Резюмета

на ас. д-р Габриела Димитрова Наскова-Учкунова

за участие в конкурс за заемане на академична длъжност „главен асистент“ по професионално направление 4.6. „Информатика и компютърни науки“

период: 10.2022 – 10.2025

1. Публикация: Naskova, G., Opportunities to Improve the Cybersecurity of Software Applications in 12th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2024 – индексирана в Scopus
    a. Резюме: Изследването се фокусира върху въпроси, свързани с киберсигурността на софтуерните приложения. Представен е обзор на ключови литературни източници за технологични мерки за сигурност за информационни системи и уеб платформи. Критично разгледани и анализирани са мерки на различни етапи от процеса на разработка на софтуер са. В подкрепа на представените концепции е проведено онлайн проучване. Данните от проучването са анализирани и въз основа на това са формулирани изводи и препоръки за софтуерни инженери и системни програмисти.

Ключови думи: софтуерни приложения, уеб приложения, киберсигурност, технологични мерки, програмиране.

    b. Abstract: This study focuses on issues related to the cybersecurity of software applications. A review of key literature sources on technological security measures for information systems and web platforms is presented. Some measures in various stages of the software development process are critically examined and analyzed. In support of the presented concepts, an online survey was conducted. The data from the survey were analyzed, and based on this, conclusions and recommendations for software engineers and system programmers were formulated.

Keywords: software applications, web applications, cybersecurity, technological measures, programming.

2. Наскова, Г.,- Киберсигурност във висшите училища – подходи и добри практики в Сборник с доклади от Национална научно-практическа конференция “дигитална трансформация на образованието – проблеми и решения, оценяване и акредитация”, Русе, България, 2023
    a. Резюме: В следствие от развиващия се свят и европейските директиви за дигитализация на образованието, висшите училища все повече разчитат на цифрови технологи. Това ги изправя непрекъснато пред голям риск от кибератаки.

Осигувянето на защита на крайните станции, включващи лаптопи, настолни компютри и други, се превръща в основна задача от стратегията за киберсигурност на всяко висше училище. ESET Endpoint Protection е популярно решение за защита на крайните станции, използвано широко в различни организации. Разгледани са предимствата и възможностите в университетска среда.

Системата се внедрява лесно, което е решаващо съображение за университетите, които в България често да имат ограничени ИТ ресурси. ESET Endpoint Protection е ефективен при откриване и предотвратяване на редица кибер заплахи, включително зловреден софтуер, фишинг атаки и рансъмуер. Софтуерът колекционира данни за крайните станции и предлага графики за анализ на поведението на всяка.

Ключови думи: дигитализация на образованието, висши училища, киберсигурност, кибератаки, крайни станции, зловреден софтуер, мониторинг и поведенчески анализ, университетска среда.

    b. Abstract: As a consequence of the developing world and the European directives on the digitization of education, higher schools increasingly rely on digital technologies. This puts them at constant risk of cyber-attacks.

Securing endpoints, including laptops, PC, and more, is becoming a core task of any higher school's cybersecurity strategy. ESET Endpoint Protection is a popular solution widely used in various organizations. The advantages and opportunities in a university environment are discussed.

The system is easy to implement, which is a crucial consideration for universities, which in Bulgaria often have limited IT resources. ESET Endpoint Protection is effective at detecting and preventing a range of cyber threats, including malware, phishing attacks and ransomware. The software collects data on endpoints and offers graphs to analyze the behavior of each.

Keywords: digitalization of education, higher education institutions, cybersecurity, cyberattacks, endpoints (endpoint devices), malware, monitoring and behavioral analysis, university environment.