ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „Н. Й. ВАПЦАРОВ“

9002 Варна, ул. „В. Друмев“ 73, тел.052/632-015, факс 052/303-163

“FILII MARIS SUMUS”

РЕЗЮМЕТА
НА НАУЧНИ ТРУДОВЕ

на гл. ас. д-р Валентина Маркова Петрова

представени за участие в конкурс за академичната длъжност „доцент“ в катедра „Информационни технологии“ на факултет „Инженерен“ във ВВМУ „Н. Й. Вапцаров“

- професионално направление: 5.3. „ Комуникационна и компютърна техника“;
- учебни дисциплини: „Информатика“, „Основи на обектно ориентираното програмиране“, „Обектно ориентирано програмиране“ и „Форензика и управление на риска в киберсигурността“;
- публикуван в ДВ брой 47/24.06.2022 г.

За участие в конкурса са представени 12 самостоятелни научни публикации и 1 монографичен труд, разделени по категории както следва:

Монографичен труд	1 бр.
Статии в международни научни списания	3 бр.
Публикации в SCOPUS и WoS	2 бр.
Публикации в Известия на Съюза на учените. Серия „Технически науки“	2 бр.
Доклади от международни научни конференции	3 бр.
Доклади от годишна университетска научна конференция	2 бр.

ПЕТРОВА, В. Аналитичен йерархичен процес за оценка и избор на защитени софтуерни решения. Монографичен труд. 2022, Принтинг хаус, ВВМУ "Н. Й. Вапцаров". ISBN: 978-619-7428-83-4 (print); ISBN: 978-619-7428-84-1 (e-book).

Прилагайки теорията на решенията, монографията реализира изследване за вземане на решение, свързано с осигуряване на защитени софтуерни решения.

Предложени са подход за оценка и избор на решение чрез аналитичен йерархичен процес, йерархичен модел за оценка и избор за вземане на решение, математическа реализация на метода „аналитичен йерархичен процес“ и подход „размити множества с аналитичен йерархичен процес за поставяне в йерархия и класиране на рискови фактори“. Предимството на подхода е, че дава по-малка размитост на изчислените размити тегла.

Осъществено е измерване на несъответствието (неконсистентността) на матрицата за сравнение по двойки с размити елементи. Методът на собствените вектори се използва при аналитичен йерархичен процес, а при прилагане на размита логика логаритмичен метод на най-малките квадрати. Решава се нелинейна оптимизационна задача, която може да се трансформирана в поредица от такива.

В оценката на софтуерния риск в монографията се включат няколко допълнителни етапа свързани с избора на защитени софтуерни решения, обхващащи: определянето на софтуерна среда и предварително посочване на бъдещи възможни злонамерени събития; анализ на последствията от тях; посочване на конкретни мерки за намаляване на софтуерния риск; противодействие срещу възможни атаки; редуциране на уязвимости и предоставяне на софтуерни средства, реализирани в програмен код, за минимализаране на риска от заплахи. Представя се преглед на софтуерните уязвимости и методите за тяхното откриване и предотвратяване.

Моделите за проектиране, разгледани в монографията, предоставят обектно ориентиран дизайн, който осигурява реализация на защитени софтуерни решения чрез използване на различни средства на обектно ориентираното програмиране.

1. ПЕТРОВА, В. Приложение на теорията на размитите множества с аналитичен йерархичен процес за оценка на риска. Годишна университетска научна конференция, НВУ „Васил Левски", 30 юни – 01 юли 2022 г., гр. Велико Търново, стр. 1471 – 1477. ISSN 1314 – 1937, електронно издание: ISSN 2367-7481.

Прилагайки теорията на размитите множества с аналитичен йерархичен процес се установява йерархия от рискови фактори и се определят теглата им. Факторите се анализират количествено и на тази основа се създава метод за контрол и оценка на риска.

Предложеният метод се базира на матрица за анализ на риска в зависимост от количествената оценка на загуби и обективни вероятности. Разглеждайки къде могат да се получат софтуерни проблеми, се прави системен анализ и се предлага оценка от софтуерните експерти, приложена в матрицата на риска. Използват се количествени и качествени данни, за да се извърши цялостна оценка на софтуерния риск на основа на предложените фактори. Създаденият метод за контрол и оценка на риска предлага отделни рискови проблеми за разрешаване, които се измерват чрез лингвистични оценки, базирани на размита логика и се посочва агрегирането към риска да се извърши чрез прилагане на правила, свързани със софтуерната сигурност.

Applying the theory of fuzzy sets with an analytical hierarchical process, a hierarchy of risk criteria is proposed and their weights are specified. The criteria

are analyzed quantitatively and on this basis a multi criteria method for risk control and assessment is created.

The proposed method is based on a risk analysis matrix depending on the quantitative assessment of the loss and objective probabilities. It looks where software problems can be obtained, a system analysis is done, and an assessment from software expert problems is offered, applied in a risk matrix. Quantitative and qualitative data are used to perform a comprehensive software risk assessment based on the proposed factors. The established method of control and evaluation of the offer of individual risk problems for resolution, which are measured by linguistic evaluations based on fuzzy logic and directed to the aggregation to the risk to be carried out by applying rules related to software security.

2. ПЕТРОВА, В. Моделиране на проблеми за вземане на решение. Годишна университетска научна конференция, НВУ „Васил Левски", 30 юни – 01 юли 2022 г., гр. Велико Търново, стр. 1719 – 1725, ISSN 1314 – 1937, електронно издание: ISSN 2367-7481.

В изследването е показан алгоритъм за вземане на решение при многостепенен проблем и са описани последователност от стъпки за достигане на очаквани полезности. Изборът на алтернатива се извършва чрез моделиране, за да може по лесен и интуитивен начин да се разреши сложна многокритериална задача.

В доклада се предлага нов подход, включващ техники за вземане на решения, като създаване на дърво на решенията и реализиране на аналитичен йерархичен процес.

In the study, an algorithm for decision making in a multilevel problem is shown and a sequence of steps to reach expected utilities is described. The choice

of an alternative is done by modeling in order to solve a complex multi-criteria task in a simple and intuitive way.

The paper proposes a new approach involving decision-making techniques such as decision tree creation and the implementation of an analytic hierarchy process.

3. ПЕТРОВА, В. Модел за вземане на решения за киберсигурност. Известия на съюза на учените – Варна, Серия „Технически науки“ – 1’2020, с.48-52, ISSN 1310-5833.

Предложеният модел осъществява проверка на ефективността на приложените мерки за контрол на кибер сигурността, осигурява оценка на кибер риска и изпълнението на кибер защитата.

За определяне на нивата на сигурност се прилага система за оценка на уязвимостта. Основните характеристики, които се разглеждат са конфиденциалност, интегритет и наличност на информацията. При криптиране на данните трябва да се вземе предвид установяване на изискването за конфиденциалност. На устройствата за данни им се дават различни атрибути в зависимост от степента на криптиране. Изискването за наличност е свързано с изтичане на време и претрупване на устройство или приложения, хоствани от устройството. Устройствата, които са част от претрупани клъстери, имат по-ниски изисквания за наличност. Изискванията за интегритет са свързани с точност на данните, които се съхраняват или използват.

The proposed model evaluates the effectiveness of the implemented cyber security control measures, provides an assessment of cyber risk and the performance of cyber protection.

A vulnerability assessment system is used to determine security levels. The main characteristics considered are confidentiality, integrity and availability of information. When encrypting the data, consideration should be given to establishing the confidentiality requirement. Data devices are given different attributes depending on the level of encryption. The availability requirement is related to the timeout and congestion of a device or applications hosted by the device. Devices that are part of congested clusters have lower availability requirements. Integrity requirements relate to the accuracy of data that is stored or used.

4. ПЕТРОВА, В. Приложение на размити множества за вземане на решения. Известия на съюза на учените – Варна, секция „Технически науки“ – 1’2021, ISSN 1310-5833.

В статията се използват математически инструменти за моделиране и управление на несигурни системи, като размити множества и размита логика за моделиране на процеса на вземане на решения. Експертите предлагат своя избор под формата на триъгълни размити елементи, които показват теглата на рисковите фактори.

Предложената техника извлича размити тегла от матрица и след това измерва несъответствието на предложенията, предоставени от вземащите решения, за да се определи индекса на консистенция NI. Стойността на индекса е между 0 и 1. В случай, че е 0 матрицата е напълно консистентна.

The paper uses mathematical tools for modeling and controlling uncertain systems, such as fuzzy sets and fuzzy logic to model the decision-making process. The experts offer their choices in the form of triangular fuzzy elements that show the weights of the risk factors.

The proposed technique extracts fuzzy weights from a matrix and then measures the inconsistency of the proposals provided by the decision makers to

determine the consistency index NI. The value of the index is between 0 and 1. In case it is 0, the matrix is fully consistent.

5. ПЕТРОВА, В. Подход за многокритериално вземане на решение. Международната научна конференция „Съвременни изследвания и технологии за отбраната“, 29 и 30 юни 2021 г., Варна, стр. II-32 - II-38, ISSN 2815-2581.

Изследването предлага йерархична структура, базирана на аналитичен йерархичен процес. Прилага се подход за анализ на процеса на вземане на решения и избор на най-подходяща система за електронно обучение от системи с отворен код, софтуер като облачна услуга (SaaS, Software as a Service) и частни системи. Платформите за електронно обучение трябва да отговарят на определени критерии, подредени по важност, за да бъдат ефективни в предварително определените сценарии, в които ще се прилагат, а също да удовлетворят нуждите на студенти и преподаватели. Тези сценарии се получават от предварителния анализ на реални случаи.

The study proposes a hierarchical structure based on an analytic hierarchy process. An analysis approach is applied to the decision-making process and the selection of the most suitable e-learning system from open source systems, software as cloud (SaaS, software as a service) and private systems. E-learning platforms must meet the service criteria for definition, ranked in importance to be effective in pre-determining the scenarios in which they will be applied and also to meet the needs of students and faculty. These scenarios are obtained from the preliminary analyzes in real cases.

6. ПЕТРОВА, В. Използване на аналитичен йерархичен процес за оценка на киберсигурност. Международната научна конференция „Съвременни изследвания и технологии за отбраната“, 29 и 30 юни 2021 г., Варна, стр. II-75 - II-81, ISSN 2815-2581.

Основната цел на доклада е да се представи приложение на аналитичен йерархичен процес чрез използване на математически изчисления, базирани на предпочитанията на вземащите решения експерти по киберсигурност с помощта на скалата на Саати, известна в научната литература като състояща се от пет прецизни нива и четири средни, описващи интензитет за оценка на киберсигурността.

Резултатите от това проучване дават информация за критериите, които са оценени с най-голяма важност: адаптивност, персонализация и удостоверяване. Адаптивността включва наблюдение на мрежовата сигурност в реално време. Незабавно се осъществяват проверки за заплахи, злонамерен трафик, уязвимости и атаки. Удостоверяването на потребителите е ефективен механизъм, който включва както аспекти за сигурност, така и използваемостта, защото трябва да гарантира безопасност на работата при използване на онлайн услугите и персонализирането на потребителите.

The main objective of the report is to present an application of an analytical hierarchy process by using mathematical calculations based on the preferences of cyber security expert decision-makers using the Saaty scale, known in the scientific literature as consisting of five precision levels and four average, describing cybersecurity assessment intensity.

The results of this study provide information on the criteria rated most important: adaptability, personalization, and authentication. Adaptability includes real-time network security monitoring. Scans for threats, malicious traffic, vulnerabilities and attacks are performed immediately. User authentication is an

effective mechanism that includes both security and usability aspects, because it should ensure safety of operation when using online services and personalization of users.

7. PETROVA, V. Network technologies for e-learning. IV International Scientific Conference "High technologies. Business. Society 2019", 11-14.03.2019, Borovets, Bulgaria. International Scientific Journal Industry 4.0, Issue 2/2019, pages 96-99. ISSN(print) 2534-8582, ISSN(WEB) 2534-997X.

Статията описва разработената от автора среда "Мрежови технологии за електронно обучение" (NTEL) с помощта на предложения модел за описание, структуриране и организиране на онтологично представяне на учебни обекти чрез предоставяне на семантична инфраструктура.

Компонентният модел за мрежови технологии за електронно обучение е разработен на базата на съществуващите стандарти, спецификации и онтологии за създаване, управление, развитие и обмен на учебни обекти, средства и съществуващата теория на дизайна на обучението.

Обсъждат се стратегии и методологии за разработване и внедряване на онтология.

The paper presents an environment "Network technologies for e-learning"(NTEL) using the offered Model for describing, structuring, and organizing the ontological representation of learning objects through providing a semantic infrastructure.

The Component model for network technologies for e-learning was developed on the grounds of the existing standards, specifications, and ontologies for the creation, management, development, and interchange of learning objects and means and the existing instructional design theory.

Strategies and methodologies in ontology development and implementation are also discussed.

8. PETROVA, V. A cybersecurity risk assessment. VI International Scientific Conference "High technologies. Business. Society 2021", 08-11.03.2021, Borovets, Bulgaria. International Scientific Journal Industry 4.0, Issue 1/2021, pages 37-40. ISSN (print) 2534-8582, ISSN(WEB) 2534-997X.

Изследването представя модел за оценка на рисковете за киберсигурността, за да се осигури конфиденциалност, интегритет и достъпност на информацията. Демонстрира се използването на аналитичен йерархичен процес за извършване на оценка на рисковете и приоритизиране им в системите. Прилагайки методология за оценка на риска те се структурират и поставят в йерархия, правят се сравнения по двойки и се изчислява приоритетното тегло, за да се организира тяхното класиране и да се прецени кои от рисковете са най-важни за преодоляване и да се постигне киберсигурност.

The study presents a model for assessing cybersecurity risks to ensure confidentiality, integrity and availability of information. The use of an analytical hierarchy process to perform risk assessment and prioritization in systems is demonstrated. Applying a risk assessment methodology, they are structured and placed in a hierarchy, pairwise comparisons are made and the priority weight is calculated to organize their ranking and assess which of the risks are most important to overcome in order to achieve cyber security.

9. PETROVA, V. A multi-criteria decision making model. VII International Scientific Conference "High technologies. Business. Society 2022",2022, Borovets, Bulgaria. International Scientific Journal Industry 4.0, Issue 1(10)/2022, pages 130-134. ISSN 2535-0005 (print), ISSN 2535-0013 (ONLINE).

В доклада се разглежда многокритериален модел за вземане на решения за оценка на риска за киберсигурността, който може да се използва в различни проучвания, независимо от вида на кибертехнологията, която се оценява. Ползата от оценката на риска е, че тя позволява относително класиране на рисковете, идентифициране на области от особена важност за проучване и количествено определяне на риска.

Използва се дърво на решенията, за да се посочат критичните аспекти на киберсигурността, което допринася да се намалят пропуските в анализите на кибер експертите.

This study proposes a Multi-Criteria Decision Making (MCDA) model for cyber security risk assessment that can be used in a variety of studies, regardless of the type of cyber technology being evaluated. A benefit of a risk assessment is that it allows relative ranking of the risks, identification of areas for particular focus of investigations and quantification of risk. The use of decision tree is suited for identifying critical aspects of a process that have a significant influence on failure and for decision analysis involves risk assessment.

10. PETROVA, V. Development of secure software. X INTERNATIONAL SCIENTIFIC CONFERENCE "TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY". 06-09.06.2022, Borovets, Bulgaria, ISSUE 1 (14), pp. 35-38, ISSN 2535-0315 (Print), ISSN 2535-0323 (Online)

Основната цел на това проучване е да се предложат подходящи инструменти за повишаване на защитата на софтуерните системи от злонамерени атаки. Авторът прилага размита многокритериална теория за вземане на решения за оценка на характеристиките и алтернативите за сигурност на системата. Идентифицирането и оценката на риска е ключов елемент от анализа на софтуерната сигурност.

Преподавателите могат да използват предложения метод при преподаване на дисциплини, свързани с програмиране на защитени софтуерни решения. Реализираната методика за оценка на риска и направените изследвания, свързани със софтуерната сигурност са включени в учебната програма на дисциплината „Форензика и управление на риска в киберсигурността" на специалност „Киберсигурност" в четвърти курс във ВВМУ.

he main objective of this study is to propose suitable tools to increase the protection of software systems against malicious attacks. Analyzes and evaluation of confidentiality, integrity and privacy of the information have been done. The author applies fuzzy multi-criteria decision theory to evaluate system security features and alternatives. Risk identification and assessment is a key element of software security analysis.

Lecturers can use the proposed method when teaching subjects related to programming of secure software solutions. The implemented methodology for risk assessment and the conducted research related to software security are

included in the curriculum of the discipline "Forensics and risk management in cybersecurity".

11. PETROVA, V. Using the Analytic Hierarchy Process for LMS selection. CompSysTech '19: 20th International Conference on Computer Systems and Technologies, June 2019, Ruse, Bulgaria, Pages 332–336, ISBN: 978-1-4503-7149-0. DOI 10.1145/3345252.3345297

Предложен е математически модел на аналитичен йерархичен процес, приложен в подход за сравняване на основата на концепции за характерни оценъчни спецификации на среди за електронно обучение. Анализът се основава на дефинирането на набор от критерии, които са свързани с характеристиките на системите за управлението на електронното обучението.

Резултатите от изследването могат да се използват от експертите и разработчиците на инструменти за електронно обучение за вземане на решения при изграждане на софтуерни системи, реализиране на електронно обучение, за разработване и управление на ресурси, курсове и учебни обекти.

A mathematical model of an analytical hierarchy process is proposed, implemented in a concept-based comparison approach for characteristic evaluation specifications of e-learning environments. The analysis is based on the definition of a set of criteria that are related to the characteristics of learning management systems.

The results of the study can be used by experts and developers of e-learning tools to make decisions when building software systems, implementing e-learning, developing and managing resources, courses and learning objects.

12. PETROVA, V. The Hierarchical Decision Model of cybersecurity risk assessment. 12th NATIONAL CONFERENCE WITH INTERNATIONAL PARTICIPATION "ELECTRONICA 2021", May 27-28, 2021, pages 18-21, ISBN 978-166544061-5 DOI 10.1109/ELECTRONICA52725.2021.9513722

Предложената в доклада оценка на риска за киберсигурността и прилагането и е от съществено значение при създаване на защитени информационни системи. Избраният аналитичен метод повлиява вземането на решения, свързани със сигурността. Посочените критерии представляват оптимални индикатори за бъдещи уязвимости в приложенията.

Процесът на аналитична йерархия комбинира качествени и количествени методи за оценка и осигурява ефективен модел, който се прилага в учебните часове по дисциплините „Основи на обектно ориентираното програмиране" и „Обектно ориентирано програмиране" и може да се използва в дейността на експертите по киберсигурност.

The cybersecurity risk assessment proposed in the report and its implementation is essential in creating secure information systems. The analytical assessment method affects security-related decision-making.

The results of the multi-criteria cyber risk assessment are used to make decisions related to the implementation of specific security measures. The specified criteria are optimal indicators of future application vulnerabilities.

The Analytical hierarchy process combines qualitative and quantitative assessment methods and provides an effective model that is applied in the cybersecurity study programs and can be used in the work of cyber security experts.