ANALYTIC HIERARCHY PROCESS IN THE FIELD OF CYBERSECURITY USING GENERATIVE AI

Dmytro Lande[a] , **Leonard Strashnoy**[b], **Oleg Driamov**[c]

[a] *Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine*
[b] *TCS, Los Angeles, USA*
[c] *GPG, Warsaw, Poland*

Abstract:

The work is devoted to demonstrating and justifying the use of generative artificial intelligence (AGI) systems in the implementation of decision support based on the method of analyzing hierarchies of Thomas Saaty. It is proposed to solve the problem of selecting experts by attracting so-called "virtual experts". The article provides an example of the use of the ChatGPT GSH system in the field of cybersecurity. This approach opens up broad opportunities for the use of GSH systems in decision support.

Keywords: *Generative artificial intelligence, AGI,* analytic hierarchy process, *virtual experts, consistency of criteria and alternatives, weight of criteria and alternatives.*

Introduction

For many years, the Analytic Hierarchy Process (AHP) [1] and the Analytic Network Process (ANP) [2], as its development, have played an important role among expert methods for supporting adoption. decisions. The wider dissemination of these methods has always been hampered by the problem of selecting experts; there were always not enough of them. Right now, when a technological revolution is taking place due to the development of generative artificial intelligence (GII) systems [3], it has become possible to solve this problem with the help of so-called "virtual experts" [4]. This article demonstrates and justifies the use of the ChatGPT GII system [5] specifically for the cybersecurity domain.

Electronic copy available at: https://ssrn.com/abstract=4621732

The implementation of this approach opens up broad opportunities for the use of generative artificial intelligence in decision-support systems in various fields.

Hierarchy Analysis Technique Procedures

The hierarchy analysis method is a structured method for organizing and analyzing complex decisions based on mathematics and psychology. MAI was developed by Thomas Saaty in the 1970s. It provides an approach to quantify the importance of criteria in the decision-making process. Pairwise comparisons conducted by experts are used to assess the relative importance of various factors. The method is based on breaking the problem into smaller parts and presenting it in the form of a hierarchical structure.

The hierarchy analysis technique is a systematic approach to structuring decision problems into a hierarchy or network. Starting with the definition of the main goal at the top of the hierarchy, other elements are placed at intermediate levels. At these intermediate levels, there are criteria that determine the importance of choosing an alternative, and they influence subsequent levels. At the lower level are concrete alternatives.

In its simplest form, a hierarchy can be thought of as a three-level structure with a goal, criteria, and alternatives. This approach helps to systematize and determine the importance of each decision element relative to the others.

After creating the hierarchical structure of a problem in the hierarchy analysis method, the next step is to prioritize the criteria and evaluate each of the alternatives to determine which one is most important.

In the hierarchy analysis method, elements are compared with each other in pairs regarding their influence on the overall characteristic. These pairwise comparisons result in a comparison matrix where each element is compared to the others.

When a task is presented as a hierarchical structure, a comparison matrix is constructed for pairwise comparisons of criteria at the second level relative to the overall goal, which is

Electronic copy available at: https://ssrn.com/abstract=4621732

located at the first level. Such comparisons help determine the importance of each criterion and its impact on achieving the goal.

The same matrices must be constructed for pairwise comparisons of each alternative at the third level, and so on, if the number of levels is more than three. In the simplified example below, only three levels are considered, with alternatives formed on the basis of certain criteria being compared in pairs with respect to the main goal.

To implement MAI using GII to build a hierarchy, and form criteria and alternatives, "virtual experts" are involved, who are assigned appropriate roles, whose responses are taken into account in the ChatGPT GII system.

In this example, the goal is to ensure cybersecurity, therefore, to determine the roles of virtual experts, the ChatGPT GII system is given the following prompt:

► Provide 5 expert roles from whose perspective Cybersecurity issues can be considered

In response to this prompt, the system issues:

Cybersecurity issues can be considered:

1. Cybersecurity Analyst: These experts focus on analyzing and responding to security threats, monitoring network traffic, and identifying vulnerabilities.
2. Ethical Hacker (Penetration Tester): Ethical hackers are cybersecurity professionals who attempt to find and exploit vulnerabilities in systems to help organizations strengthen their security.
3. Network Security Engineer: These experts specialize in securing network infrastructures, implementing firewalls, and ensuring data encryption to protect against cyber threats.
4. Compliance Officer: They ensure that an organization complies with relevant cybersecurity laws, standards, and regulations, reducing the risk of legal issues.
5. Chief Information Security Officer (CISO): This senior executive is responsible for the overall cybersecurity strategy of an organization, including risk management and incident response.

Electronic copy available at: https://ssrn.com/abstract=4621732

Since this solution, according to the authors, corresponds to reality, it is “virtual experts” with these roles that are further used to identify cybersecurity criteria.

Definition of criteria

The criteria represent a separate level of the hierarchy that is being built. The procedure for determining the main criteria for ensuring cybersecurity is considered by repeatedly accessing the ChatGPT system on behalf of various experts, taking into account various answers, and highlighting the most frequently encountered ones (the final list of criteria can, of course, be confirmed by a human expert). Below is a prompt for determining cybersecurity criteria, which is formulated on behalf of the “Cybersecurity Analyst” expert, and accordingly, the response of the ChatGPT system:

► Identify the 5 main cybersecurity criteria from the perspective of a Cybersecurity Analyst

ChatGPT response:

From the perspective of a Cybersecurity Analyst, the five main cybersecurity criteria to consider are:

1. Threat Detection: The ability to identify and detect various types of threats, including malware, phishing attempts, and intrusion attempts, is a fundamental aspect of cybersecurity analysis.
2. Vulnerability Assessment: Evaluate the organization's systems and networks to discover potential vulnerabilities and weaknesses that could be exploited by attackers.
3. Incident Response: Developing and implementing procedures to respond to security incidents and breaches effectively, minimizing their impact and preventing future occurrences.
4. Security Monitoring: Continuously monitoring network traffic, system logs, and user activities to identify anomalies and potential security breaches in real-time.
5. Security Policy Compliance: Ensuring that the organization complies with security policies and industry

Electronic copy available at: https://ssrn.com/abstract=4621732

regulations to maintain a strong security posture and reduce risks.

Summarizing the answers received from all the previously mentioned virtual experts, we obtain the criteria:

- Access control;
- Incident response;
- Security awareness;
- Security policies;
- Threat modeling;
- Vulnerability assessment;
- Encryption.

Defining Alternatives

To determine alternatives (the third level of the hierarchical network), a procedure is implemented to repeatedly contact the ChatGPT system, in which criteria from the list defined earlier are indicated and possible options for its implementation are requested.

Below is a prompt for determining alternatives based on the "ACCESS CONTROL" criterion and the response from the ChatGPT system:

► Name 2 primary alternative solutions for addressing cybersecurity ACCESS CONTROL criteria

ChatGPT response:

Here are two primary alternative solutions for addressing cybersecurity access control criteria:

1. Role-Based Access Control (RBAC): RBAC is a model that assigns permissions and access rights to users based on their roles and responsibilities within an organization. It ensures that individuals have the appropriate level of access for their job functions, reducing the risk of unauthorized access.
2. Attribute-Based Access Control (ABAC): ABAC is a more flexible access control model that takes into account various attributes or characteristics of users, resources, and the environment. It allows for fine-grained control and can adapt access permissions based on dynamic factors, such as time of day or location.

Electronic copy available at: https://ssrn.com/abstract=4621732

As a result of the responses of the ChatGPT system to such prompts, we receive a list of alternatives and, thus, the entire hierarchy shown in Fig. 1:

- Role-based access control (RBAC);
- Attribute-based access control (**ABAC**);
- Security information and event management (SIEM);
- Threat intelligence sharing and collaboration;
- Security awareness training programs;
- Phishing simulation and testing;
- Security policy framework;
- Security policy auditing and compliance tools;
- Attack surface reduction;
- Threat modeling tools;
- Automated vulnerability scanning;
- Manual penetration testing;
- End-to-end encryption (e2e);
- Application layer encryption.

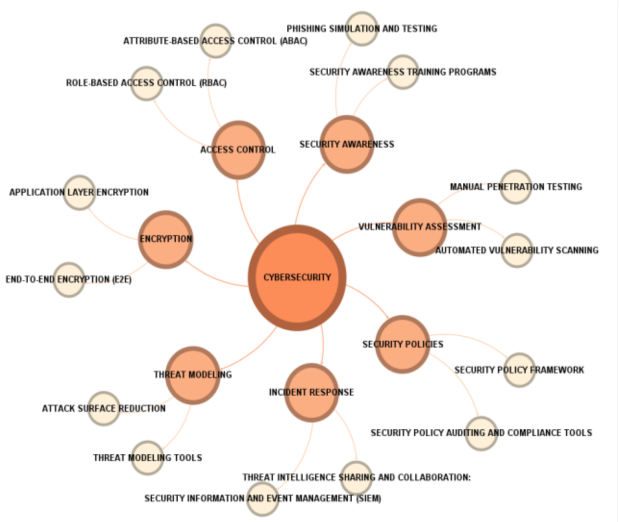
PHISHING SIMULATION AND TESTING
ATTRIBUTE-BASED ACCESS CONTROL (ABAC)
SECURITY AWARENESS TRAINING PROGRAMS
ROLE-BASED ACCESS CONTROL (RBAC)
ACCESS CONTROL
SECURITY AWARENESS
MANUAL PENETRATION TESTING
APPLICATION LAYER ENCRYPTION
VULNERABILITY ASSESSMENT
ENCRYPTION
AUTOMATED VULNERABILITY SCANNING
END-TO-END ENCRYPTION (E2E)
CYBERSECURITY
SECURITY POLICIES
THREAT MODELING
SECURITY POLICY FRAMEWORK
INCIDENT RESPONSE
ATTACK SURFACE REDUCTION
SECURITY POLICY AUDITING AND COMPLIANCE TOOLS
THREAT MODELING TOOLS
THREAT INTELLIGENCE SHARING AND COLLABORATION:
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Figure 1 – Simplified MAI hierarchy for the goal “Ensuring cybersecurity”

Electronic copy available at: https://ssrn.com/abstract=4621732

Weights of criteria and alternatives, consistency

The procedure for determining weight coefficients from pairwise comparisons can be used both to assess the priorities of the criteria themselves and to evaluate alternatives based on pairwise comparisons conducted by experts both on the criteria and on the alternatives. The input is a matrix of pairwise comparisons. Matrices for both criteria and alternatives are formed in the same way, so let's consider, for example, the matrix for comparing alternatives $\boldsymbol{A}$ (elements of which are $\boldsymbol{a_{ij}}$). The alternatives are compared in pairs by experts, and then their answers are summarized (generally averaged). If, when comparing alternatives $\boldsymbol{A}_i$ and $\boldsymbol{A}_i$ a numerical estimate of the advantage was obtained $\boldsymbol{A}_i$ How $\boldsymbol{a_{ij}}$**,** then in a reverse comparison the advantage is assessed as the inverse value: $\mathbf{1/}\boldsymbol{a_{ij}}$**.** Obviously, the advantage when comparing an alternative with itself is assessed as 1. To determine the weighting coefficients of alternatives (or criteria, if a comparison of criteria is considered), it is enough to find the eigenvectors of the matrix $\boldsymbol{A}$**.** It is the eigenvector values of this matrix, corresponding to the maximum eigenvalue, that will be the weighting coefficients for the criteria (weighting coefficient - the element of the eigenvector corresponds to the criterion number). However, this approach makes sense if the pairwise comparison matrix is consistent. We will check the consistency of the matrices obtained on the basis of such methodological principles. To ensure consistency of the comparison matrix, the consistency coefficient is calculated μ. It is calculated by the formula:

$$\mu = \frac{|\lambda_{\max} - n|}{n-1},$$

Where $\lambda_{\max}$ – the determination is made as follows: from the values of the comparison matrix and the values of the eigenvector, a matrix $\boldsymbol{E}$ is constructed, where each element

$$e_{ij} = a_{ij}\frac{w_i}{w_j},$$

Electronic copy available at: https://ssrn.com/abstract=4621732

Here w_i, w_j – elements of the eigenvector. After this, the sum of the elements of matrix ***E*** is calculated for each row and the maximum value is selected λ_{max}.

If the matrix of alternatives is completely consistent, then $\lambda_{max} = n$, otherwise $\lambda_{max} > n$. There is a table of consistency indices [1], which contains the values of the reference indices for different values $n - \mu_T(n)$. If $\mu/\mu_T < 0.1$, then the matrix of alternatives is considered consistent.

Model calculation

To determine the matrix of pairwise comparisons of criteria, on behalf of virtual experts, contact the ChatGPT system with a request to evaluate the importance of the selected criterion relative to all other criteria (each separately). Below is an example of a prompt in which the "ENCRYPTION" criterion is compared with others:

> ▶ The values for ensuring the cybersecurity criterion "ENCRYPTION" need to be determined through expert judgment in comparison to the criteria listed below. Please provide only one generalized comparative numerical expert assessment for each criterion (in terms of times). The criteria and assessments should be presented in the form of a list. Please provide an assessment of the advantages of the "ENCRYPTION" criterion for the following criteria: ACCESS CONTROL; INCIDENT RESPONSE; SECURITY AWARENESS; SECURITY POLICIES; THREAT MODELING; VULNERABILITY ASSESSMENT. To provide generalized numerical assessments of the impact of the "ENCRYPTION" criterion compared to other criteria, you can use a scale where 1 corresponds to equal importance, less than 1 indicates lesser importance, and greater than 1 indicates greater importance.

The response from the ChatGPT system, which will serve as the basis for generating the corresponding column of the pairwise comparison matrix, looks like this:

- ACCESS CONTROL: 1
- INCIDENT RESPONSE: 0.7
- SECURITY AWARENESS: 0.8
- SECURITY POLICIES: 1.2

Electronic copy available at: https://ssrn.com/abstract=4621732

- THREAT MODELING: 1.1
- VULNERABILITY ASSESSMENT: 1.2

As a result of executing similar prompts for all criteria, we obtain a matrix of pairwise comparisons of the following form:

Criterion	1	2	3	4	5	6	7
1	1	0.9	0.8	0.8	1.2	0.9	1
2	1	1	0.9	0.9	0.9	1.1	0.7
3	0.9	1.1	1	0.8	0.8	0.8	0.8
4	1.2	1.2	1.2	1	1	1	1.2
5	1.1	1	1.1	1.1	1	1	1
6	1.3	1.3	1.1	1.2	1.1	1	1.1
7	1.1	1.1	0.9	1.1	0.9	0.9	1

The matrix obtained in this way can be considered as two matrices obtained by two groups of virtual experts, based on the prompts specified to compare each with each (a part of the matrix above the diagonal and a part of the matrix below the diagonal, supplemented by transposed matrices). Therefore, calculations were carried out for each of these matrices and similar results were obtained. The matrices turn out to be consistent according to the specified criterion. The vector of averages for two matrices of weight values has the form: (0.35; 0.35; 0.35; 0.40; 0.39; 0.41; 0.38), from here we can conclude that the criteria are close in importance, the most influential: 4th and 6th (SECURITY POLICIES and VULNERABILITY ASSESSMENT).

To determine the matrix of pairwise comparisons of alternatives (in a simplified form without directly taking into account the criteria), the ChatGPT system is contacted with a request to assess the importance of each alternative selected above relative to all other alternatives. Below is a prompt that compares the "APPLICATION LAYER ENCRYPTION" alternative with others:

►You need to determine the advantages of the "APPLICATION LAYER ENCRYPTION" concept for cybersecurity compared to the

Electronic copy available at: https://ssrn.com/abstract=4621732

concepts listed below through expert judgment. Please provide only one generalized comparative numerical expert assessment for each concept (in terms of times). The concepts and assessments should be presented in the form of a list. Please provide an assessment of the advantages of the "APPLICATION LAYER ENCRYPTION" concept for the following concepts:
ATTRIBUTE-BASED ACCESS CONTROL (ABAC);
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM);
THREAT INTELLIGENCE SHARING AND COLLABORATION;
ROLE-BASED ACCESS CONTROL (RBAC);
AUTOMATED VULNERABILITY SCANNING;
PHISHING SIMULATION AND TESTING;
ATTACK SURFACE REDUCTION;
THREAT MODELING TOOLS;
SECURITY POLICY FRAMEWORK;
SECURITY AWARENESS TRAINING PROGRAMS;
END-TO-END ENCRYPTION (E2E);
SECURITY POLICY AUDITING AND COMPLIANCE TOOLS;
MANUAL PENETRATION TESTING.
To provide generalized numerical assessments of the importance of the "APPLICATION LAYER ENCRYPTION" concept compared to the other concepts, you can use a scale where 1 corresponds to equal importance, less than 1 indicates lesser importance, and greater than 1 indicates greater importance.

The response of the ChatGPT system, which serves as the basis for the formation of the corresponding column of the matrix of pairwise comparisons of alternatives, has the following form:

- ATTRIBUTE-BASED ACCESS CONTROL (ABAC): 0.8
- SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM): 0.9
- THREAT INTELLIGENCE SHARING AND COLLABORATION: 0.9
- ROLE-BASED ACCESS CONTROL (RBAC): 0.8
- AUTOMATED VULNERABILITY SCANNING: 0.9
- PHISHING SIMULATION AND TESTING: 0.9
- ATTACK SURFACE REDUCTION: 0.9
- THREAT MODELING TOOLS: 0.9
- SECURITY POLICY FRAMEWORK: 0.8
- SECURITY AWARENESS TRAINING PROGRAMS: 0.9

Electronic copy available at: https://ssrn.com/abstract=4621732

- END-TO-END ENCRYPTION (E2E): 1.2
- SECURITY POLICY AUDITING AND COMPLIANCE TOOLS: 0.9
- MANUAL PENETRATION TESTING: 0.9

By executing such prompts for each alternative, we obtain a matrix of pairwise comparisons of alternatives of the following form:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
1	1	0.9	1.1	1.2	1.5	0.7	1.2	1.2	0.9	1.1	1.2	1.3	1.2	0.8
2	0.8	1	1.1	1.2	0.8	0.8	1.1	1.1	1.3	1.2	1.3	1.2	1.3	0.9
3	0.9	0.9	1	1.2	0.9	0.9	1.3	1.3	1.4	1.3	1.3	1.2	1.4	0.9
4	0.9	0.9	1.1	1	1.1	1	1.4	1.4	1.4	1.3	1.4	1.4	1.3	0.9
5	0.8	1.1	1.1	1.2	1	1.2	1.2	1.2	1.2	1.1	1.3	1.3	1.2	0.8
6	0.9	0.9	1.1	1.2	0.8	1	0.9	1.1	1.2	1.1	1.2	1.2	1.2	0.8
7	0.9	0.9	1.1	1.2	0.9	1.1	1	0.9	1.3	1.2	1.5	1.5	1.2	0.9
8	0.9	0.9	1.1	1.2	1.2	1.1	1.1	1	0.7	0.9	1.3	1.3	1.3	0.9
9	0.9	0.9	1.1	1.2	1	0.9	1.3	1.4	1	1.1	1.4	1.4	1.4	0.9
10	0.8	0.9	1.1	1.2	1.3	0.8	1.1	1.2	1.3	1	1.5	1.5	1.3	0.9
11	0.9	0.9	1.1	1.2	1	0.8	1.3	1.4	1.4	1.2	1	1.4	1.2	0.8
12	1.2	0.8	1.1	1.2	0.9	0.7	1.2	1.3	0.9	1.1	1.4	1	1.3	0.9
13	0.9	0.9	1.1	1.2	1.2	0.9	1.4	1.5	1.2	1.1	1.3	1.3	1	0.9
14	0.9	0.9	1.1	1.2	0.8	1	1.2	1.2	1.1	1.1	1.2	1.2	1.2	1

The resulting matrix can also be considered as two matrices obtained by groups of virtual experts. Thus, as in the previous case, calculations were carried out for each of these matrices, and weights that were close in value were obtained.

The matrices turned out to be consistent according to the criterion established above. The vector of average weights for two matrices has the following form: (0.29; 0.28; 0.24; 0.23; 0.27; 0.28; 0.24; 0.24; 0.26; 0.26; 0.27; 0.27; 0.30; 0.28). We can conclude that the identified alternatives are close in importance, the most influential are 1st and 13th (ATTRIBUTE-BASED ACCESS CONTROL and SECURITY POLICY AUDITING AND COMPLIANCE TOOLS).

Conclusions

As a result of an experiment in the field of cybersecurity, the possibility of using generative artificial intelligence to support decision-making using the method of multi-criteria analysis was

Electronic copy available at: https://ssrn.com/abstract=4621732

proven. A hierarchy of the goal “Ensuring cybersecurity” was obtained, including 7 criteria and 14 alternatives, the importance of which was determined by virtual experts and confirmed by real experts. Using the GII, the corresponding matrices of pairwise comparisons were obtained, after which the consistency of these matrices was confirmed, and the weights (ranking) of the criteria and alternatives were calculated. The implementation of this approach opens up wide opportunities for the use of GII in decision support systems in various fields and contributes to the “renaissance” of Thomas Saaty’s methods at the present stage.

Literature

1. Saaty, Thomas; Alexander, Joyce (1989). Conflict Resolution: The Analytic Hierarchy Process. – New York, New York: Praeger. – 252 p.
2. T.L. Saaty, L.G. Vargas. Decision Making with the Analytic Network Process. Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks. International Series in Operations Research & Management Science. – Springer New York, NY. ISBN 978-1-4419-4154-1. 2006. – 278 p.
3. Stephen Wolfram. What Is ChatGPT Doing ... and Why Does It Work? Wolfram Media, Inc., March 9, 2023. – 112 p. ISBN-13: 978-1-57955-081-3
4. Lande, Dmitry and Strashnoy, Leonard. Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). Available at SSRN: https://ssrn.com/abstract=4420452
5. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now. – Kyiv: Engineering, 2023. – 168 p. ISBN 978-966-2344-94-3

Electronic copy available at: https://ssrn.com/abstract=4621732