се изключи загубени пакети. Проведени са експерименти, при които основният метод на мултиагентна система, съставена от самообучаващи се стационарни агенти, беше допълнен с обучение с подкрепление (RL) и размити множества (FS), за да се определи дали агентите да се научат да категоризират нормалната и необичайна дейност в мрежата. Направени са препоръки за избор на методи на изкуствен интелект при различните фази на киберзащитата.

Г7.14. *Анализ на манипулативността на редундантет робот-манипулатор*

Увеличеният брой приложения на роботизираните системи в живота на човека води до необходимостта от възлагане на по-сложни задачи на такива системи. Редундантността на роботизираната конфигурация повишава производителността и прецизността на изпълнение на възложените задачи. Направен е анализ на характеристики като ъгъл на обслужване и коефициент на манипулативност като важна стъпка от проектирането на роботизирани системи. Изследван е планарен роботизиран манипулатор с ограничен ъгъл на съединението, който има кинематично редундатна конфигурация по отношение на равнинното движение в работното му пространство. Оценен е коефициентът на манипулативност и стойностите на сервизния ъгъл за всяка точка от работното пространство. Чрез тази оценка могат да бъдат намерени ъглите на ставите с най-голяма манипулативност. Експериментите потвърждават, че анализът на манипулативността може да покаже дали избраната конфигурация е приложима за задачата, която ще бъде възложена на робота. Анализът на коефициента на манипулативност може да се използва при проектиране на стратегии за управление и планиране на траектория за среди с препятствия и предоставя полезна информация за зоните, за които се очаква роботът да може да

поддържа по-високи скорости на ставите или да устои на по-голяма сила, а също така илюстрират оптималната конфигурация на ъгъла на ставите за избрани позиции на хващача.

Г7.15. ***Анализ и експерименти с 3D отпечатан крачещ робот за подобряване преодоляване на препятствия чрез катерене***

Изследвани са възможните размери на крачещ робот чрез подобрения на дизайна и експерименти. Представена е оригинална концепция за проектиране на крачещ робот с минимален брой двигатели. Определят се геометрични и силови ограничения за преодоляване на препятствие и условията за поддържане на статична устойчивост. Експериментите за преодоляване на вертикално препятствие се провеждат с 3D принтиран модел. Използват се 3D принтирани крака на роботи с различни форми и материали. Резултатите от експериментите са представени графично в проценти на успех спрямо базов модел. В това изследване е въведен безразмерен индекс за сравнение на височината на преодоляното препятствие и размерите на робота. Позволява обективно да се сравнят възможностите за преодоляване на препятствия между различни видове мобилни роботи. Направени са изводи и насоки за подобрения на дизайна.

Г7.16. ***Изследване на сигурни мобилни агенти като инструмент в системите за откриване на проникване***

Разработени са различни сценарии, свързващи различни области на изкуствения интелект със система за откриване на проникване (IDS). Разработени са няколко приложения за наблюдение на мрежовото поведение на различни видове атаки и тяхното правилно откриване. Един от основните експерименти беше извършен в областта на технологиите, базирани на мобилни агенти и тяхната комбинация с други видове методи от изкуствения интелект като инструмент за нови решения за информационна сигурност. Идеята е да се предложат гъвкави и ефективни решения на проблем, който е труден за справяне с конвенционалните подходи.

Г7.17. ***Нови подходи при изследването и класифицирането на кибер заплахи на базата на прилагането на методи на изкуствен интелект***

Изследванията и практиката на внедряването на методи от изкуствения интелект за киберзащита показват, че няма достатъчно универсален метод, който да е достатъчно ефективен. Извършен е цялостен анализ на най-съвременните подходи за разследване на киберзаплахи, за да реши проблема със създаването на критерии за избор на най-подходящите методи за изкуствен интелект за потенциално разпознаване на модел на атака и да се разработят модели за активна киберзащита. Изследвани са над 40 вида заплахи (някои с няколко подвида) по отношение на тяхното развитие, ниво на въздействие и сложност, усъвършенстване, наличност и т.н. Резултатите от този избор могат да бъдат формулирани по следния начин: а) основни критерии: максимална ефективност и минимален процент фалшиви аларми; б) допълнителни критерии: гъвкавост за използване в различни среди; генерична методология; скоростта на обработка, необходима за анализиране на съдържанието на пакетите, за да се изключат загубени пакети. Прилагането на тези критерии води до следния избор на методи за изкуствен интелект: а) в случай на тактическо киберразузнаване - мрежа от самообучаващи се мултиагентни системи; б) в случай на оперативно киберразузнаване, методът Echo State Network (ESN) с Reservoir Computing за обучение; в) в случай на справяне с инциденти - така нареченото подсилващо обучение (RL).

Г7.18. ***Един метод за мрежова киберсигурност, базиран на изкуствен интелект***

Разработени са и са внедрени сценарии за тестване, за да се провери и оцени ефективността на архитектурата на многоагентна система от самообучаващи се агенти като основен метод за киберзащита на телекомуникационни мрежи, като идеята е да експериментира и надгражда основния метод с друг метод на изкуствен интелект, за да се повиши ефективността .

Експериментите потвърждават, че системата отговаря на изискванията на спецификациите. Модулът NP успява да характеризира нормалното поведение на TCP\IP протокола и да открие повечето атаки, насочени към засягане на заглавката на пакета с висока точност и в реално време. Освен това прилагането на мултиагентна технология при проектирането и внедряването на предложената система, осигурява по-гъвкави и мащабируеми функции и преодолява проблемите с претоварването на мрежовия трафик.

Г7.19. *Подобряване на ефективността на IDPS чрез използването на хибридни методи от изкуствен интелект*

Проучени са размита логика, обучение за валидиране и многоагентни технологии от изкуствен интелект за създаване на система за откриване и предотвратяване на атаки. Създаден е концептуален модел, тестван в лабораторна среда с използване на софтуер за симулация с отворен код, за да се провери и оцени ефективността на предложената хибридна интелигентна система. Поради факта, че се основава на симулации и в момента на експеримента зависи от данни за обучение, конвергенцията не е гарантирана.

Г7.20. *Алгоритъм за преодоляване на препятствия за мобилни роботи*

За да се постигне автономна работа на мобилните роботи в ежедневната жизнена среда и да се постигнат усъвършенствани когнитивни функции на интелигентността на роботите, от тях се изисква да извършват сложни движения, като се вземат предвид местоположението на околните статични обекти, движението на мобилните обекти и постигане на предварително поставената цел като се избягва сблъсък със статичните и динамични обекти в средата. Анализирана е комбинацията от алгоритми за планиране на траектория и следването ѝ, избягване на препятствия, избор на маневра, генериране на най-добрата траектория, реципрочни техники за избягване на сблъсък, алгоритми на теорията на игрите за минимизиране на времето до сблъсъка, вземане на решения и разбиране на ситуацията, оценка на риска, комуникация. Използването на дълбоки (DNN) и рекурентни невронни мрежи (RNN) позволява да се реализират изчислителни модели, които позволяват интегрирането на сензорно-моторни времеви серии от данни и самоорганизирането на мултимодални представяния за поведение на обектите в динамичната среда, в която се намира роботът.

Г7.21. *Няколко модела за сигурност, базиран на мултиагентни системи*

Статията представя модел за IDS, където мултиагентните системи и изкуственият интелект са приложими чрез прости модели в реално време, конструирани в лабораторна среда. Целта на предложената система е да защити мрежовите сървъри, точката за достъп до Интернет и отделните хостове срещу атаки и злонамерен софтуер, без да разчита на структура на база данни. Предлаганата система работи в среда на Microsoft Windows и защитава критичните обекти на операционната система, като защитава и протоколите на мрежово ниво, особено TCP, ICMP и UDP. Предложеният модел се състои от две основни мултиагентни рамки – базирана на хост система за наблюдение и система за наблюдение на мрежов шлюз (частично базирана на правила). Предимствата на предложената система са защита срещу атаки и зловреден софтуер, премахване на фалшиви аларми, откриване в реално време, ранно откриване на атаки, просто изграждане, влизане и докладване.

Г7.22. *Адаптивни техники за оптимизация за интелигентна мрежова сигурност*

Разгледани са принципите на няколко техники за адаптивна оптимизация за интелигентна мрежова сигурност – размита логика, Генетични алгоритми, Q-обуение, Обучение с подкрепление, Теория на игрите и един нов подход за адаптиране на многоагентно базирано размито обучение с обучение с подкрепление. Това са теоретичните

основи за проведеното изследване на техники за повишаване на мрежовата сигурност. В резултат на направените анализи се предлага сътрудничество между различните подходи. Специално внимание се обръща на обучението с подкрепление и размитата логика, които са методите, избрани за нашите основни и бъдещи изследвания.

Г7.23. ***Интелигентен метод за прогнозиране чрез изкуствени невронни мрежи***

Представени са методи и инструменти за краткосрочно прогнозиране на финансови операции, използващи изкуствени невронни мрежи. Направен е анализ на чувствителността на система с невронна мрежа, която се използва за краткосрочно прогнозиране на движението на цените на акциите. Разработената система е със самоопределяне на оптималната топология на невронната мрежа, поради което тя става по-гъвкава и по-точна.

Г7.24. ***Приложение на невронни мрежи във финансовата сфера***

Представени са експерименталните резултати от разработен модел на невронна мрежа за прогнозиране на посоката на движение на финансови данни с една стъпка напред. Архитектурата на невронната мрежа използва четири различни технически показателя, които се основават на суровите данни и текущия ден от седмицата. Методът на обучение е алгоритъм с обратно разпространение на грешката. Слабото звено в използването на невронни мрежи за прогнозиране на финансовите пазари е големият брой възможни изходи, които затрудняват обучението на системата. Посочени са факторите, които оказват значително влияние върху ефективността на невронната мрежа: избор на входни променливи, предварителна обработка на данните и архитектура на невронната мрежа.

Г7.25. Оценяване на отворени данни

Подробно е разгледано качеството на отворените данни, като е представена методологията за оценката им. Представен цялостен преглед на установени методологии за оценка на качеството на данните;маркира разликите между тези подходи в различни измерения; посочени са и са сравнени методите за оценка на качеството; свързани различни подходи със съответните индикатори; дефинирани инструменти, подходящи за всеки подход, класифицирани по тип данни, класиране на автоматизация и необходимо ниво на оперативни умения на потенциалните потребители. Констатациите, направени от Оценката на отворените данни, са от съществено значение при избора на апробационна технология за динамичен референтен модел на българското електронно правителство.

Г7.26 Адекватен отговор на новите предизвикателства пред киберсигурността чрез методите на изкуствения интелект. Приложения в бизнеса и икономиката.

Когато става въпрос за бъдещето на информационната сигурност, ИИ изглежда като много обещаващо поле за изследване, което се фокусира върху подобряването на мерките за сигурност в киберпространството. Изследван е автономен агент, който може да действа независимо в непозната среда и да повишава своята компетентност. Предложената система на базата на такъв автономен агент успява да открива атаки и злонамерени код, който е насочен към защитената система с висока точност и в реално време.

IV. СПИСЪК НА ПУБЛИКАЦИИ и РЕЗЮМЕТА - ***Показател Г8***:

Списък на научните публикации в нереферирани списания с научно рецензиране или в съвременни български научни издания с научно рецензиране от Националния референтен списък

№	Заглавие на публикация
Г8.1	Д.Авишай, **Г. Павлова**, Академично обучение по интелигентно инженерство, подготовка на инженерни кадри за четвъртата индустриална революция Автоматизация на дискретното производство, бр. 4, юли 2022, с. 22-26, ISSN 2682-9584 MNTK ADP BG (tu-sofia.bg)
Г8.2	Д. Авишай, В. Павлов, **Г. Павлова,** Дистанционното обучение във висшето инженерно образование - лекции, лабораторни упражнения и изпити, Автоматизация на дискретното производство, бр.3, юли 2021, с. 25-29, ISSN 2682-9584 MNTK ADP BG (tu-sofia.bg)
Г8.3	G. Tsochev, R.Trifonov, O.Nakov, S. Manolov, **G. Pavlova**, Mobile agents in Intrusion Detection Systems: Advantages and Disadvantages, WSEAS Transactions on Information Science and Applications, Vol 17, 2020, pp. 61-68, E-ISSN: 2224-3402, DOI: 10.37394/23209.2020.17.7
Г8.4	G.Tsochev, R. Trifonov, O. Nakov, S. Manolov and G. Pavlova. Some Recommendations for the Implementation of GDPR at the University, International Scientific Conference Computer Science'2020, Velingrad, Bulgaria, October 18th – 21th, 2020,p. 188-194, ISBN: 978-619-167-433-6
Г8.5	R. Trifonov, O. Nakov, S. Manolov, G.Tsochev and **G. Pavlova,** A New Approach to Cyber Security Policy Development Using Artificial Intelligence Methods International Scientific Conference Computer Science'2020, Velingrad, Bulgaria, October 18th – 21th, 2020,p. 195-202, ISBN: 978-619-167-433-6
Г8.6	R. Trifonov, R. Yoshinov, S. Manolov, G. Tsochev and **G. Pavlova**, Artificial Intelligence methods suitable for Incident Handling Automation, MATEC Web of Conferences, Vol 292, 2019, 23rd International Conference on Circuits, Systems, Communications and Computers (CSCC 2019), Athens, July 14-17, 2019, eISSN: 2261-236X, https://doi.org/10.1051/matecconf/201929201044
Г8.7	Р. Трифонов, Г. Павлова, Г. Цочев .Проблеми на колаборативната работа на хора и роботи, сп. Автоматика и информатика, 3, 2019, с. 17-23, ISSN 0861-7562, https://sai-bg.com/wp-content/uploads/2020/10/AI-3-2019.pdf
Г8.8	R. Trifonov, S. Manolov, G. Tsochev, **G. Pavlova.** Examination of the cyber threats focused on choise of adequate cyber intelligence methods, Communication & Cognition (C&C), 52, 1-2, 2019, p. 45-58, ISSN 0378-0880 (https://www.lotuswebtec.com/nl/vorige-nummers-c-c)

Г8.9	Ivan Chavdarov, Roumen Trifonov, **Galya Pavlova**, New Innovative Approaches in Robotics, Computer and Communications Engineering, Vol. 12, No. 1/2018, p. 18-27, ISSN 1314-2291
Г8.10	R. Trifonov, S. Manolov, G. Tsochev, **G. Pavlova,** Artificial Intelligence Methods Suitable For Operational Cyber-Threat Intelligence, "Intelligent Systems and Applications" of the journal Communication & Cognition, volume 51, No. 3-5, 2018 p.57-72, ISBN 004-232-8, ISSN 0378-0880 https://www.lotuswebtec.com/nl/vorige-nummers-c-c
Г8.11	Chavdarov, I., R. Trifonov, **G. Pavlova**, Innovative Technologies and Materials in Robotics, International Scientific Conference Computer Science'2018. Kavala, Greece, 13-15 September 2018, p.54-60, ISBN: 978-619-167-177-9, http://www.conf.cceng.eu/_eProceeding/pdf/page_54.pdf
Г8.12	R.Trifonov, G. Tsochev, R. Yoshinov, S.Manolov, **G. Pavlova**, Conceptual model for cyber intelligence network security system, International Journal of Computers, Volume 11, 2017, ISSN: 1998-4308, pp. 85-92, https://www.naun.org/main/NAUN/computers/2017/a302007-067.pdf
Г8.13	R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov**, G. Pavlova**, Increasing the level of network and information security using artificial intelligence, Fifth Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2017, 2-3 September, 2017, Zurich, Swiss, ISBN: 978-1-63248-131-3, doi: 10.15224/ 978-1-63248-131-3-25

Г8.1. ***Академично обучение по интелигентно инженерство, подготовка на инженерни кадри за четвъртата индустриална революция***

В статията се разглеждат методологиите на обучение на интелигентното инженерство. За да добият дипломираните инженери качества, подпомагащи прилагането на технологиите на четвъртата индустриална революция. Разгледани са основните дисциплини, които трябва да бъдат изучавани, използването на изкуствения интелект при обучението и опасностите от директното му прилагане.

Г8.2. ***Академично обучение по интелигентно инженерство, подготовка на инженерни кадри за четвъртата индустриална революция,***

Разглежда се въвеждането на дистанционно обучение във висшето инженерно образование. Предлага се дозиране на съдържанието в учебните програми за запазване на висока концентрация на възприятието на обучаемите. Основната цел е и при тези условия да се гарантира. подготовка на креативно мислещи специалисти. Тезата е развита за трите форми на обучение и оценка във висшето образование - теоретични лекции, лабораторни упражнения и установяване на придобитите знания чрез изпити. Също така е разгледано и хибридно обучение, като вид приложена алтернатива.

Г8.3. ***Мобилни агенти в системите за откриване на проникване: предимства и недостатъци***

Представено е използването на мобилни агенти като инструмент за нови видове решения за информационна сигурност. Предлагат се гъвкави и ефективни решения на проблем, който е труден за справяне с конвенционалните подходи, тъй като разпределеният характер на мобилните агенти прави по-трудно заобикалянето или деактивирането на тестовете за сигурност, отколкото при централен монитор или базиран на хост подход за проверка на сигурността. Мобилните агенти са подходящи за приложения за управление на мрежата в хетерогенна среда

Г8.4. ***Препоръки за прилагане на GDPR в университета***

Съвременното информационно общество, заедно с прилагането на новите технологии, налага нови изисквания към защитата на личните данни и променя разбирането за „неприкосновеност на личния живот“. Това води до необходимостта от постоянно актуализиране на прилаганите мерки за защита на личните данни в съвременните информационни системи. Пробив в системата може не само да навреди на самия потребител, но може да доведе и до загуба на доверие от компанията, отговорна за самите данни. Регламентирани са основните задачи по защита на личните данни университета.

Г8.5 ***Нов подход към разработването на политика за киберсигурност с помощта на методи на изкуствен интелект***

Бързото развитие на приложенията за изкуствен интелект и по-специално на автономните агенти в областта на киберсигурността засилва необходимостта от координиран подход и насоки за тяхното създаване, проектиране и развитие. създаването на политика е итеративен процес, включващ последователни цикли от следните стъпки: оценка на риска, предвиждане на мерки за намаляването му, оценка на тези мерки, оценка на ръководството за осъществимостта и целесъобразността на бъдещите разходи. Анализирани са ограниченията при внедряването на системи от автономни самообучаващи се агенти, тъй като поведението им не може да бъде еднозначно определено от техния софтуерен код. Тяхното поведение понякога е непредвидимо и е резултат от комбинация от техния софтуер, тяхното обучение и тяхното възприемане на света около тях.

Г8.6. ***Методи на изкуствения интелект, подходящи за автоматизация на обработката на инциденти***

Анализирана е способността да се проследи статуса на инцидент и да се комбинира събраната информация, резултати от изследвания и информация за предприетите действия. Предложен е алгоритъм за подобряване на прогнозния модел. Проведен е експеримент за прилагане на методите на изкуствения интелект с контролирано обучение в оперативното киберразузнаване, които показват, че най-важната част от решаването на класификационната задача е да се намерят характеристики, които адекватно отразяват обективните зависимости от статуса на класификация. Тъй като последствията от инцидента пряко зависят от скоростта на процеса на обработка на инциденти, основната цел на различните форми на автоматизация е да се сведе до минимум времето за справяне с инцидента.

Г8.7. ***Проблеми на съвместната работа на хора и роботи***

Съвместните дейности на хора и роботи са твърде много по вид и характер, затова е направено типизиране не взаимодействието. Показани са рисковете, които трябва да бъдат управлявани от системите с изкуствен интелект по време на проектирането на роботите и производствените процеси с цел безопасна съвместна работа между хора и роботи. Три са основните въпроси, които трябва да се имат предвид когато се говори за регулиране на ИИ: Какво (обектът на регулиране); защо (причините, поради които са налага да се вземат мерки за регулирането и необходимо ли е то) и направленията, методите и формите на регулиране. Трябва да се обърне внимание на регулирането на изпълнителния, автономния и основания на човешкото поведение ИИ.

Г8.8. ***Изследване на киберзаплахите, насочено към избор на адекватни методи за киберразузнаване***

Изследвани са методите за извършване на кибер атаки и са предложени нови подходи за идентифицирани на заплахите, анализ на пораженията и е направена класификация на заплахите. Тази класификация е предпоставка за избор на методи от изкуствения интелект за киберзащита. Анализите показват, че мултиагнтна система е подходяща в случай на тактически интелигентни кибератаки, а рекурентни невронни мрежи за случаите на операционни интелигентни кибератаки.

Г8.9. ***Нови иновативни подходи в роботиката, компютърното и комуникационното инженерство***

Разгледани са новите иновативни подходи и предизвикателствата на съвременната роботика, както и нови материали и технологии, които могат да бъдат използвани за намиране на нови конструктивни решения, за подобряване на сцеплението, за да се увеличи статичната стабилност на робота и създаването на нов тип директно сглобени кинематични съединения със сложна форма. Направено е сравнение на традиционните методи на производство, 3D и 4D технологиите за печат по отношение на цена, скорост, дизайн и качество. Предложена е систематизация на нови функции, които предоставя технологията за 3D принтиране и са потърсени области за тяхното приложение в моделирането на роботи.

Г8.10 ***Оперативно откриване на кибер-заплахите чрез методи на изкуствения интелект***

Формулирани са основните характеристики на киберзаплахите. Идентифицирането и извличането на добри характеристики от сигналите е решаваща стъпка, защото в противен случай алгоритъмът за класифициране ще има проблеми с идентифицирането на класа на тези характеристики, т.е. поведенческото състояние на възможния противник. Направен е анализ на методи на изкуствения интелект, които се прилагат за осигуряване на мрежова и информационна сигурност. Направен е извод, че активността и изходящият трафик в мрежата на предполагаемия противник е основният източник на информация за изграждане на поведенческия му модел трябва да се изгради и оптимизира ансамбъл от класификатори, базирани на обучени модели, които да се използват за оценка на поведението.

Г8.11. ***Иновативни технологии и материали в роботиката***

Направено е сравнение на различни технологии за 3D печат и са изследвани нови материали, които могат да се използват за намиране на нови конструктивни решения в роботиката. Това дава възможност за получаване на детайли от разнородни материали и нови качества на съединенията и манипулативността на роботите. Въз основа на проучването на технологиите и материалите за 4D и 3D печат ще бъдат избрани подходящи дизайнерски решения за създаване на единици с изключително сложна форма, които да бъдат внедрени в така роботи, разработени от екипа.

Г8.12 Концептуален модел на интелигентна система за сигурност на мрежата

Разгледани са някои от приложенията на методи на изкуствения интелект – размита логика, генетични алгоритми, Q-обучение и др. Разработен е нов подход за адаптиране на многоагентно базирано размито обучение с подкрепление. На тези теоретични основи е създаден концептуален модел на колаборативна интелигентна IDPS система, състоящ се от три слоя, с който да се направи изследване на техники за повишаване на мрежовата

сигурност. Мениджмънта на знанията позволява да се характеризират аномалиите в поведението като множество от свързани концепции.

Г8.13 Повишаване нивото на мрежовата и информационната сигурност с помощта на изкуствен интелект

Представени са и са сравни различни методи на изкуствен интелект (невронни мрежи, изкуствена имунна система, размита логика и размити множества, интелигентни агенти) за борба с престъпността в киберпространството или по-скоро приложението им в системи за откриване и предотвратяване на проникванията (IDPS).

Дата: 23.01.2022 Подпис:……

/гл. ас. д-р инж. Галя Павлова /