



S8-1.8

Assessment of Cyber Security Maturity for Critical Domains in Republic of Moldova

Au. Buzdugan

Moldova State University, Chisinau, Republic of Moldova

In this paper we present the evaluation results based on the model for cyber security maturity assessment upon the cyber security program development for critical infrastructures (CI) in Republic of Moldova [1]. During last year the healthcare domains has become a target of strategic interest amongst cyber criminals. These events can lead not only to security breaches, but also to safety events that affect human lives. The findings confirm the recommendations of previous case studies on evaluation of cyber security requirements for healthcare inclusive nuclear and radiological domain. Therefore, we classify the results based on the dimensions of the recently developed Model for Cyber Security Maturity Assessment in CI [1]. The proposed model focuses on four primary dimensions: policies and administration, education and training, work environment, cyber risk management. It has been developed with the goal to help decision makers analyze the efficiency of information systems used for cyber risk management. The model is multidimensional and can also show the actual state of cyber security maturity in an organization, fact which was also proven by external reviews. The experimental test of this analysis confirm the applicability of the Model for organizations at different stages of cyber security development, as well as from different domains.