data

MDPI

Article

Cybersecurity Risk Assessments within Critical Infrastructure Social Networks

Alimbubi Aktayeva [1,*], Yerkhan Makatov [2], Akku Kubigenova Tulegenovna [3], Aibek Dautov [1], Rozamgul Niyazova [4], Maxud Zhamankarin [1] and Sergey Khan [5]

[1] Department of Information Systems and Informatics, Abay Myrzakhmetov Kokshetau University, Kokshetau 000002, Kazakhstan; d.abeke@mail.ru (A.D.); zhamankarin@yandex.kz (M.Z.)
[2] Department of Information Security, L. N. Gumilyov Eurasian National University, Astana 010000, Kazakhstan; m.yerkhan@list.ru
[3] Department of Information Systems, S. Seifullin Kazakh Agrotechnical University, Astana 010000, Kazakhstan; akkukubigenova@gmail.com
[4] Department of Artificial Intelligence Technologies, L. N. Gumilyov Eurasian National University, Astana 010000, Kazakhstan; rozamgul@list.ru
[5] Department of Information and Communication Technologies, Sh. Ualikhanov Kokshetau University, Kokshetau 000002, Kazakhstan; s.khan_59@mail.ru
* Correspondence: aakhtaewa@gmail.com; Tel.: +7-716-2-254259

Abstract: Cybersecurity social networking is a new scientific and engineering discipline that was interdisciplinary in its early days, but is now transdisciplinary. The issues of reviewing and analyzing of principal tasks related to information collection, monitoring of social networks, assessment methods, and preventing and combating cybersecurity threats are, therefore, essential and pending. There is a need to design certain methods, models, and program complexes aimed at estimating risks related to the cyberspace of social networks and the support of their activities. This study considers a risk to be the combination of consequences of a given event (or incident) with a probable occurrence (likelihood of occurrence) involved, while risk assessment is a general issue of identification, estimation, and evaluation of risk. The findings of the study made it possible to elucidate that the technique of cognitive modeling for risk assessment is part of a comprehensive cybersecurity approach included in the requirements of basic IT standards, including IT security risk management. The study presents a comprehensive approach in the field of cybersecurity in social networks that allows for consideration of all the elements that constitute cybersecurity as a complex, interconnected system. The ultimate goal of this approach to cybersecurity is the organization of an uninterrupted scheme of protection against any impacts related to physical, hardware, software, network, and human objects or resources of the critical infrastructure of social networks, as well as the integration of various levels and means of protection.

Keywords: fractal characteristics; self-similarity; social network security; network anomaly detection; social network traffic; critical social network infrastructure; risk assessment

check for updates

Citation: Aktayeva, A.; Makatov, Y.; Tulegenovna, A.K.; Dautov, A.; Niyazova, R.; Zhamankarin, M.; Khan, S. Cybersecurity Risk Assessments within Critical Infrastructure Social Networks. *Data* **2023**, *8*, 156. https://doi.org/10.3390/data8100156

Academic Editor: Han Woo Park

Received: 11 August 2023
Revised: 26 September 2023
Accepted: 15 October 2023
Published: 19 October 2023

1. Introduction

In the context of the high dynamics in the implementation of digital technologies and the formation of new digital segments, an intensive transformation of technological, managerial, and business approaches in the information space is being carried out. Social networks are dynamic platforms and applications that rely heavily on data. Social networks are rapidly developing, providing information for collection, which obviously raises interest in social network analysis, and gives way to new approaches that are gaining traction in areas such as searching for experts, recruiting professional teams, providing social advising, marketing, communications, and advertising.

Social network analysis currently aids in the study of a number of economic and organizational phenomena and processes, including combating money laundering, identity theft, online fraud, cyber-attacks, the investigation of illegal transactions with securities and investments, preventing riots, and others. Social networks contain opportunities for influencing the formation of public opinion, making political, economic, and military decisions, influencing the information resources of the enemy, and disseminating specially prepared or deceptive information. Social networks are even widely used for their informational and psychological impacts.

Social network workflows are subject to cyberthreats associated with the introduction of new solutions and the use of new business models, which may be accompanied by the absence or insufficiency of information for prompt decision making on ensuring the cybersecurity of critical social network infrastructure. This makes a review and analysis especially essential and pending for the basic tasks of collecting information, monitoring, and analyzing methods of social networks used to detect, prevent, and combat threats to ensure cybersecurity. There is a need to design certain methods, models, and program complexes aimed at analyzing cyber context awareness and supporting the activities of objects and assets in the critical social network infrastructure.

Cybersecurity belongs to an area of active research and development in the information technology community, thanks to the efforts of all of the ICT ecosystem components (see Figure 1).

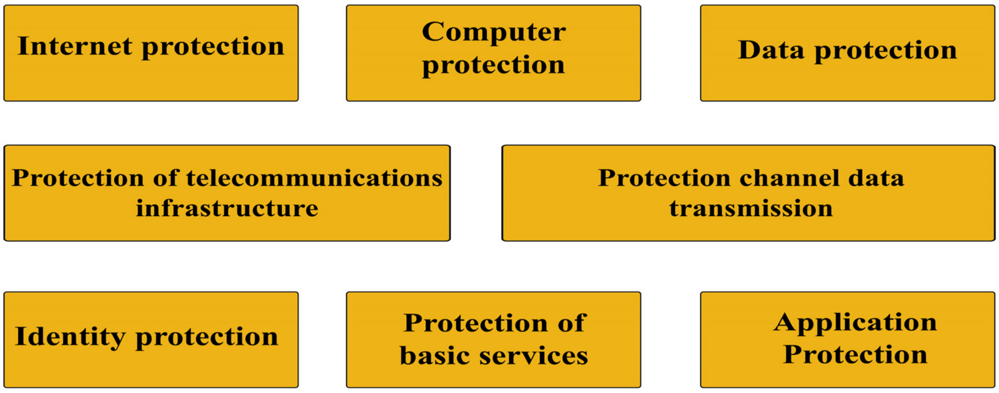

Internet protection
Computer protection
Data protection
Protection of telecommunications infrastructure
Protection channel data transmission
Identity protection
Protection of basic services
Application Protection

Figure 1. ICT ecosystems of cybersecurity components.

Infrastructure is recognized as critical when its failure or destruction significantly impacts security, the economy, social welfare, and health [1]. Failures or interruptions of critical infrastructure in social networks may inflict damage to society and the economy, or lead to a cascade of accidents that lead to failures in multiple infrastructures with potentially devastating impacts [2]. Critical infrastructures are designed to operate for a long time (several decades), and their operation is ensured through maintenance, updating, and the integration of new technologies.

Cyber-physical systems (CPSs) integrate the cybernetic principle, computer hardware, and software technologies, as well as qualitatively integrate new actuators built into their environments. CPSs are capable of perceiving and responding to their alterations; they are configured to self-learn and adapt. One of the main CPS requirements, in addition to functional efficiency, is the safety of the interaction of its components, considering the complex impact on the objects managed. Ensuring the safety of CPSs is associated with two key properties:

(1) Safety, aimed at ensuring the protection of the system from random failures;
(2) Security, aimed at protecting the system from intentional attacks.

2. Materials and Methods

The key trend in solving safety problems is theories based on the concept of risk [3], which normally include determining the current states of the system elements, the determinants of the occurrence and development of incidents, emergencies, and catastrophic situations, as well as qualitative and quantitative descriptions of scenarios and consequences when reaching the limit states that result in accidents and catastrophes.

In accordance with the international standard [4], cybersecurity rests on application security, information security, network security, internet security, and the protection of key information systems of critical infrastructure; at the same time, it is not identical to any of the abovementioned standards. It covers the baseline security practices for stakeholders in cyberspace. This international standard provides the following:

1. An overview of cybersecurity;
2. An explanation of the relationship between cybersecurity and other types of security;
3. A definition of stakeholders and a description of their roles in cybersecurity;
4. Guidance for addressing common cybersecurity issues;
5. A framework to enable stakeholders to collaborate in resolving cybersecurity issues [4,5].

Many areas of cybersecurity have common themes and issues that require a comprehensive approach. In the vast majority of cases, the most successful attacks by hackers or intruders are directed at servers and end-user computers connected to the Internet, according to an analytical expert's report. Figure 2 reflects the position of cybersecurity relative to other areas of security [6].

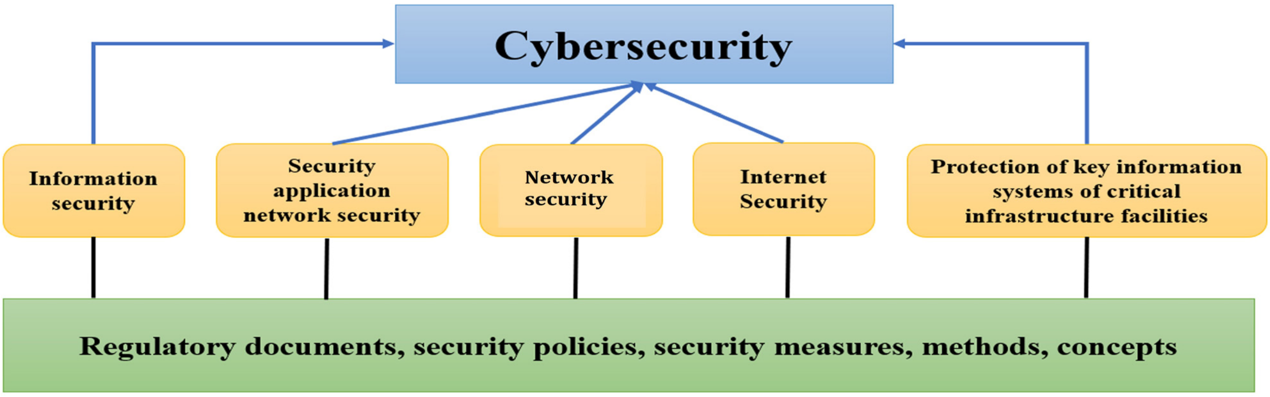

Cybersecurity
Information security
Security application network security
Network security
Internet Security
Protection of key information systems of critical infrastructure facilities
Regulatory documents, security policies, security measures, methods, concepts

Figure 2. Positioning of cybersecurity [6].

Destructive impacts on critical social network infrastructure and espionage are the main goals of cybercriminals. Attacks often use tools such as malware, Trojans, botnets, phishing, distributed denial of service (DDoS) attacks, and man-in-the-middle attacks [7]. Figure 3 highlights some of the major cybersecurity problem areas for cyber physical systems, and shows where some of these problems can be addressed with technical solutions.

The cybersecurity risk assessment process is an important prerequisite for conducting science-based and efficient risk assessments. Critical resources and their potential vulnerabilities can be identified based on a description of the social network architecture. The process for assessing cybersecurity risks is illustrated in Figure 4.

Similarly, a significance-based rating of resources and their vulnerabilities is carried out, as well as an analysis of existing security measures. Approaches to ensuring the cybersecurity of social networks have a common structure, and include four principal stages:

1. Identification of critical resources and their vulnerabilities.
2. Determination of threats, the implementation of which violates the functioning of critical resources.
3. Risk estimation and determination of damage from the implementation of threats.
4. Selection and application of risk reduction measures and acceptance of residual risks [8,9].

The cybersecurity risk assessment process includes the preparation of risk assessment, asset identification, threat identification, vulnerability identification, damage identification, risk calculation, and other stages. It can be divided into a few steps when working with the specifications [8,9].

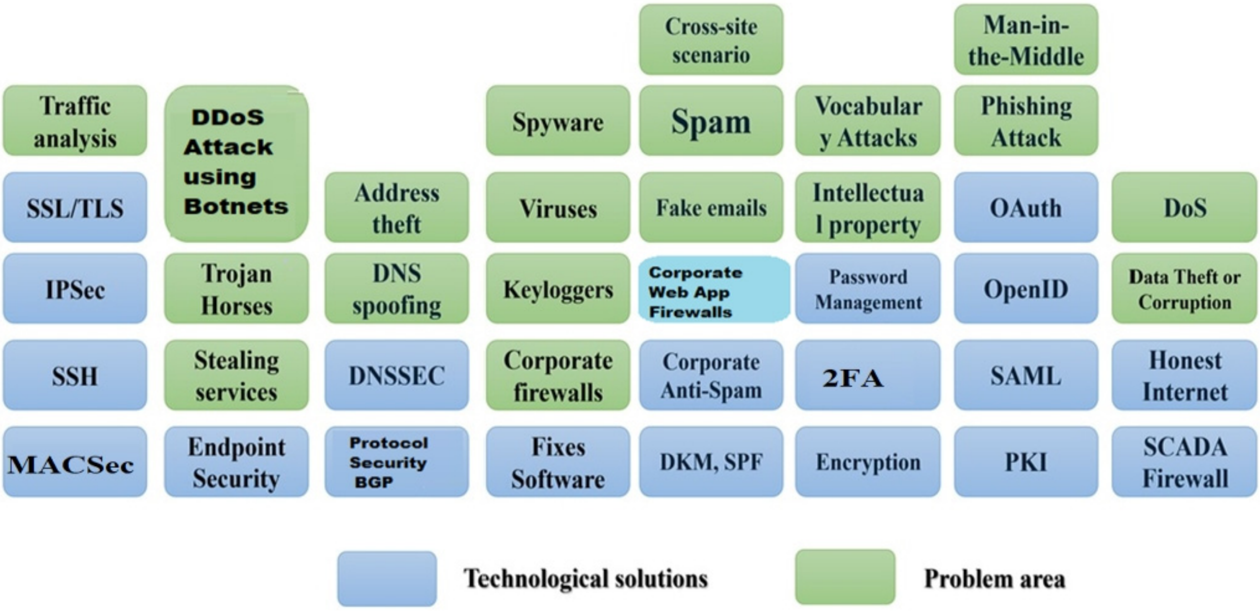


Figure 3. Cybersecurity issues and technological solutions: 2FA—two-factor authentication; SAML—security assertion markup language; PKI—public key infrastructure; DKM—domain keys identified mail; SPF—sender policy framework; BGP—border gateway protocol; SCADA—supervisory control and data acquisition; DoS—denial of service attacks; OAuth—open authentication; MACSec—media access control security.

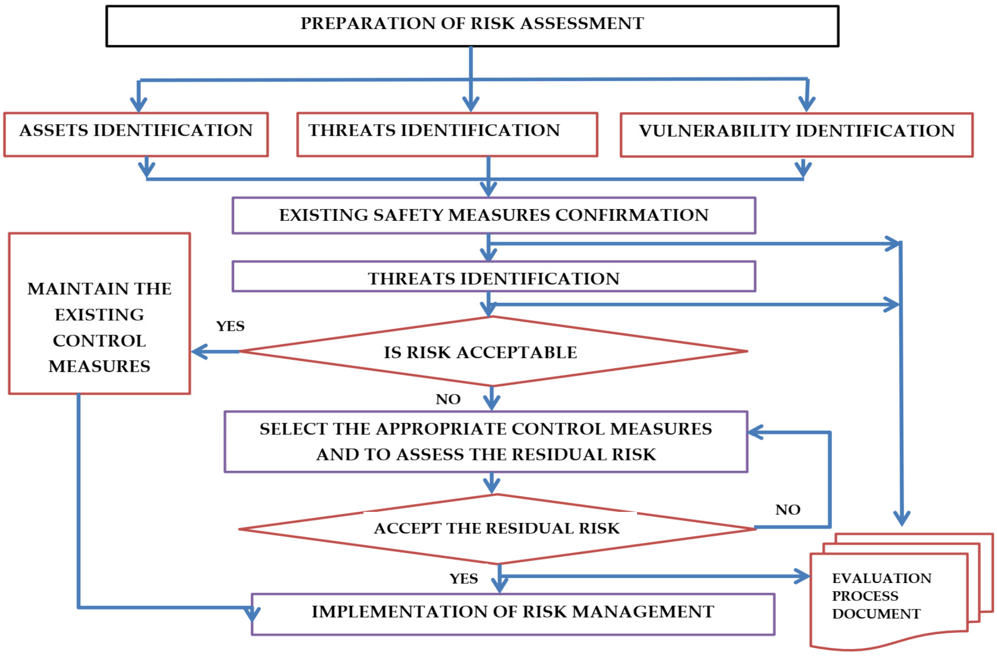

PREPARATION OF RISK ASSESSMENT
ASSETS IDENTIFICATION
THREATS IDENTIFICATION
VULNERABILITY IDENTIFICATION
EXISTING SAFETY MEASURES CONFIRMATION
THREATS IDENTIFICATION
MAINTAIN THE EXISTING CONTROL MEASURES
YES
IS RISK ACCEPTABLE
NO
SELECT THE APPROPRIATE CONTROL MEASURES AND TO ASSESS THE RESIDUAL RISK
NO
ACCEPT THE RESIDUAL RISK
YES
IMPLEMENTATION OF RISK MANAGEMENT
EVALUATION PROCESS DOCUMENT

Figure 4. The process of the information security risk assessment [8,9].

3. Results and Discussion

Currently, one of the most complex and urgent problems is assessing the cybersecurity risks of social network critical infrastructure objects as part of managing cybersecurity. The difficulty lies in the lack of generally recognized approaches and methodologies for risk assessment.

Cognitive modeling can address interdisciplinary cybersecurity challenges that require cutting-edge approaches in the humanities and computational sciences, such as the following:

1. Adversarial arguments and behavioral game theory for predicting the subjective utilities of attackers and the decision probability distribution;
2. The human factor of cyber tools for solving the problems of integrating human systems, assessing the cognitive states of the defender, and the possibility of automation;
3. Dynamic simulation involving attacker, defender, and user models for profound inquiry into cyber epidemiology and cyber hygiene;
4. Evaluation of the effectiveness of training and learning scenarios for solving cybersecurity problems, enhancing cybersecurity skills, and making effective decisions.

The building of models can initially happen at the group level based on the average trends of each subject's subgroup, supported by available statistics such as skill levels, demographics, and cultural factors.

More accurate and reliable predictions are achieved through cognitive models that are fine-tuned for each individual attacker, defender, or user profile, and that are updated over time using techniques such as model routing and dynamic parameter fitting. Cognitive flexibility is commonly understood as a three-component structure, namely the following:

(a) Cognitive flexibility means the ability to exercise cognitive control and change mindsets, as well as overcome automatic or dominant reactions.

(b) Cognitive exposure stands for receptivity to new ideas, experiences, and perspectives.

(c) Focused attention is the ability to note the relevant drivers and ignore the distractions.

The cognitive component involves the analyst's ability to perform a cognitive analysis of the data presented, to identify the technical implications, and to draw the conclusions required for making informed decisions and obtaining the best result. Qualitative, quantitative, or hybrid approaches are applied for risk analysis and the determination of damage from the implementation of threats [10,11].

Qualitative assessments use linguistic or scoring scales, quantitative approaches employ probabilistic models and scoring scales, and hybrid approaches combine the above two and are considered to be the most complete [12,13]. Generally, risk is calculated as a product of threat, vulnerability, and consequences, which are together called the general risk model:

$$R = \{T,\ V,\ C\}, \tag{1}$$

where T is threats, V is vulnerabilities, and C is damage.

Cybersecurity defines the presented approach to risk assessment as a three-factor approach. When using a three-factor approach, the level of cybersecurity risk is determined by the possibility of exploiting a vulnerability V, the possibility of implementing a threat T using a given vulnerability V, and the damage C from the implementation of a threat [12,13].

Risk factors (meaning, threat, vulnerability, and damage) are analyzed using heuristic approaches, resulting in a variety of data. Simultaneously, security is to be maintained at all stages of the system life cycle, including creation, implementation, operation, modification, and decommissioning, taking into account the object protection class. The choice of security measures is carried out primarily for risks with a high probability of occurrence and significant damage [14–16].

Furthermore, the risk assessment procedure consumes time and labor. Implementing intellectual policy concepts for security incident response and risk management in social networks requires consideration of the following potential factors associated with modern technologies:

1. The more complex the social network is, the higher the number of vulnerabilities to potential attacks and unintentional mistakes.
2. Social networks interconnected with other networks, which can also occupy multiple "smart" network domains, increase the likelihood of cascading failures.

3. A large number of interconnections between software components increase the vulnerability of the program code, which expedites the introduction of malicious code and vulnerabilities into the program code by attackers.
4. The larger the number of social network nodes, the greater the number of access points to the system there are for intruders [17].

Approaches to system risk assessment are helpful in analyzing systems that lack the data to accurately predict future system performance. To achieve this, the system undergoes decomposition into subsystems and components that possess more information. The overall probabilities and risk depend on the architecture of the system, and are related to probabilities at the levels of the subsystems and components.

Risk quantification, often referred to as probability estimation, is related to system analysis methods. Risk quantification assessment adjusts the current state of the art, including uncertainties about phenomena, processes, activities, and systems under analysis. Its purpose is to identify possible hazards and threats, as well as analyze their causes and consequences. The risk assessment includes three stages (see Figure 5).

3. EVALUATION
2. ANALYSIS
1. IDENTIFICATION

Figure 5. The risk assessment.

Risk analysis is accompanied by the identification of significant threats and vulnerabilities, as well as an assessment of their likelihood. In this study, risk analysis is carried out in the framework of analyzing cyberthreats and modeling scenarios of extreme situations in social networks. Risk is considered to be a combination of the consequences of some event (incident) and the possibility of occurrence associated with it (probability of occurrence), and risk assessment is considered to be the overall process of identification, analysis, and assessment of risk. Cybersecurity risks are considered, on the one hand, to be risks to the cybersphere, and, on the other hand, a type of cybersecurity risk associated with a disruption in the functioning of the technological infrastructure of a social network, inflicting adverse effects.

IT risk analysis constitutes the core process of managing the cybersecurity of social network critical infrastructure objects. In the scope of security, risk measures the likelihood and severity of a condition in which a given threat exploits specific weaknesses, causing the loss or damage of technological infrastructure and, consequently, indirect or direct losses for participants in these social networks [18]. Risk analysis of the technological infrastructure of a social network includes three principal stages:

1. Identification of dangers/threats/possibilities (sources).
2. Cause-and-effect analysis, including vulnerability analysis.
3. Description of risk using probabilities and expected values [19,20].

The fractal approach facilitates the representation of any technology as a set of information objects (layers) and their mappings. The technology in this case is designed in terms of the description of information objects and the means to map from each layer to the next. These methods provide tools to support specific information technologies, including social networking technology [21]. In a fractal approach, typical social networking technology segregation allocates three levels (see Figure 6).

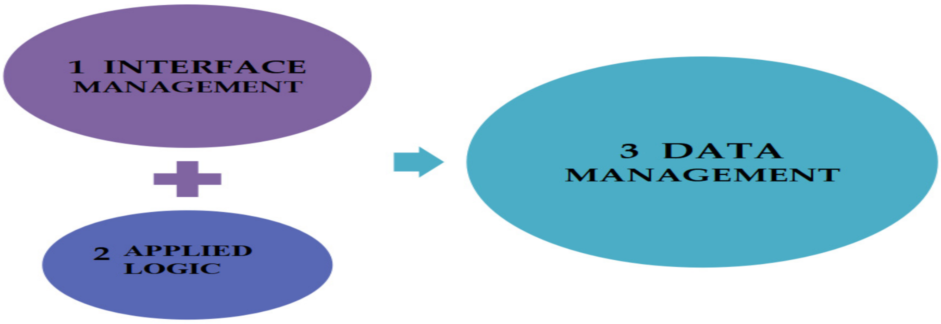


Figure 6. Social networking technology segregation levels.

The fractal approach to data and knowledge mapping facilitates the segregation of data and knowledge space D, and sets up the images from every layer to each [21]. Here, the information resources (data and knowledge) in the framework of studying the cybersecurity of critical social network infrastructure objects are displayed as follows:

$$D = \{M,\ E,\ V,\ T,\ R\} \tag{2}$$

where M is for approaches suggested, E is for critical social network infrastructure objects, V is for the security vulnerability of social network assets, T stands for cyberthreats, and R is for the risk model.

The incorporation of a methodological approach required a breakdown of knowledge on critical social network infrastructure objects by means of ontological engineering (refer to Figure 7) and a fractal approach.

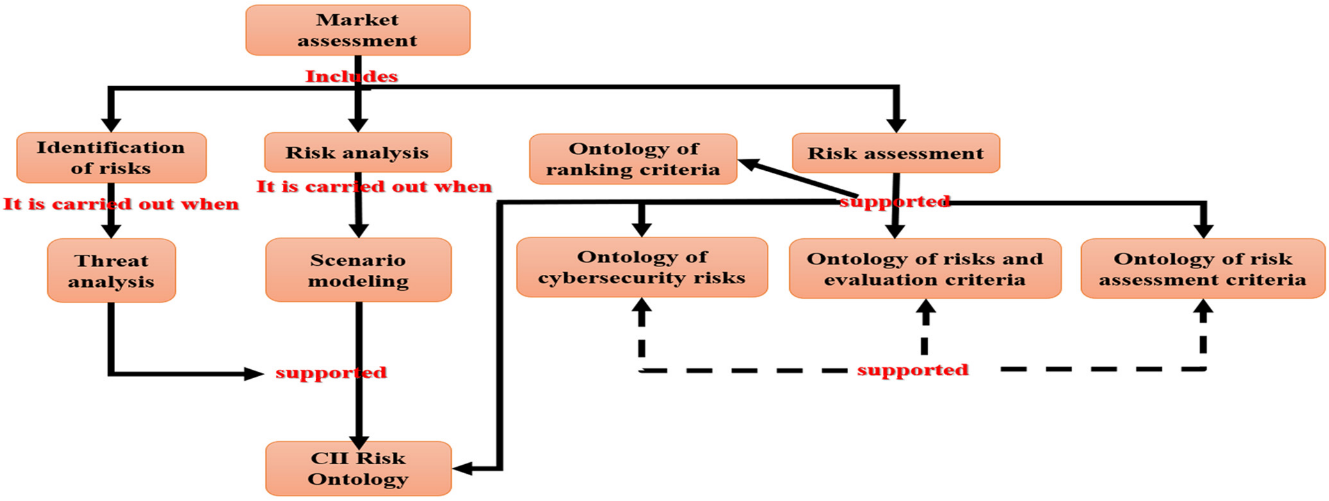


Figure 7. Ontologies for assessing risks of cybersecurity violation of social network infrastructure.

A methodological approach to analyzing the cybersecurity of social network critical infrastructure objects includes the following:

1. A fractal stratifiable model of knowledge breakdown;
2. A system of cybersecurity ontologies (see Figure 8);
3. A probability model of scenarios of extreme situations caused by the implementation of cyberthreats built using Bayesian belief networks;
4. A numerical approach for determining the cybersecurity risk level;
5. Cybersecurity risk analysis methodology.

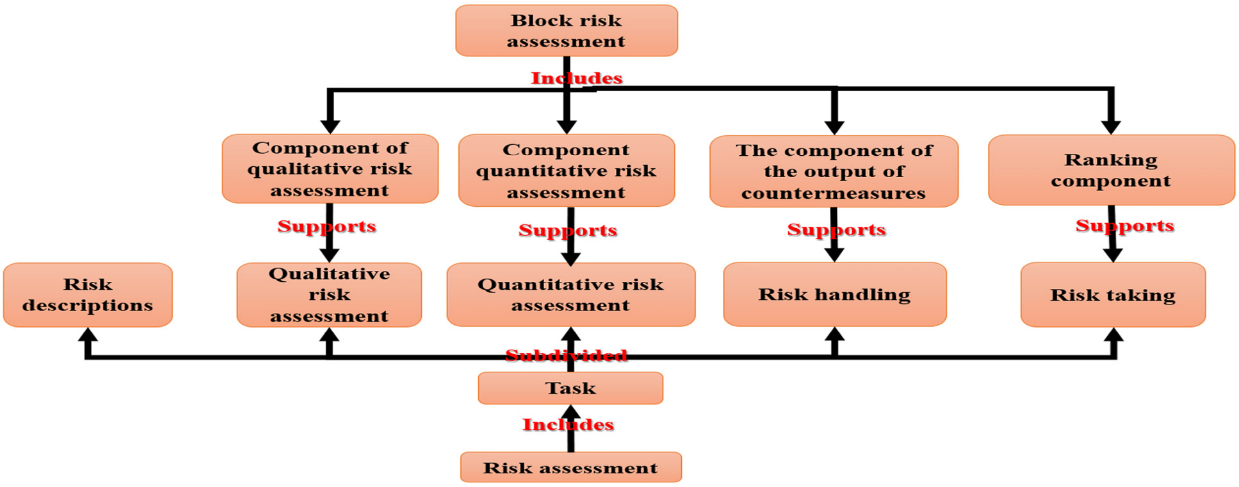

Block risk assessment
Includes
Component of qualitative risk assessment
Component quantitative risk assessment
The component of the output of countermeasures
Ranking component
Supports
Supports
Supports
Supports
Risk descriptions
Qualitative risk assessment
Quantitative risk assessment
Risk handling
Risk taking
Subdivided
Task
Includes
Risk assessment

Figure 8. Ontology of the main components of the fractal approach.

The proposed methodological approach guides the determination of critical assets of the social network infrastructure, revealing vulnerabilities and corresponding cyberthreats, establishing relationships between the threats to cyber and information security, and identifying and assessing the risks of the consequences of a cybersecurity breach, taking into account the possibility of an extreme situation caused by the implementation of cyberthreats.

3.1. Methodology for Assessing the Risks of Cybersecurity Breaches of the Critical Infrastructure of a Social Network

The methods for assessing the risks of infrastructure cybersecurity violations are aimed at risk assembly, with its consequent qualitative and quantitative assessment. It also includes the rating of the objects considered by specified criteria, whether it is the value of the object wise integral risk indicator or individual types of risks associated with technological accidents and their consequences, the lack of options in resources for participants (users), or something else [22]. The critical infrastructure of the social networking is an essential big data resource for the cyber security of economic welfare and national security. There are four stages within the methodology for assessing the risks of cybersecurity breaches of the critical infrastructure of a social network [23,24].

Stage 1. Risk description. Risk is considered the product of probability and damage. Each concerned scenario describes the states of the "consequence-type" object and their probabilities, as well as the states that cause such a consequence. For each state of the "consequence-type" object, the possible damage is expertly determined, i.e., risks are described in accordance with the formula $R = \{T, V, W, C, D\}$, and can be represented in Table 1.

This study's refinement determines whether the risks should be described both for each scenario outcome and for the scenario as a whole. A description of the risks of all significant scenarios should be performed in accordance with the classification of risks.

Stage 2. Risk assessment. The development of the scale of consequences shall be based on the level of their impact on cybersecurity. It includes two stages:

1. Qualitative;
2. Quantitative.

The formation of a probability scale rests on statistical data on the social network itself and similar external incidents. Qualitative risk assessment is carried out using the risk matrix presented in Table 2, where the risk assessment criteria are the probability of risk occurrence and the level of damage.

Table 1. Risk description.

Scale Levels	Threats	Damage	Vulnerabilities
Very low (from 0 to 0.2)	The event almost never occurs.	Insignificant loss of material and resources, which are quickly replenished, or insignificant impact on reputation.	Vulnerability that can be neglected.
Low (from 0.2 to 0.4)	The occurrence is rare.	A more significant loss of tangible assets, a more significant impact on reputation, or an infringement of interests.	Minor vulnerability that is easy to fix.
Average (from 0.4 to 0.6)	The event is quite possible under certain circumstances.	Sufficient loss of tangible assets or resources, or sufficient damage to reputation and interests.	Moderate vulnerability.
High (from 0.6 to 0.8)	Most likely, the event will occur when an attack is organized.	Significant damage to reputation and interests, which may pose a threat to the continuation of activities.	There is a serious vulnerability, the elimination of which is possible, but associated with significant costs.
Very tall (from 0.8 to 1)	The event is most likely to occur when an attack is staged.	Devastating consequences and the inability to surf the social network.	A critical vulnerability that calls into question the possibility of its elimination.

Table 2. Risk matrix.

Probability of Risk Occurrence	Level of Damage				
Insignificant	Low	Medium	High	Very high	
Extremely high	Low	Medium	High	High	High
High	Low	Medium	Medium	High	High
Medium	Low	Low	Medium	Medium	High
Low	Low	Low	Low	Medium	Medium
Extremely low	Low	Low	Low	Low	Low

The quantitative measurement of the risk level employs the Bayesian probability of the ensuing consequences, and the assessment of possible damage in monetary terms. The quantitative assessment is expressed in the calculation of the likely damage according to the formula $R_i = P\ (c_i) \times D_i$, where the probability P is a function of Y.

Clustering criteria are recommended for the quantitative risk assessment of extreme scenarios in social networks because of cyberthreats. The highest divergence risks and the highest probability require further risk treatment first.

Stage 3. Rating of Critical Information Infrastructure Objects. Available vulnerabilities in the risk assessment allow the determination of the list of critical social media assets to further justify the security financial costs. Subject to any information about the cybersecurity of a group of interdependent objects (users) located in a certain territory, it is possible to rate them in alignment with the risks of violating cybersecurity:

$$K = \{C,\ R,\ F\}, \tag{3}$$

where K is for the criterion of significance, C is for the risk assessment criterion, R is for the integrated risk index, and F is for the set of objects of critical infrastructure in the social networks.

The proposed approaches provide a gradual description of how the list of critical assets of social networks could be examined to identify vulnerabilities and cyberthreats, as well as ways of forming a scenario for a hypothetical emergency situation at the facility, and identifying risks for their further processing. A list of critical assets and the most likely threats and vulnerabilities that can lead to significant damage is provided for reference.

This stage depends on the level of study refinement, and will result in a rated list of objects to be protected, meaning the assets or objects of critical infrastructure in a social network. For further support of the methodological approach, it is proposed to develop an intelligent system based on the principles of building intelligent systems.

Stage 4. Determination of the level of cybersecurity of the critical infrastructure of social networks. Risk management covers both measures to prevent the occurrence of hazards and threats, as well as measures to reduce their potential consequences. The ratio of the number of considered scenarios to the number of possible scenarios in the model is calculated using the following formula:

$$L = \frac{Y}{2^{n-1}}, \tag{4}$$

where L is the level of cybersecurity of the critical infrastructure of social networks, Y is the calculated number of scenarios, and $2^{\mathrm{n}-1}$ is the total number of scenarios. Accordingly, n is determined in the indicated order:

$$n = |V| + |T| + |W|, \tag{5}$$

3.2. Features of the Social Network Cybersecurity Risk Assessment

Cybersecurity risk (R) is a complex value that is defined as a function (or functional) of a number of factors, such as cybersecurity threats (X_1), potential damage (X_2), and social network vulnerabilities (X_3). The main challenges of the analysis are associated with assessing cybersecurity risk and its factors (*threats*, *potential damage*, *and vulnerabilities*).

This results from the following problems:

1. Incomplete information about risk components and their ambiguous properties;
2. The complexity of creating a social network model and assessing its vulnerability;
3. The duration of the evaluation process and the rapid loss of relevance of its results;
4. The complexity of aggregating data from various sources, including statistical information and expert assessments;
5. There a need to involve several specialists in risk analysis to improve the adequacy of the assessments.

Therefore, the task is to choose from a set $\{Y\}$ of methods for assessing the risk of cybersecurity a method y* that would provide the maximum probability of an adequate assessment, taking into account adaptability to qualitative data on the set $\{X\}$ of risk factors:

$$y^* \in Y \leftrightarrow max \; \{p_1^*(X, \; p_2(y))\} \tag{6}$$

where X $\{X_1,X_2,X_3\}$ is a set of risk factors, p_1 is the probability of an adequate risk assessment, and p_2 is an indicator of the adaptability of the method of qualitative data.

However, the solution to this problem is associated with a number of problems:

- Evaluating indicator p_1, for which you need to know X.
- Forming X, taking into account those risk factors that may appear in the real conditions of the system's functioning.
- Ensuring a sufficient value for the indicator p_2.
- Reviewing and analyzing the set to evaluate the effectiveness of the methods.

Thus, the specified requirements require a risk assessment methodology that takes into account these limitations and complexities.

The scale for measuring the level of information risk is as follows:

- *Negligible (0):* The risk can be neglected.
- *Very low (0.10):* If the information is regarded as having a very low risk, it is necessary to determine whether there is a need for corrective actions or whether it is possible to accept this risk.

- *Low (0.25):* The level of risk allows you to work, but there are prerequisites for disrupting normal work.
- *Below average (0.375):* It is necessary to develop and apply a corrective action plan within an acceptable period of time.
- *Moderate (0.5):* The level of risk does not allow stable operation. There is an urgent need for corrective actions that change the mode of operation in the direction of risk reduction.
- *Above average (0.625):* The system can continue to function, but the corrective action plan must be applied as soon as possible.
- *High (0.75):* The level of risk is such that business processes are in an unstable state.
- *Very high (0.875):* It is necessary to immediately take measures to reduce the risk.
- *Critical (1):* The level of risk is very high and unacceptable for the organization, which requires the termination of the operation of the system and the adoption of radical measures to reduce the risk.

The problem of fuzzy modeling was solved through a fuzzy inference system. The graphical interface of the editor after defining the input and output variables, as well as setting the parameters of the fuzzy inference system, are shown in Figure 9.

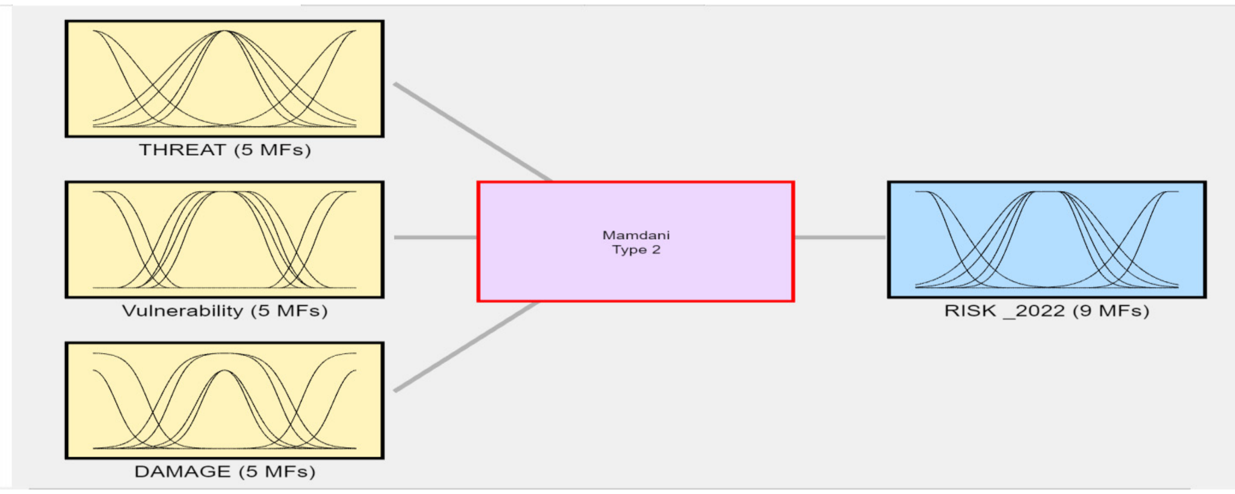


Figure 9. Graphical interface of the FIS editor (MATLAB).

3.3. Cybersecurity Risk Assessment for Critical Social Network Infrastructure

Cybersecurity risk is the probability of an undesirable outcome from an incident, event, or occurrence, defined by its probability and the damage caused. This risk is one component of organizational risk, which can include many types of risks, e.g., program management risk and security risk. Risk assessment is proposed to be based on fuzzy set theory. The linguistic variables below are referred to as entry-level risk factors, taking into account their adaptability to qualitative data on the set of risk factors:

- X1: vulnerabilities at the security level of the software products used.
- X2: vulnerabilities in the protection level of the engineering and technical means used.
- X3: impact on the level of protection of the social network's information and communication infrastructure.

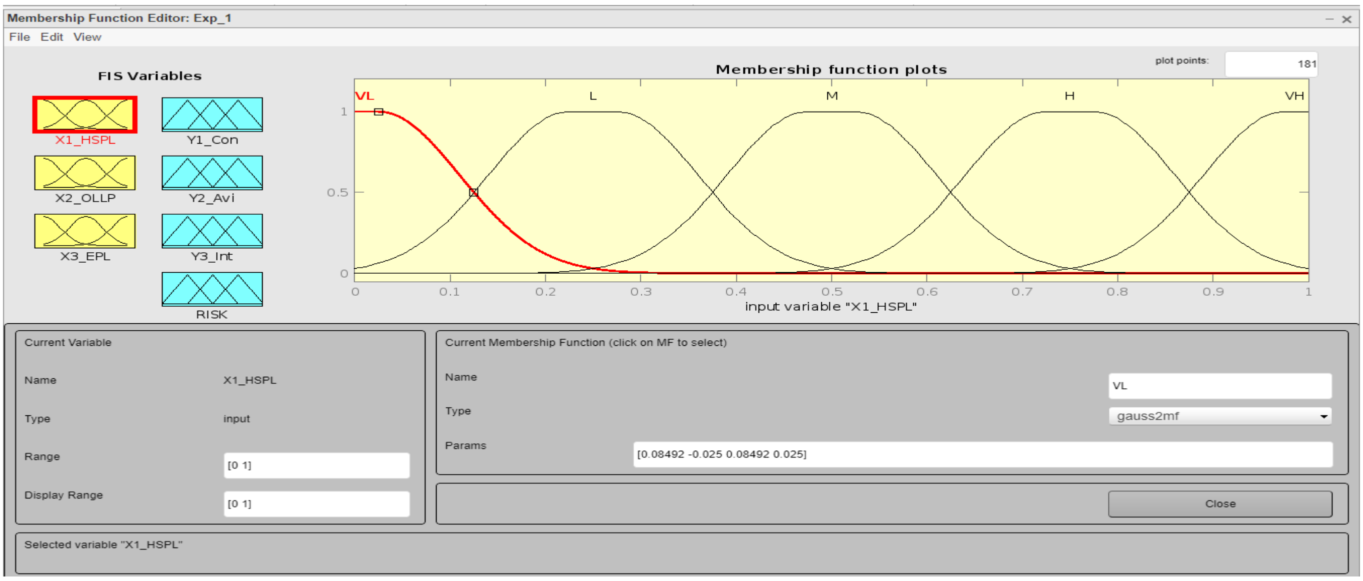
The output linguistic variables are:

- Y1 is the probability of a threat to the confidentiality of information.
- Y2 is the probability of a threat to accessibility.
- Y3 is the probability of a threat to integrity.
- R: risk.

For the created fuzzy model, the following parameters are selected:

- Three input variables (threat, damage, and vulnerability) and one output variable (risk).
- Type of fuzzy inference system: Mamdani (Sugeno).
- The and method (method of logical conjunction); the prod method (method of algebraic product).
- Or method (method of logical disjunction): probor (algebraic sum method).
- Implication (conclusion output method): min (minimum value method).
- Aggregation (method of aggregation); max (method of maximum value);
- Defuzzification (method of defuzzification): WTAVER (weighted average method).

Three input variables (threat, damage, and vulnerability), five fuzzy classes (very low, low, medium, high, and very high), and a trapezoidal membership function were selected (see Figure 10).



Membership Function Editor: Exp_1

Current Variable

Name X1_HSPL

Type input

Range [0 1]

Display Range [0 1]

Current Membership Function (click on MF to select)

Name VL

Type gauss2mf

Params [0.08492 -0.025 0.08492 0.025]

Selected variable "X1_HSPL"

Figure 10. Graphical interface of the FIS editor (MATLAB) after defining input and output variables.

For the output variable (risk), nine fuzzy classes (negligible low, very low, low, below average, moderate, above average, high, very high, critical) are selected, which in a fuzzy Mamdani-type (or Sugeno-type) system takes the abovementioned fixed values on the segment [0, 1], so there is no membership function for the output variable. For each linguistic variable, term sets {*VL*, *L*, *M*, *H*, and *VH*} are defined where the following apply:

- *VL* is on a very low level with an accessory function value range of {0; 0.1}.
- *L*: low level with accessory function value range of {0.11; 0.25}.
- *M*: medium level with a range of values for the accessory functions: {0.26; 0.5}.
- *H*: high level with a range of values of the membership functions: {0.51; 0.75}.
- *VH*: critically high level with a range of membership function values {0.76; 1}.

A hierarchical fuzzy system is constructed to assess the cybersecurity risk of the social network infrastructure (see Figure 11). The proposed risk assessment algorithm is based on Mamdani fuzzy logic inference systems (*F1*, *F2*, *F3*, and *F4*) and uses Fuzzy Logic Toolbox™ application, which provides MATLAB® functions, apps, and a Simulink® block, which is an extension package containing tools for analyzing, designing, and simulating fuzzy logic systems.

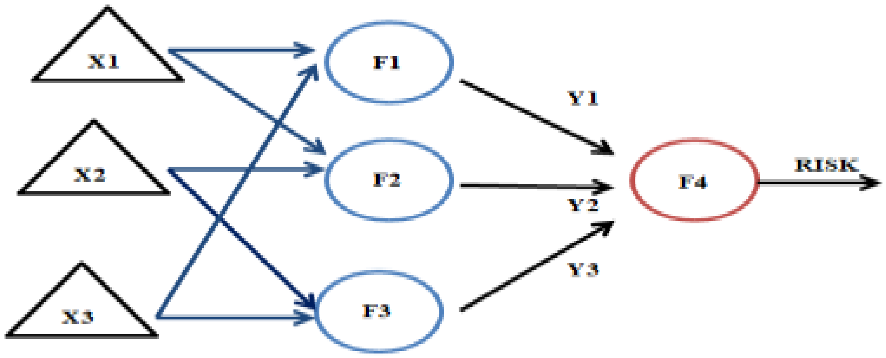
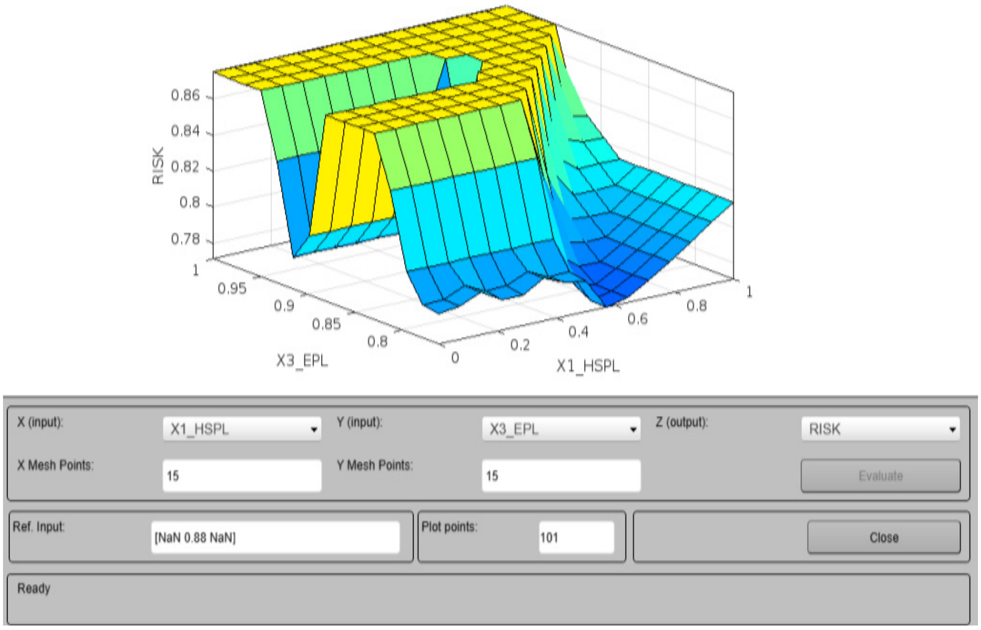


Figure 11. Hierarchical fuzzy system for cybersecurity risk assessment of critical social network infrastructure.

The fuzzy logic inference mechanism of the developed system uses the Mamdani algorithm, which has received the greatest practical application in fuzzy modeling tasks, and consists of the application of the mini–max composition of fuzzy sets. The fuzzy inference rule processing process in this case consists of four steps:

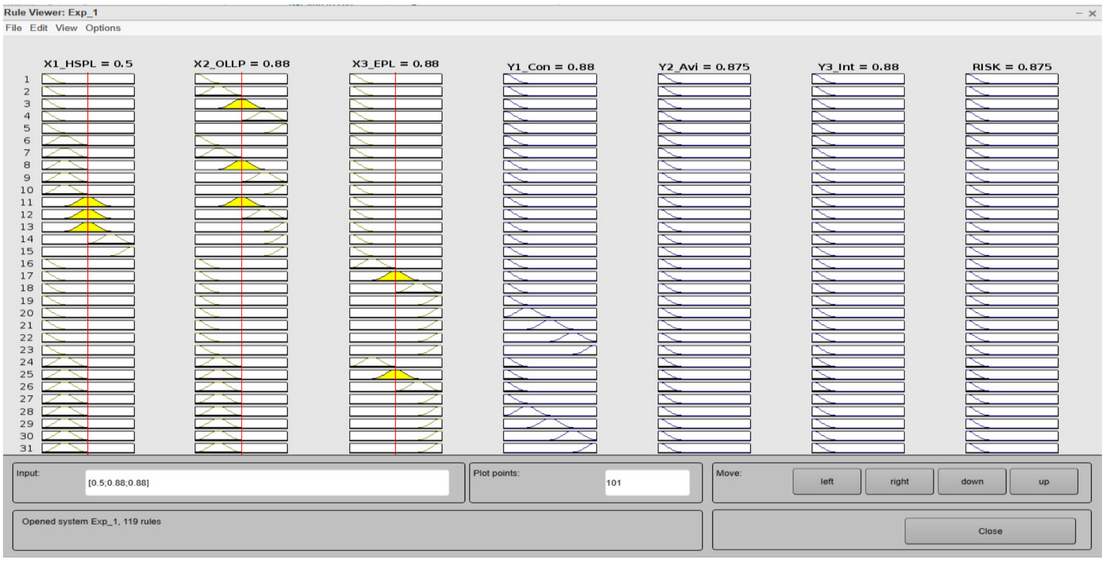
1. Phasification, which consists of determining the degree of truth, i.e., the value of the membership function for the prerequisites (left-hand sides) of each rule.
2. Fuzzy inference consists of applying to the conclusions (right-hand sides) of the rules the calculated truth-value for the premises of each rule. Mamdani's algorithm uses a minimum (min) operation that "*cuts off*" the membership function of a rule's conclusion by the height corresponding to the calculated truth-value of the rule's premises.
3. A composition that combines, using the maximum (max) operation, all fuzzy subsets defined for each inference variable and forms one fuzzy subset for each inference variable.
4. Defuzzification implementing scalarization of the composition result, i.e., the transition from a fuzzy subset to scalar values.

Three-dimensional surfaces of output variable dependence on input variables, obtained using the Surface Viewer GUI module, are shown in Figures 12 and 13.



X (input): X1_HSPL
Y (input): X3_EPL
Z (output): RISK
X Mesh Points: 15
Y Mesh Points: 15
Ref. Input: [NaN 0.88 NaN]
Plot points: 101
Ready

Figure 12. Probability of threat initiation y1 = f(X1, X3) as a function of adversary capability levels and intentions.



Input: [0.5;0.88;0.88]

Plot points: 101

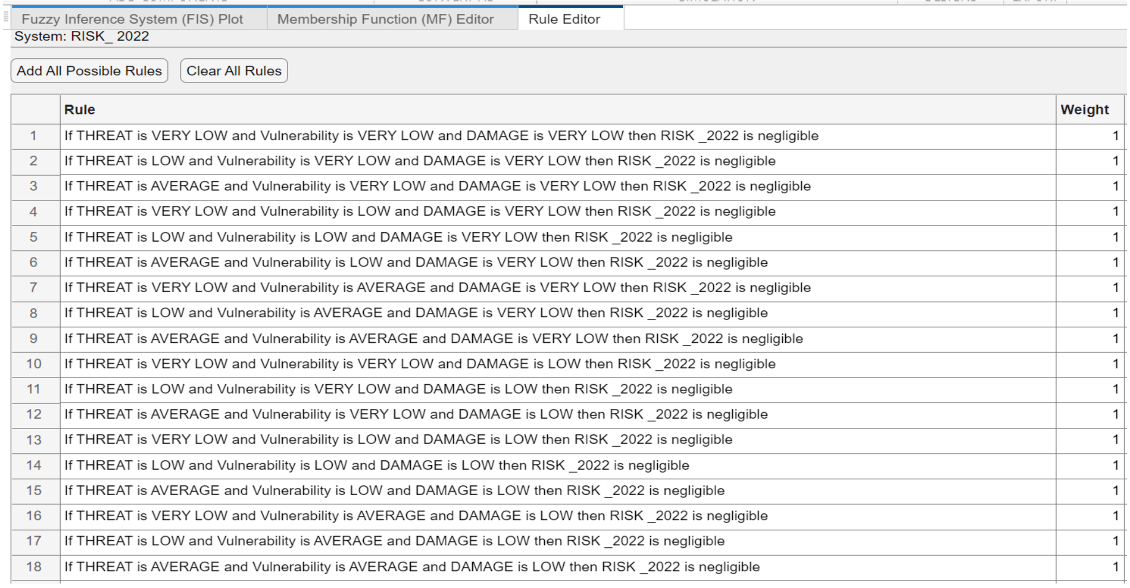
Opened system Exp_1, 119 rules

Figure 13. Risk assessment: R = f(x3, y1) y as a function of exposure levels and the overall probability of threat realization.

In this case, the training data are a numerical matrix of dimensions m × (n + 1) in which the number of rows m corresponds to the sample size, the first **n** columns correspond to the values of the input variables of the model, and the last column corresponds to the value of the output variable.

For definiteness, it is necessary to assume that, because of a preliminary survey, some estimates of the likelihood of a threat realizing itself, the magnitude of potential damage, and the degree of vulnerability have been obtained.

The fuzzy risk analysis model should contain 125 fuzzy inference rules for all possible combinations of fuzzy classes of input variables. Some of the rules are shown in Figure 14. Therefore, the fuzzy inference system contains three input variables with five terms, 125 fuzzy production rules, and one output variable with nine terms. To create an artificial neural network, you must first create a training data file (a plain text file with the **.dat extension*).

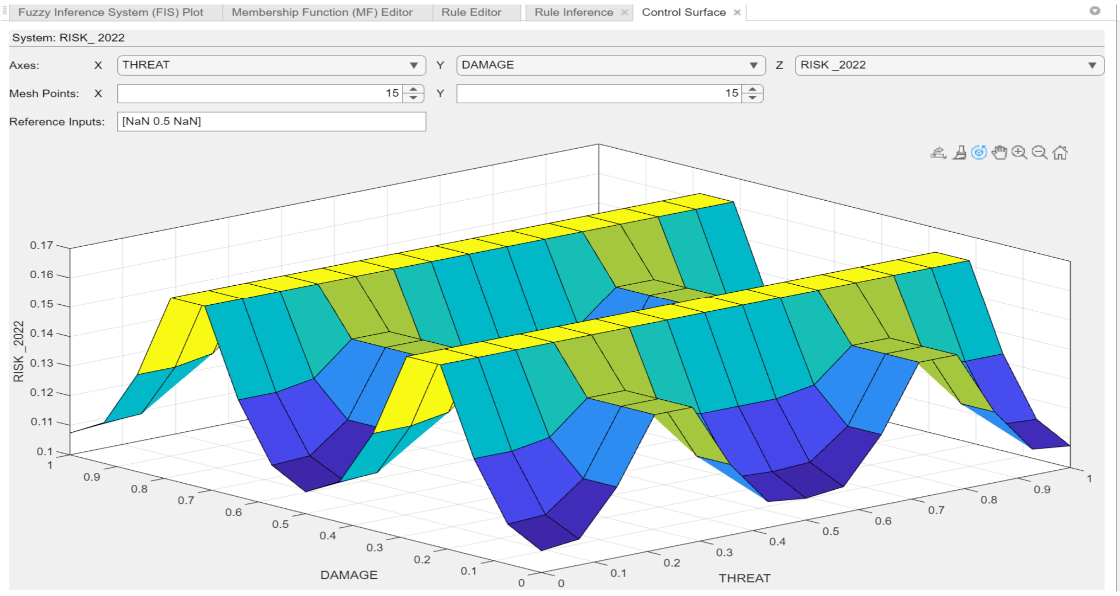

Fuzzy Inference System (FIS) Plot
Membership Function (MF) Editor
Rule Editor
Add All Possible Rules
Clear All Rules

System: RISK_ 2022

	Rule	Weight
1	If THREAT is VERY LOW and Vulnerability is VERY LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
2	If THREAT is LOW and Vulnerability is VERY LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
3	If THREAT is AVERAGE and Vulnerability is VERY LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
4	If THREAT is VERY LOW and Vulnerability is LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
5	If THREAT is LOW and Vulnerability is LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
6	If THREAT is AVERAGE and Vulnerability is LOW and DAMAGE is VERY LOW then RISK _2022 is negligible	1
7	If THREAT is VERY LOW and Vulnerability is AVERAGE and DAMAGE is VERY LOW then RISK _2022 is negligible	1
8	If THREAT is LOW and Vulnerability is AVERAGE and DAMAGE is VERY LOW then RISK _2022 is negligible	1
9	If THREAT is AVERAGE and Vulnerability is AVERAGE and DAMAGE is VERY LOW then RISK _2022 is negligible	1
10	If THREAT is VERY LOW and Vulnerability is VERY LOW and DAMAGE is LOW then RISK _2022 is negligible	1
11	If THREAT is LOW and Vulnerability is VERY LOW and DAMAGE is LOW then RISK _2022 is negligible	1
12	If THREAT is AVERAGE and Vulnerability is VERY LOW and DAMAGE is LOW then RISK _2022 is negligible	1
13	If THREAT is VERY LOW and Vulnerability is LOW and DAMAGE is LOW then RISK _2022 is negligible	1
14	If THREAT is LOW and Vulnerability is LOW and DAMAGE is LOW then RISK _2022 is negligible	1
15	If THREAT is AVERAGE and Vulnerability is LOW and DAMAGE is LOW then RISK _2022 is negligible	1
16	If THREAT is VERY LOW and Vulnerability is AVERAGE and DAMAGE is LOW then RISK _2022 is negligible	1
17	If THREAT is LOW and Vulnerability is AVERAGE and DAMAGE is LOW then RISK _2022 is negligible	1
18	If THREAT is AVERAGE and Vulnerability is AVERAGE and DAMAGE is LOW then RISK _2022 is negligible	1

Figure 14. The rule viewer's graphical interface after the fuzzy inference procedure.

The fuzzy inference system surface viewer allows you to view the surface of a fuzzy inference system and visualize plots of output variables versus individual input variables. An example of the appearance of the inference surface from the threat and damage variables is shown in Figure 15.


Fuzzy Inference System (FIS) Plot
Membership Function (MF) Editor
Rule Editor
Rule Inference
Control Surface

System: RISK_ 2022

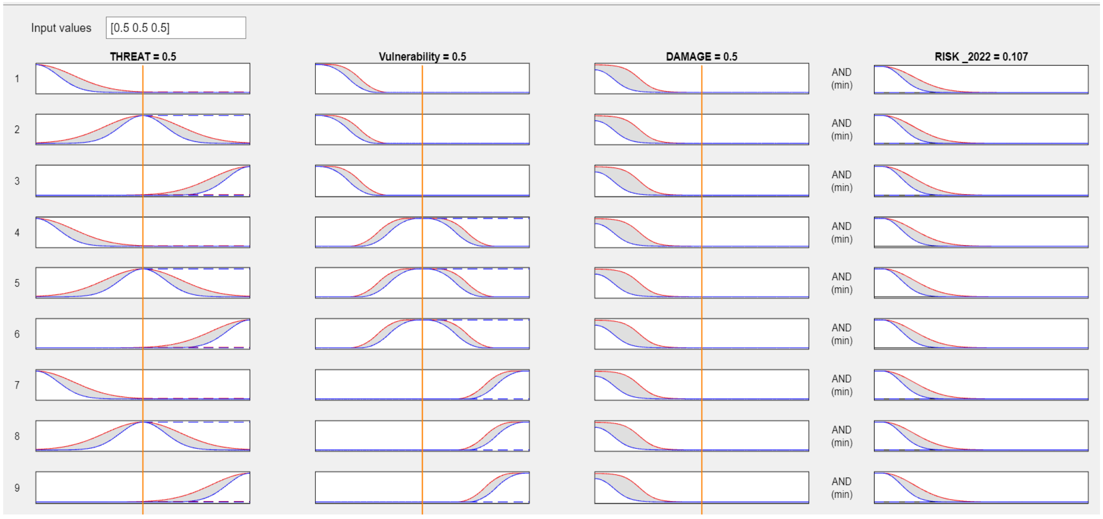
Axes: X THREAT Y DAMAGE Z RISK _2022

Mesh Points: X 15 Y 15

Reference Inputs: [NaN 0.5 NaN]

Figure 15. Visualization of the fuzzy inference surface of the model under consideration for the input variables "THREAT" and "DAMAGE".

The constructed ANS has flexible settings, is convenient and easy to use, and accurately and clearly displays the dependence of the level of information risk on the values of cybersecurity threats, potential damage, and social network vulnerabilities. The fuzzy inference procedure performed by the MATLAB system in the developed fuzzy model results in the value of the output variable being equal to 0.3, which corresponds to the standard configurations. The resulting surface allows you to analyze the dependence of the values of the output variable on individual input variables. Combinations of input variables are set in accordance with their placement on the axes of the coordinate system (refer to Figure 16).


Input values [0.5 0.5 0.5]

THREAT = 0.5

Vulnerability = 0.5

DAMAGE = 0.5

RISK _2022 = 0.107

Figure 16. Testing the built and trained artificial neural networks (ANN).

Modern solutions for automating a technological business process at critical social network infrastructure facilities are becoming more complex and use advanced technologies, which lead to an increase in the risks of security breaches up to the occurrence of extreme situations.

The processes of identifying, quantifying, analyzing, and assessing risks, as well as their processing, should be integral to the overall management decision-making process. Known vulnerabilities are to be identified by scanning and expert methods for checking the security of program code in the process of certification tests, as well as case studies on the security requirements of critical social network infrastructure objects.

Automated vulnerability search tools are also used to identify technical vulnerabilities. Moreover, generating a list of vulnerabilities applies the available results of security analysis and penetration testing.

Analyses of protection measures for each vulnerability provide quick elimination of vulnerabilities, minimizing or completely eliminating them safely for the business processes of social networks. To calculate the final risk rating (R), the methodology uses a matrix calculation method that aggregates all qualitatively assessed factors into one quantitative value. The risk rating (R), expressed as a number from 0 to 1, and the corresponding risk level, are determined according to Table 3.

Table 3. System for determining the appropriate rating (R) risk level.

Risk Rating	Low	Medium	High	Critical
R	$R < 0.25$	$0.25 \leq R < 0.5$	$0.5 \leq R < 0.75$	$0.75 \leq R$

This makes it possible to take into account not only the diversity of expert opinions, but also the difference in weights, which increases the objectivity of the assessment. Thus, the social network cybersecurity risk assessment model contributes to the solution of key tasks for ensuring cybersecurity:

1. The assessment result is a range of risk rating values, which makes it possible to compare the assessment results and rank them according to their level of importance.
2. It is possible to assess the dynamics of the risk level when a slight change in certain risk factors occurs.
3. The methodology is applicable to any scale of assessment.
4. The algorithm and evaluation criteria are clear enough for all users.
5. The process of evaluation by experts does not require large time commitments, and is simple and convenient to use.

4. Conclusions

Social networks are dynamic platforms and applications that rely heavily on data. This study considered some methodological issues that arise when an inquiry is conducted within the framework of assumptions about cyber risk assessment developed for practical application in a MATLAB environment. The algorithm for assessing cyber risks based on the application of the developed methodology consists of the following stages:

(1) The application areas include cybersecurity risk analysis, assessment, and management.

(2) According to the results of the computational experiment, the optimal methods for generating a set of training data for an artificial neural network and the method of its training are established.

(3) The requirements for the social network security risk assessment model used to form a set of training data for an artificial neural network are determined.

(4) The developed artificial neural networks can be used in real social networks to protect confidential information and build improved algorithms for their functioning.

Despite the small number of indicators selected, the fuzzy logic-based risk assessment showed a high degree of correlation with the results obtained from the standard regression analysis. The presented prototype of fuzzy logic-based risk assessment allows not only for solutions to the assigned problems, but also significantly expands the capabilities of modeling methods, and adequately uses qualitative and quantitative estimates of input parameters obtained from experts. This once again proves that fuzzy multiple models are very easy to build and provide reliable results, even in conditions of high uncertainty.

The methodology has broad capabilities that allow it to be adapted to various profiles of application systems and integrated into one's own development of risk management systems. Thus, the presented fuzzy multiple models fully satisfy the criteria for the adequacy of cyber risk assessment, and can be used to solve practical problems.

In the future, the practical significance of the risk assessment of the fuzzy multiple models will be determined by the implementation of the following:

1. An intelligent software package capable of implementing the developed numerical method and probabilistic model.
2. An intelligent software package for planning the technological business processes of social network objects in the context of digital transformation.
3. Development and implementation of new models and algorithms for automated control tasks.
4. Improvements in the software and hardware complexities of automated control systems.

Thus, in later studies, the unit of analysis could be extended to include cognitive modeling of the method for assessment of the risk, regardless of the category, to study the repercussions that social networks can have on the web traffic of cybersecurities. The proposed microcontroller-based model will be implemented with hardware and software in the future to assess the cybersecurity risks of critical social network infrastructure in real time.

Author Contributions: Conceptualization, A.A., Y.M. and R.N.; methodology, A.A., Y.M., R.N. and A.D.; software, A.A., Y.M., R.N. and A.D.; validation, A.A., Y.M., R.N. and M.Z.; formal analysis, A.A., Y.M., R.N. and A.K.T.; investigation, A.A., Y.M., R.N. and A.D.; resources, A.A., Y.M., R.N. and A.K.T.; data curation, A.A., Y.M., R.N. and A.D.; writing—original draft preparation, A.A., Y.M., R.N. and A.K.T.; writing—review and editing, A.A., Y.M., R.N. and A.D.; visualization, A.A., Y.M., A.K.T. and S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: In our work, data and studies that were used to support the findings of this research are included within this article and all the data are simulated data generated by the parameters in the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114&qid=1697471770811 (accessed on 16 October 2023).
2. Zio, E. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 137–150. [CrossRef]
3. Haimes, Y.Y. *Systems-Based Risk Analysis: Global Catastrophic Risks*; Oxford University Press: Oxford, UK, 2008; pp. 146–163. [CrossRef]
4. *ISO/IEC 27032:2012*; Information technology—Security Techniques—Guidelines for Cybersecurity. ISO: Geneva, Switzerland, 2012. Available online: https://www.iso.org/ru/standard/44375.html (accessed on 26 September 2023).
5. *ISO/IES 27032:2012*; Information Technology: Security Methods. ISO: Geneva, Switzerland, 2012.
6. *ISO/IEC 27005:2018*; Information Technology—Security Techniques—Information Security Risk Management. ISO: Geneva, Switzerland, 2018.

7. Zgoba, A.I.; Markelov, D.V.; Smirnov, P.I. Cybersecurity.Threats, Calls, Solutions. *Vopr. Kiberbezopasnosti* **2014**, *5*, 30–38. Available online: https://www.elibrary.ru/item.asp?id=22872258 (accessed on 26 September 2023).
8. Anikin, I.V. Fuzzy Assessment of Information Security Risk Factors. *IT Secur.* **2016**, *23*, 78–87. Available online: http://bit.mephi.ru/index.php/bit/issue/view/1 (accessed on 26 September 2023).
9. Chucklyaev, I.I. Scientific and methodological support of integrated risk management of violations of the security of functionally oriented information resources of information management systems. *Vopr. Kiberbezopasnosti* **2016**, *4*, 61–71. Available online: https://www.elibrary.ru/item.asp?id=27441076 (accessed on 26 September 2023). [CrossRef]
10. Deb, R.; Roy, S. A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets. *Expert Syst. Appl. Int. J.* **2021**, *183*, 115383. [CrossRef]
11. Mikov, D.A. Analysis of methods and tools which are used in the various stages of information security risk assessment. *Vopr. Kiberbezopasnosti* **2014**, *4*, 49–54. Available online: https://www.elibrary.ru/item.asp?id=22698877 (accessed on 26 September 2023).
12. Buldakova, T.I.; Mikov, M. Ensuring consistency and adequacy of assessment of information security risk factors. *Vopr. Kiberbezopasnosti* **2017**, *3*, 8–15. Available online: https://www.elibrary.ru/item.asp?id=29457217 (accessed on 26 September 2023). [CrossRef]
13. *ISO/IEC 27004:2016*; Information Technology—Security Techniques—Information Security. Management—Monitoring, Measurement, Analysis. ISO: Geneva, Switzerland, 2016.
14. *ST RK ISO/IEC 27005-2013*; Information Technologies. Security Methods. Information Security Risk Management. ISO: Geneva, Switzerland, 2013.
15. *IEC 31010:2019*; Risk Management—Risk Assessment Techniques. ISO/TC-262: Geneva, Switzerland, 2019. Available online: https://www.iso.org/standard/72140.html (accessed on 26 September 2023).
16. Fung, C.C.; Akbari Roumani, M.; Wong, K.P. A proposed study on economic impacts due to cyber attacks in Smart Grid: A risk based assessment. In *IEEE Power & Energy Society General Meeting*; IEEE: Piscataway, NJ, USA, 2013; pp. 1–5. [CrossRef]
17. Dorofeev, A.; Markov, A. Information security management: Basic concepts. *Vopr. Kiberbezopasnosti* **2014**, *1*, 67–73. Available online: https://www.elibrary.ru/item.asp?id=21288724 (accessed on 26 September 2023).
18. Rot, A. IT Risk Assessment: Quantitative and Qualitative Approach. In Proceedings of the World Congress on Engineering and Computer Science 2008, (WCECS 2008), San Francisco, CA, USA, 22—24 October 2008; Available online: https://www.researchgate.net/publication/44262457_IT_Risk_Assessment_Quantitative_and_Qualitative_Approach. (accessed on 26 September 2023).
19. Aven, T. *Quantitative Risk Assessment: The Scientific Platform*; Cambridge University Press: Cambridge, UK, 2011. [CrossRef]
20. Neural Network Toolbox. User's Guide. Version 4, 2002. The Math Works. Available online: http://cda.psych.uiuc.edu/matlab_pdf/nnet.pdf (accessed on 16 October 2023).
21. Massel, L.V. Fractal approach to knowledge structuring and examples of its application. *Des. Ontol.* **2016**, *6 Pt 2*, 149–161. [CrossRef]
22. Massel, A.G.; Gaskova, D.A. Application of risk-based approach to identify critical facilities in the energy sector with regard to cyber threats. In *Proceedings of the 19th International Workshop on Computer Science and Information Technologies*; Publisher Ufa USATU: Baden-Baden, Germany, 2017; Volume 1, pp. 159–163.
23. Maglaras, L.; Janicke, H.; Ferrag, M.A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors* **2022**, *22*, 5105. [CrossRef] [PubMed]
24. Yang, M. Information Security Risk Management Model for Big Data. *Adv. Multimed.* **2022**, *2022*, 3383251. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.