РЕЗЮМЕТА НА НАУЧНИ ТРУДОВЕ

на гл. ас. д-р инж. Александър Христов
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: „Компютърни системи, комплекси и мрежи“,
обявен в ДВ брой 101 / 27-11-2025

I. ОБЩА ХАРАКТЕРИСТИКА НА НАУЧНИТЕ ТРУДОВЕ

Гл. ас. д-р инж. Александър Христов, представя за участие в конкурса 1 монографичен труд (Показател В3) и 16 публикации (Показатели Г7 и Г8). Реферирани и индексирани в Scopus и/или Web of Science са 12 публикации. Останалите 4 са публикации в нереферирани списания с научно рецензиране или в съвременни български научни издания с научно рецензиране от Националния референтен списък.

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

Александър Христов*, „СЪСТОЯНИЕ И ПРОБЛЕМИ НА ИНТЕРНЕТ НА НЕЩАТА: СВЪРЗАНОСТ, ПРИЛОЖЕНИЕ И СИГУРНОСТ“, ТУ-София, 2025, България, ISBN 978-619-167-575-3*

Настоящата монография има за цел да представи в систематизиран вид резултатите получени през последните няколко години относно конкретни проблеми на Интернет на нещата. Разглеждат се принципите, организацията и особеностите при симулиране на мрежовата свързаност, приложението и сигурността на Интернет на нещата. Дефинират се основните термини и понятия, както и техниките и технологиите свързани с работата им. Описват се характеристиките на радиоканала, типа модулация и мултиплексиране на сигнала, методите за достъп до средата и др. техники, използвани в съвременните WLAN, 5G и 6G мобилни комуникационни системи..

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

1. Hristov A., Trifonov R., Hristov V. A Cyberattacks detector with logistic regression module, Proceedings of the 11th International Scientific Conference COMPUTER SCIENCE, 18 – 20 September 2023, Sozopol, Bulgaria, DOI: 10.1109/COMSCI59259.2023.10315802

2. Hristov A. Using Python for development of an application for building and experimenting with GPSS simulation models, Proceedings of the 31st scientific conference "TELECOM 2023", 16 – 17 November 2023, Sofia, Bulgaria, DOI: 10.1109/TELECOM59629.2023.10409696

3. Hristov A. et al. Developing and experimenting simulation model of DDoS attacks in IIoT networks using Python, Proceedings of the 31st scientific conference "TELECOM 2023", 16 – 17 November 2023, Sofia, Bulgaria, DOI: 10.1109/TELECOM59629.2023.10409747

4. Hristov A. Simulation of Cookie Poisoning network attacks, Proceedings of the 59th International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2024, July 1-3, 2024, Sozopol, Bulgaria, DOI: 10.1109/ICEST62335.2024.10639772

5. Hristov A., V. Hristov, Investigation of time for conducting a successful DDoS attacks in IIoT network, Proceedings of the 12th International Scientific Conference COMPUTER SCIENCE, 13 – 15 September 2024, Sozopol, Bulgaria, DOI: 10.1109/COMSCI63166.2024.10778501

6. Hristov V., G Matsinski, A. Hristov, Windows application for calculation of Markov's Chains characteristics, Proceedings of the 12th International Scientific Conference COMPUTER SCIENCE, 13 – 15 September 2024, Sozopol, Bulgaria, DOI: 10.1109/COMSCI63166.2024.10778525

7. Hristov A. Development of a System for Monitoring Hardware Metrics, Proceedings of the 32nd scientific conference "TELECOM 2024", 21 – 22 November 2024, Sofia, Bulgaria, DOI: 10.1109/TELECOM63374.2024.10812314

8. Hristov A. Development of laboratory exercise "Cybersecurity of IIoT protocols", Proceedings of the 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2025, Ohrid, N. Macedonia, June 26-28, 2025, DOI: 10.1109/ICEST66328.2025.11098378

9. Hristov A. Creating an Environment for Software-Defined Network Simulations with Mininet and Open Network Operating System, Proceedings of the 13th International Scientific Conference on Computer Science (COMSCI), 13 – 15 September 2025, Sozopol, Bulgaria DOI: 10.1109/COMSCI67172.2025.11225217

10. Hristov A. Creating a Virtual Private LAN Service with Mininet and Open Network Operating System, Proceedings of the 13th International Scientific Conference on Computer Science (COMSCI), 13 – 15 September 2025, Sozopol, Bulgaria DOI: 10.1109/COMSCI67172.2025.11225227

11. Hristov, A. Development of a Smart Parking Clamp System, Proceedings of the 33rd National Conference with International Participation (TELECOM), 20-21 November 2025, Sofia, Bulgaria, DOI: 10.1109/TELECOM66943.2025.11304106

12. Hristov, A., I. Garnizov, R. Yoshinov, Development of a Network Traffic Monitoring System, Proceedings of the 33rd National Conference with International Participation (TELECOM), 20-21 November 2025, Sofia, Bulgaria, DOI: 10.1109/TELECOM66943.2025.11304054

1. Cyberattacks detector with logistic regression module

Целта на настоящата статия е да се анализират последните тенденции в откриването на мрежови атаки, насочени към устройства от Интернет на нещата, както и да се предложи комбиниран детектор, базиран на логистична регресия и емоционален модел, използван за откриване на компрометирани IoT устройства.

2. Using Python for development of an application for building and experimenting with GPSS simulation models

Настоящата статия има за цел да предложи приложение с отворен код и графичен потребителски интерфейс за симулиране на модели, създадени с General Purpose Simulation System (GPSS). Приложението има следните функционалности: отваряне на GPSS файл, въвеждане или редактиране на модели директно в прозореца на редактора за GPSS модели, експериментиране GPSS модели и показване на резултатите на екрана.

3. *Developing and experimenting simulation model of DDoS attacks in IIoT networks using Python*

Изследван е векторът на разпределени атаки за отказ от обслужване (DDOS) върху програмируеми логически контролери (PLC) в автоматизирана система за управление на технологични процеси и е разработен симулационен модел за определяне на вектора на DDOS атака върху PLC в IIoT мрежа, използвайки Python. Предложеният симулационен модел може да се използва за прогнозиране на времето за провеждане на успешна DDoS атака, което позволява да се оцени максималното време за реакция на защитните системи.

4. *Simulation of Cookie Poisoning network attacks*

Целта на статията е да се разработи симулационен модел за мрежови атаки с „отравяне“ на бисквитки (Cookie Poisoning). Анализирани са текущото състояние на проблема, както и някои известни решения. На базата на този анализ са описани етапите на атаката и са предложени методи за изследване, които могат да се използват за разработване на симулационен модел. Дадени са получените резултати при провеждане на числен експеримент и същите са анализирани.

5. *Investigation of time for conducting a successful DDoS attacks in IIoT network*

Цялата тази статия да представи провеждането на натурен експеримент, да се издигнат хипотези за статистически закони за разпределение на времето за провеждане на DDoS мрежови атаки в IIoT. За постигане на целта е необходимо да се решат следните задачи: създаване на концептуален модел, определяне на достатъчен брой итерации, провеждане на натурен експеримент, обобщаване на данните. Приема се хипотезата, че полученото разпределение има конкретно теоретично разпределение.

6. Windows application for calculation of Markov's Chains characteristics

Целта на работата е да се реализира калкулатор с функционалност за определяне на вероятностни оценки на вериги на Марков, който използва итерации за проверка вида на Марковската верига и определяне съответните ѝ характеристики. Разработено е Windows приложение за автоматизиране на изчисленията при определяне на характеристиките на

вериги на Марков. Приложението предлага графичен потребителски интерфейс за въвеждане на данни. Дискутирани са резултатите от експеримент, проведен с разработеното приложение, както и е потвърдена коректността на неговата работа.

7. *Development of a system for monitoring hardware metrics*

В тази статия е разработена система за мониторинг на хардуерни метрики, която събира, съхранява и визуализира данни от различни компютърни системи. За тази цел е изградена инфраструктура, използваща Vagrant за автоматизация на процеси и VirtualBox за хипервизор, Telegraf агентите са конфигурирани да събират данни (индекси) за производителността на хардуера - процесор, памет, дисково пространство и мрежова карта, InfluxDB е инсталиран и конфигуриран да съхранява събраните от хостовете данни, а Grafana е интегриран като инструмент за визуализация и анализ за динамична визуализация на данни.

8. *Development of laboratory exercise "Cybersecurity of IIoT protocols"*

Целта на статията е да представи едно лабораторно упражнение за студентите от специалност „Интелигентни системи в индустрията“ в Техническия университет - София. Това лабораторно упражнение изследва възможностите за провеждане на man-in-the-middle (MITM) атаки в индустриални мрежи при използване на един от най-разпространените протоколи – Modbus. Изследват се възможностите за защита от MITM атаки чрез промяна на комуникационния протокол от Modbus на Secure Modbus.

9. Creating an environment for software-defined network simulations with Mininet and Open Network Operating System

Open Network Operating System - ONOS е мощен инструмент за управление на софтуерно дефинирани мрежи (SDN) с удобен графичен интерфейс. Инструментът Mininet предоставя гъвкава платформа за емулация на мрежови топологии. Съвременните SDN мрежи осигуряват гъвкави и ефективни подходи за изграждане на сигурни и мащабируеми мрежи. Използването на ONOS и Mininet позволява емулация на SDN мрежи без наличие на съответния хардуер. Целта на тази работа е да се обсъдят използваните технологии и процесът на инсталиране на Mininet и ONOS, както и възможностите за създаване и експериментиране с виртуални мрежи.

10. Creating a Virtual Private LAN Service with Mininet and Open Network Operating System

Протоколът Virtual Private LAN Service (VPLS) е най-ефективното и бързо корпоративно решение за изграждане на директна свързаност между отдалечени офиси, разположени в различни части на град или в различни градове в една корпоративна мрежа. Използването на ONOS и Mininet позволява симулиране на VPLS мрежи без наличие на съответния хардуер. Целта на тази работа е да се анализират технологиите, използвани за симулиране на VPLS мрежи, и да се демонстрира процесът на създаване и експериментиране с VPLS в Mininet и ONOS.

11. Development of a smart parking clamp system

Целта на статията е да покаже стъпките в разработването на цялостна система за автоматизиране на процеса на отключване на паркинг скоби. За тази цел в настоящата работа се решават следните задачи: 3D моделиране и прототипиране на скобата, избор на електронни компоненти, проектиране и внедряване на интелигентната скоба и на кросплатформено мобилно приложение, както и изграждане на мрежова услуга.

12. Development of a network traffic monitoring system

Настоящата статия е посветена на разработването на система за мониторинг на мрежовия трафик, която има за цел да осигури гъвкава среда за наблюдение, анализ и визуализация на производителността на компютърните мрежи. Разработената система има следните функционалности: използване на достъпни и енергийно ефективни хардуерни компоненти, прилагане на безплатен софтуер и инструменти с отворен код, възможности за наблюдение в реално време и интеграция между различни софтуерни и хардуерни модули.

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

1. Hristov A., Trifonov R. An application for temperature monitoring of integrated circuits of bitcoin miners, CAx technologies, ISSN 1314-9628, No 7, 2019, pp. 19-24

2. Hristov A. USING LOGISTICS REGRESSION FOR DETECTING CYBERATTACKS IN INTERNET OF THINGS, Bulgarian Journal for Engineering Design, ISSN 1313-7530, No 46, 2023, pp. 5-11

3. Hristov A., Vakadinova V, Trifonov T. Using Arduino for prototyping an alarm system, CAx technologies, ISSN 1314-9628, No 4, 2016, pp. 27-31

4. Hristov A., Trifonov R. Design of system for remote control of electrical appliances over the Internet, CAx technologies, ISSN 1314-9628, No 6, 2018, pp. 43-48

1. *An Application for Temperature Monitoring of Integrated Circuits of Bitcoin Miners*

Настоящата статия е посветена на решаването на актуален проблем за мониторинг на температурата на ASIC интегрални схеми в устройства за добив на криптовалута, и по-специално за устройствата за добив на биткойн - Antminer S9. Устройствата Antminer S9 могат да прегреят, тъй като очакваната им консумация е около 1300 вата с хешрейт 13Th/s, ефективност 93% при околна температура 25^0C. Целта на настоящата статия е да се проектира Windows приложение за мониторинг на температурата на Antminer S9. При проектирането на тази система решени следните задачи: анализирани са подобни технически решения, избрана е безплатна облачна услуга на Google за съхранение на данни за температурата, както и е избран Sikuli като инструмент за автоматизиране на операциите по изпращане на SMS съобщения. Предложена е методология, а стъпките и работата на предложената система за мониторинг на температурата са разгледани подробно.

2. *Using logistic regression for detecting cyberattacks in Internet of Things*

Целта на настоящата статия е да се анализират последните тенденции в откриването на мрежови атаки, насочени към устройства от Интернет на нещата, както и да се предложи комбиниран детектор, базиран на логистична регресия и емоционален модел, използван за

откриване на компрометирани IoT устройства.

3. *Using Arduino for prototyping an alarm system*

Анализирани са възможностите да се използва Arduino за проектиране на прототипи на различни устройства, вариращи от обикновени термостати до самолети. Целта на тази статия е да представи възможностите за използване на Arduino за прототипиране на алармена система. В настоящата статия са анализирани някои от развойните системи Arduino. Въз основа на този анализ е определена конкретната развойна система Arduino, която се използва за проектиране и прототипиране на домова алармената система. Също така са предложени програма на езика С и структура на прототипа на алармената система.

4. *Design of system for remote control of electrical appliances over the Internet*

Целта на тази статия е да представи проектирането и прототипирането на система за дистанционно управление на електрически уреди през интернет, използвайки Arduino. Анализират се някои технологии за дистанционно управление на електрически уреди. Въз основа на този анализ е избрана клиент-сървър архитектура за проектиране и прототипиране на системата. Също така са предложени програмно осигуряване на С и уебсайт за системата.

Дата: 23.01.2025 Подпис:……

/гл. ас. д-р инж. Александър Христов /