EUROPEAN CONFERENCE

Conference Proceedings

IX International Science Conference
«Global scientific area: challenges, achievements, and technological innovations»

November 02 - 04, 2026
Munich, Germany

GLOBAL SCIENTIFIC AREA: CHALLENGES, ACHIEVEMENTS, AND TECHNOLOGICAL INNOVATIONS

Abstracts of IX International Scientific and Practical Conference

Munich, Germany
(November 02 - 04, 2026)

UDC 01.1

ISBN – 979-8-90553-906-0

The IX International scientific and practical conference «Global scientific area: challenges, achievements, and technological innovations», November 02 - 04, 2026, Munich, Germany, 274 p.

Text Copyright © 2026 by the European Conference (https://eu-conf.com/).
Illustrations © 2026 by the European Conference.
Cover design: European Conference (https://eu-conf.com/).
© Cover art: European Conference (https://eu-conf.com/).
© All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted, in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher. The content and reliability of the articles are the responsibility of the authors. When using and borrowing materials reference to the publication is required. Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine and from neighboring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

The recommended citation for this publication is: Hryhorenko T., Chuzhma N., Bazaieva A. Natural food base and its importance in rearing different age groups of common carp. Abstracts of IX International Scientific and Practical Conference. Munich, Germany. Pp. 11-14.

URL: https://eu-conf.com/en/events/global-scientific-area-challenges-achievements-and-technological-innovations/

PHYSICAL CULTURE AND SPORTS		
53.	Пиж'янов В.В., Григор'єв Ю.М. ПОРІВНЯЛЬНИЙ АНАЛІЗ СТРІЛЕЦЬКОЇ ЗБРОЇ В КУРСІ "ОСНОВИ НАЦІОНАЛЬНОГО СПРОТИВУ": АК-74 (АКМ) ПРОТИ М4А1	224
PSYCHOLOGY		
54.	Кудря А.О. КОПІНГ-СТРАТЕГІЇ ВІЙСЬКОВОСЛУЖБОВЦІВ	229
55.	Чауш А.О. СОЦІАЛЬНО-ПСИХОЛОГІЧНІ МЕХАНІЗМИ ВПЛИВУ СТАТУСУ НА СЕКСУАЛЬНУ ПОВЕДІНКУ ТА ВИБІР ПАРТНЕРА	233
SOCIOLOGY		
56.	Kuryazova D.A. PUBLIC RELATIONS IMIJ SHAKLLANTIRISHNING STRATEGIK VOSITASI SIFATIDA	237
57.	Pukhkal O.H., Klykov A. MECHANISMS OF PUBLIC GOVERNANCE: SOCIAL DIALOGUE AND DIGITAL DEMOCRACY	245
TECHNICAL SCIENCES		
58.	Davydova V., Solodovnyk G. MULTI-CRITERIA MODEL FOR SELECTING SOFTWARE TOOLS FOR INFORMATION SYSTEM PROTECTION	252
59.	Rastsvietaiev V. IMPROVING THE ENERGY EFFICIENCY AND OPERATIONAL PERFORMANCE OF OIL PIPELINE SYSTEMS THROUGH INDUCTION HEATING	256
60.	Zaichenko S.V., Trachuk A.R., Kurinniy M.V. METHODOLOGY FOR ACCELERATING THE TRANSITION OF UKRAINE'S POWER SECTOR TO CLEAN TECHNOLOGIES THROUGH THE UTILIZATION AND IMPLEMENTATION OF RENEWABLE ENERGY SOURCES	262

MULTI-CRITERIA MODEL FOR SELECTING SOFTWARE TOOLS FOR INFORMATION SYSTEM PROTECTION

Davydova Viktoriia
Bachelor's Degree Student,
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine

Solodovnyk Ganna
PhD in Technical Sciences, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine

Relevance. The rapid development of information technologies and the growing dependence of organizations on information systems lead to increased requirements for ensuring their cybersecurity [1]. The constantly changing cyber threat landscape, the emergence of new methods of unauthorized access, the improvement of methods for carrying out cyberattacks, and the discovery of new vulnerabilities require continuous revision of approaches to protecting information resources [2].

Additional difficulties arise because the decision maker (DM) responsible for purchasing and implementing software is not always a cybersecurity specialist and may lack sufficient specialized knowledge to objectively assess its protective capabilities. A particular challenge is the need to simultaneously consider multiple criteria, some of which can be expressed quantitatively, while others are characterized by qualitative assessments and require expert evaluation. The criteria may be conflicting, since increasing the level of protection is often accompanied by higher software costs and greater complexity of its implementation and operation.

The presented facts determine the relevance of developing models and methods for identifying the best software alternative for information system protection based on multiple criteria.

The object of the study is the decision-making process regarding the selection of software tools for information system protection.

The subject of the study is models and methods for multi-criteria evaluation and selection of a rational software alternative for information system protection based on a generalized utility criterion.

Problem Statement. The problem is to find the best application for protecting an information system (IS) according to the utility criterion when the decision maker (DM) has several possible alternatives.

The task formulated on the basis of this problem is to determine the best alternative according to multiple criteria, some of which cannot be expressed quantitatively. Thus, when selecting an application for IS protection, it is necessary to consider a set of factors characterizing the level of information system protection, the functional capabilities of the software, as well as the economic and operational characteristics of its use.

To solve this problem, the Analytic Hierarchy Process (AHP) can be used, which makes it possible to transform judgments about the relative importance of different criteria into a linear set of weighting coefficients suitable for ranking alternatives. AHP transforms qualitative factors into quantitative characteristics in three stages: examining the structure of the problem and identifying the most important elements of the hierarchy (i.e., decision-making criteria), determining the relative importance of each element of the hierarchy through pairwise comparisons of their subjective assessments, and comparing the quality assessments of alternatives for each element of the hierarchy [3].

Problem Solution. To evaluate alternative software solutions for information protection, twelve criteria were established and grouped into three categories of factors:

1. Level of protection (F1): effectiveness of malware detection, phishing protection, ransomware protection, response speed to new threats;
2. Functional capabilities (F2): user interface usability, centralized management, impact on system performance, compatibility with operating systems;
3. Economic and operational characteristics (F3): technical support, cost of use, ease of implementation, scalability.

Four software alternatives were selected for comparison:

1. Bitdefender GravityZone, alternative A, which is characterized by a high level of malware detection, advanced protection against modern cyber threats, and centralized management capabilities, but requires significant financial expenditures and appropriate administrator training [4].
2. ESET PROTECT, alternative B, which combines a high level of protection, convenient centralized management tools, and a relatively low impact on information system performance [5].
3. Microsoft Defender for Business, alternative C, which is convenient for implementation in information systems running Windows but depends on the Microsoft infrastructure being used [6].
4. Avast Business Security, alternative D, which provides basic information system protection functions with relatively simple implementation and an understandable user interface [7].

After forming the hierarchy of evaluation criteria and the set of alternatives, we proceed to the stage of determining the relative importance of each element of the hierarchy through pairwise comparisons of their subjective assessments. For this purpose, using Saaty's fundamental scale of relative importance, we construct pairwise comparison tables for each of the three factors, each of the twelve criteria, and each alternative. Based on these tables, we construct the aggregated priority matrix and the aggregated priority vector (Fig. 1).

Priority Aggregation Matrix

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	SUM
A	0.1439	0.0470	0.0856	0.0202	0.0073	0.0477	0.0112	0.0208	0.0085	0.0061	0.0030	0.0104	0.4115
B	0.0811	0.0260	0.0519	0.0112	0.0073	0.0264	0.0208	0.0208	0.0085	0.0112	0.0030	0.0058	0.2735
C	0.0470	0.0260	0.0278	0.0112	0.0135	0.0264	0.0208	0.0112	0.0046	0.0112	0.0055	0.0058	0.2107
D	0.0263	0.0097	0.0146	0.0041	0.0039	0.0098	0.0065	0.0065	0.0026	0.0164	0.0016	0.0021	0.1042

Aggregated Priority Vector	0.4115*A+0.2735*B+0.2107*C+0.1042*D
Highest Priority	0.411548414
The Following Alternative Should Be Selected	A

Figure 1 – Priority Aggregation Matrix
Source of the figure: developed by the authors.

Alternative A (Bitdefender GravityZone) was identified as the best alternative. It should be noted that this conclusion was made on the basis of the authors' subjective preferences regarding the importance of the evaluation criteria and does not constitute a recommendation for selecting information protection software.

The solution was automated using spreadsheet tools. To form the Aggregated Priority Vector, the CONCAT() function was used with references to the last column of the Priority Aggregation Matrix. The Highest Priority was determined using the statistical function MAX(). The final result was obtained using the formula INDEX(A83,MATCH(MAX(N83),N83,0)).

Conclusions. The constant threats of information damage at automated facilities posed by cyber threats require special attention to the selection of appropriate protection tools. Management entities responsible for investing in the implementation of such tools are often not specialists in the field of information protection. Therefore, the task of providing information support for such decisions using scientifically substantiated methods is relevant.

The presented results of automating the solution to the problem of finding the best application for information system protection make it possible to simplify the decision-making process regarding the selection of information protection tools and to take into account the subjective preferences of the decision maker. Further development of this work involves improving the interface and adding graphical data representation.

References

1. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024 // ENISA. 2024. URL: https://doi.org/10.2824/0710888

2. Verizon. 2025 Data Breach Investigations Report // Verizon. 2025. URL: https://www.verizon.com/about/news/2025-data-breach-investigations-report

3. Cabrera J.S., Reyes A.R.L., Lasco C.A. Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach // *Advances in Technology Innovation*. 2021. Т. 6, № 1. С. 31–38. URL: https://ojs.imeti.org/index.php/AITI/article/view/5476

4. Bitdefender. GravityZone Business Security Premium // Bitdefender. URL: https://www.bitdefender.com/en-us/business/products/gravityzone-premium-security

5. ESET. ESET PROTECT Platform // ESET. URL: https://www.eset.com/us/business/protect-platform/
6. Microsoft. Microsoft Defender for Business Documentation // Microsoft Learn. URL: https://learn.microsoft.com/defender-business/
7. Avast. Avast Small Business Solutions Overview // Avast Business Help. URL: https://businesshelp.avast.com/Content/Products/AfB_Antivirus/AntivirusManagement/NewAfBSMBSolutions.htm