A Procedure for Assessing the State of Cybersecurity of Power Grids

Ihor Yakoviv[1[0000-0001-7432-898X]] and Vitaliy Tsyganok[2[0000-0002-0821-4877]]

[1] Institute of Special Communication and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[2] Institute for Information Recording of National Academy of Sciences of Ukraine, Kyiv, Ukraine
iyakov52@gmail.com, tsyganok@ipri.kiev.ua

Abstract. Intensity of implementation, diversity, and damage from complex cyber-attacks are constantly increasing. This process is further enhanced by ongoing expansion of attackers' scope of knowledge of the weak spots of computer networks and improvement of invasion technologies. Existing concepts of information system security assessment do not allow us to operationally consider changes of factors, which determine the efficiency of protection.Cybernetic segment of electric power grids has its own peculiar features, which, if properly taken into consideration, can improve the efficiency of security assessment.

We suggest an approach to development of a procedure for operative assessment of electric power grid cyber-security condition, based on knowledge of the relevant threat level and of particular features of the processes related to control of these grids.The paper includes the results of analysis of components of the suggested assessment system, and defines the fundamental principles of its functioning.

Keywords: Cyber-security, cyber-vulnerability, expert estimation, decision-making support, electric power grid.

1 Introduction

A series of cyber-attacks on the control systems of electric power supply infrastructure of Ukraine (power grid) was detected in 2015-2016. On December 23, 2015, when 225,000 clients of "Prykarpattyaoblenergo" joint-stock company got disconnected, we witnessed the first registered successful cyber-attack on the power system, which brought it out of service. Electric power systems are an important component of the national critical infrastructure. After these events many national security specialists from different states have to face the possibility of similar scenarios in their respective countries.A special place within the complex of activities on power supply infrastructure protection against cyber-attacks belongs to the procedure of current cyber-security situation assessment (further referred to as Assessment). As a result of this procedure a specialist, usually, has to get information (estimate) that would allow him to provide answers to the following questions:

- Is the level of protection adequate (inadequate) for the current level of cyber-threats?
- What is the extent of discrepancy between the current cyber-security level and the required level?
- Which actions should be taken in order to achieve the necessary level?
- How to define the security assessment procedure for the specific system, and to determine, whether it is adequate for the present situation?

Assessment procedure, in its turn, can be represented by the following interconnected procedures:

- Acquiring information on the current state of the assessment object (AO);
- Normalization of the acquired information in accordance to estimation scales (ES);
- Formation of estimates based on comparisons according to estimation criterion (criteria).

In the situation of growing intensity of new complex cyber-attacks on the critical infrastructure, based on constant expansion of knowledge of attackers on the vulnerabilities of computer systems, the problem of development of operational methods for electric power grid cyber-security state assessment becomes extremely relevant.

In order to fill the Assessment concept with specific content (meaning), we need to clarify the following aspects:

- What is the assessment object (AO);
- Which modern principles of cyber-security enhancement are used;
- How existing approaches to IT-system security assessment can be implemented to assess the cyber-security state of electric power grids.

Research objective is to define, analyze, and formalize the factors, which influence the system of operative evaluation of electric power grid's cyber-security condition.

2 Analysis of assessment object

Modern *power grids*have two basic components [1, 2]:

- Power component (generating, distributing, supplying electric power to users);
- Cybernetic (computer) component (monitoring of power processes and managing their state).

The power component includes [2]:

- Electric power stations (generating objects),
- Electric power sub-stations (electric power transformation by transformers and other equipment; distribution of electric power flows by commuting devices; control of electric power flow condition using different sensors and actuators);
- Electric power supply networks, which connect power stations with sub-stations and clients (consumers);
- Subscribers' metering devices.

The cybernetic component is generally called the Industrial Control System, or ICS. Depending on control scales and tasks, ICS, in their turn, are divided into [3]:

- Supervisory Control and Data Acquisition (SCADA) systems;
- Distributed Control Systems, DCS;
- Programmable Logic Controllers, PLC.

A PLC can be a part of a DCS, whilea DCS, in its turn, can be a part of a SCADA system.

For management of electric power supply operator's business processes separate information technology systems of management (ITSoM) are used. Due to cyber-security considerations, such systems should be distinguished from ICS [3], however in practice this rule is often violated.Well-known cyber-attacks on electric power grids of Ukraine were launched throughITSoM. This should be kept in mind in future, when determining the essence of cyber-vulnerability level assessment.For example, during clarification of assessment object composition we should distinguish between the situations when ITSoM is within the cybernetic component of the power grid and when it is not. At the first phase, it is appropriate to perform assessment for the case when the "cybernetic component is just the ICS", and at the second phase – for the case when the "cybernetic component is both ICS andITSoM".

3 Analysis of relevant cyber-security-ensuring principles

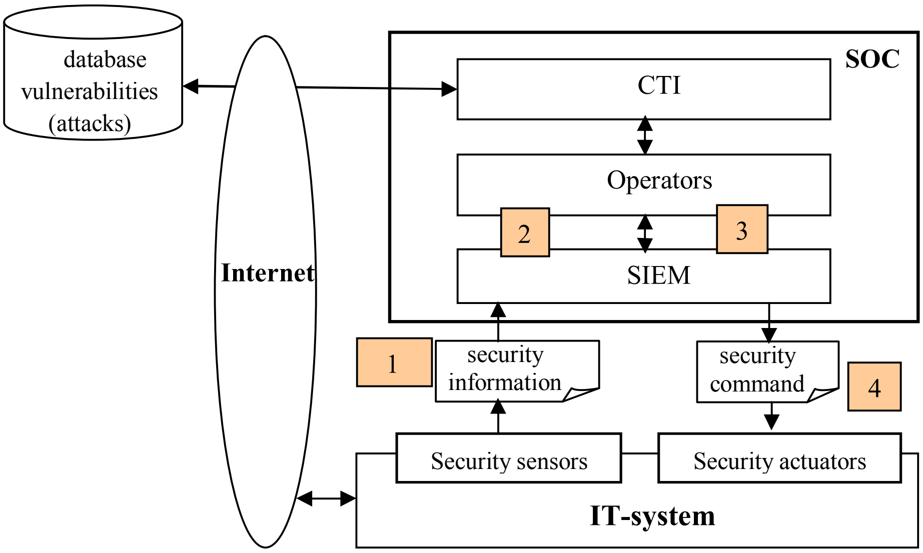
Analysis of existing corporate information and telecommunication system (ITC) protection practices allows us to single out two relevant strategies for cyber-attack counteraction: reactive defense and proactive (preventive) defense.The common basis for these strategies is provided by the following processes:

1) Observation (in real time) of the events within the assigned cyberspace segment;
2) Formation (using sensors), collection, and normalization of information on security-related events in the unified operative processing center;
3) Analysis of events and making decisions on whether the cyber-attack is taking place or not;
4) Making a decision on attack counteraction and implementation of this decision through security actuators (executive security devices).

Under reactive strategy, decision on attack detection is made after the attack ends. Counteractions might only help prevent a similar attack in future.Under proactive (preventive) protection strategy, the attack should be detected before it ends. Insuchcasethe time for implementation of activities to thwart (interrupt) the attack still remains.

The key part of modern cyber-protection systems is the Cyber-Security Operations Center (CSOC or SOC). Such centers, using operators and/or Security of Information and Event Management (SIEM) tools, with different degrees of automation, implement the above-listed processes 1-4. Ukrainian normative and legal documents in the field of information and telecommunication system protection neither explicitly define nor regulate real-time protection processes.As a rule, implementation of protection from unauthorized activities (UAA) within a complex information protection system (CIPS)is performed based on reactive protection strategy. Information on security events is formed by the complex of means of protection (CPM)from unauthorized actions based on criteria (features), determined back at development stage.Reaction (response) to security incidents is, as a rule, formed after the incident is over.

Figure 1 represents the structure and key information processes of the operative cyber-protection system.



SIEM – Security of Information and Event Management; CTI – cyber-threat intelligence
Processes: 1 – securityeventmonitoring; 2 – collection and analysis; 3 – decision on attack detection; 4 – decision on response and its implementation

Fig.1. Model of processes of real-time cyber-protection system

Consecutive fulfillment of cyber-protection processes 1-4 represents a cycle that is permanently repeated.In the beginning of the cycle Security sensors (based on Indicators of Compromise, IOCs) track security events (or compromise). In case of an event,security information is communicated to the SOC, where operators, using SIEM software tools, analyze it as to compliance with security policy. In the case when a cyber-attack is detected, a decision on counteraction is made. At the end of the cycle, Security actuators, based on received security commands,implement this decision.The background for sensor-based security monitoring isprovided by IOCs, detected by Cyber Threat Intelligence (CTI). The sources of IOCs may be external databases of threats and attacks (DataBase of Vulnerabilities/Attacks, DBV/A), or special methods of external/internal CTI organization.

Broad-scale implementation of complex cyber-attacks of APT (Advanced Persistent Threat) type against the national infrastructure became a powerful incentive for development of proactive protection methods based on SOC. Characteristic features of APTs are as follows.

- The attack represents a complex set of malefactor's actions, interconnected in space and time. When taken separately, these actions might not seem suspicious;
- The target action of the attack within the cyber-segment is prepared for a long time (from several months to a year or more);
- The combination of malefactor's actions is a chain of tactic steps, allowing him to achieve the goal of the attack. In spite of diversity of means, used in APTs, the set of most tactics and their essence remain the same.

All these factors contribute to development of constructive methods for proactive protection against APTs.

4 A model procedure for assessment of cyber-security state of power grid

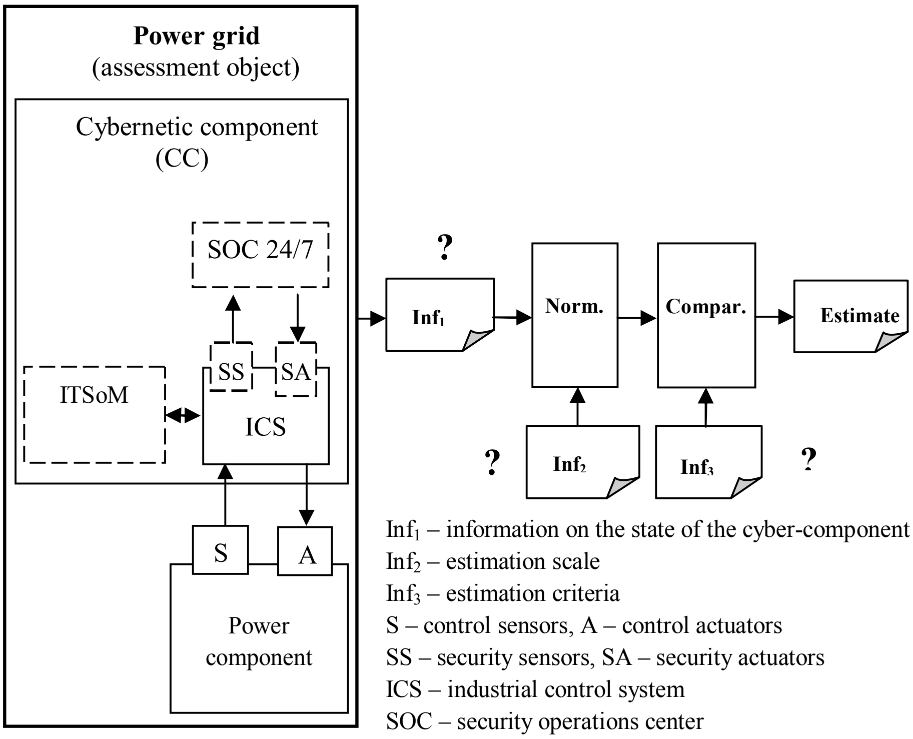
Above-mentioned analysis of modern real-time cyber-protection technologies allows us to perform further formalization. For this purpose, let us consider the assessment procedure as a system in the form of an information and functional structure (Fig. 2). Such a structure (model) is the first level of assessment procedure formalization.It allows us to specify the assessment problem through its decomposition into different situations (scenarios) according to certain features.

For example, according to "cybernetic component composition", the following list of situations can be compiled (further on we refer to it as the scale of situations of cybernetic component composition, SCCC, table 1).

Table1.

SCCC scale				
	CC-1	CC-2	CC-3	CC-4
ICS	+	+	+	+
ITS	-	+	-	+
SOC 24/7	-	-	+	+

For situationCC-2 the information on the current CC state (Infl) should reflect more parameters than for CC-1 (NCC-2 >NCC-1, whereNis the number of parameters). For CC-3 – NCC-3>NCC-2. Assessment for the situationCC-4 will be the most complex from the standpoint of SCCC scale. In terms of this scale the issue of Infl relevance is also very important. Ongoing rapid development of CC intervention technologies entails the need for increasing the assessment frequency, which can be represented by assessment period (TAS).Situations when the assessment frequency 1/TAS = 2 per year, 1/TAS = 2 per month, and 1/TAS = 2 per hour are significantly different from each other.In the first two cases there is time for implementation of expert estimation methods to form Infl (that is, information based on knowledge of the present situation, obtained from competent specialists, i.e. experts in the areas of cyber-security).In the latter case, there is no time to use expert data-based approaches.



Inf$_1$ – information on the state of the cyber-component
Inf$_2$ – estimation scale
Inf$_3$ – estimation criteria
S – control sensors, A – control actuators
SS – security sensors, SA – security actuators
ICS – industrial control system
SOC – security operations center

Fig.2.A model (information and functional structure) for assessment of cyber-security state of electric power grids

At subsequent phase we have to addressthe question of semantic content of information being used (Infl, Inf2, Inf3–?). If information is anattribute (a set of attributes) of an object, reflected in another object (attributive-transfer approach to the essence of information, [4]), then the semantic (sense) of Inf2 (estimation scale) will be a set of security parameters, characteristic for the given ICS, which were predefined based on cyber-security policy. Semantic of Inf3 (estimation criteria) will be the set of values of security parameters, predefined by security policy for the given ICS. According to the logic of assessment structure under consideration, semantic meaning of Infl (current information on the CC) for situation CC1 will be the current values of monitored parameters in the estimation scale (Inf2).Once normalized, these current values are compared to cyber-security criteria for the given ICS.Based on results of these comparisons, the overall estimate of cyber-security state is formed.

In addition, we should note that there is other necessary information, not reflected in the structure, which, nevertheless, should be taken into consideration within assessment procedure. We are talking about the list of possible security parameters, based on which we can form estimation scales for different ICS configurations.Let us call this information the “alphabet of ICS parameters”,Inf4.

Adequacy of the suggested model (structure) can be determined if we compare it to the existing model of information and telecommunication system security assessment (this term is used in the national Ukrainian normative documents, and its meaning is similar to the term “IT-system”). Procedure for assessing ITS protection against unauthorized actions is regulated by such documents as НД ТЗІ 2.5-004-99 and НД ТЗІ 2.5-005-99 (ND TPI – the normative document on technical protection of information) [5, 6]. The essence of the existing ITS assessment procedure can be briefly described as follows[7]:

a) there is a structured general set of protection services (SPS). Every service corresponds with a respective known threat. The services are implemented by the respective protection means.All protection services are divided into 4 groups, depending on the types of basic threats: 1) information confidentiality breach (C); 2) integrity violation (I); 3) accessibility (availability) violation (A); 4) observability violation (O);

b) based on the general SPS and selected security policy, the functional set of services for a specific ITS is formed (the so-called functional protection profile, FPP, of theITS), which complies with the key protection tasks;

c) according to the FPP, protection system developer defines and installs certified protection tools within the ITS;

d) the estimate of security state is formed as part of the national expert examination based on verification of correspondence between the developed protection system and the previously developed FPP.

Table 2 presents the results of comparison of the suggested assessment model and the existing ITS security assessment procedure.

Table2.

	ITS security assessment procedure	**Amodelofpower grid security assessment**
1	Structured general set of protection services (SPS)	Alphabet of ICS cyber-security parameters (Inf$_4$)
2	Functional protection profile, FPP	Estimation scale (Inf$_2$)
3	Every service of the SPS should be implemented within the ITS protection system	Estimation criteria (Inf$_3$)
4	Availability of the protection service in the protection system (information is defined in the process of state expert examination)	Current information on ICSstate (Inf$_1$).

Each kind of information, defined within the suggested model (information and functional structure) of electric power grid cyber-security assessment corresponds with an information object from the existing procedure of ITS security assessment.The difference of the procedures should be determined through additional studies, which would take the following aspects into consideration:

- peculiar features of power (PC) and cybernetic (CC) component structures;
- peculiar features of interaction between PC and CC;
- requirements to efficiency of assessment procedure for ICS.

Specific features of interaction between PC and CC can be analyzed based on the model of information processes in a cybernetic system and criteria of their security [8]. At the same time, approaches to formalized representation of cyberspace and cyber-security should also be taken into account [9].

5 Technology for group decomposition of a problem and expert evaluation

When the frequency of information change allows us to allocate the time for preliminary analysis (not in real-time mode), it is appropriate to use technologies, in which knowledge of experts and knowledge engineers is engaged for construction of a subject domain model. Such a model can be a constructed as a hierarchy of criteria through decomposition process [10].Based on this model it is possible to assess the state of cyber-vulnerability of critical infrastructures.

5.1 The essence of technology

The technology is intended for use in weakly structured domains where information for substantiate decision making is insufficient and knowledge in the field is significantly limited, non-formalized, and, mostly, distributed among highly specialized experts. The technology is currently implemented as a web-based distributed computer system [11], which allows knowledge engineers (expert session organizers) and experts to work together remotely and provide knowledge, required to build an adequate model.

The technology involves the following stages:

- Formulation of the main criterion of evaluationby expert examination organizer (decision-maker);
- Formation of a group of competent experts for the examination;
- Decomposition of the main criterion by the expert group. This stage is divided into the following sub-stages:
  - Formulation by each individual member of the expert group of a set of factors that, in his / her opinion, significantly influence formation of the estimate according to the criterion (the relative impact of a sub-criterion should amount to at least 10%);
  - When each of the experts participating in the examination has formed a set of components of the criterion (most significant from his / her point of view), the expert examination organizer performs grouping of all experts' formulations according to their semantic similarity;
  - Group choice of (by voting for) the best formulation in each group of formulations with the same semantics. Voting provides an opportunity to vote for one of

the formulations, or refuse to chooseany of the formulations provided by members of the group (if, according to the voter, the influence of the respective factor upon the given upper-level criterion is not significant enough, he can refuse to make a choice).

As a result of this stage, the group of experts, coming to a consensus, forms the set of the most important factors influencing a certain criterion. In the beginning, this is the main criterion, formulated by the decision-maker (organizer), and in the process of subsequent decomposition, this may be any criterion, division of which into components makes sense. Thus, interconnected components form the generalized criterion for evaluation.

Decomposition of the main criterion is carried out as a result of the repeated iterative process, which is controlled by the expert examination organizer. This person, as a knowledge engineer, decides, whether it is necessary to further decompose criteria, that make up the components of the assessment system. For every such decomposition, a separate group of experts (who are most competent in the current issue under consideration) may be formed [12]. The decision to stop criterion decomposition process is made by the knowledge engineer in the case when it is possible to obtain easily measurable, preferably, quantitative, indicator, characterizing the system according to this criterion.

- Group expert evaluation of the mutual influences of the criteria in the evaluation system. At this stage, groups of experts, who conducted the respective particular decomposition, evaluate relative direct impacts of factors upon higher-level criteria in the hierarchy. As a result, relative impacts of all criteria in the hierarchy are determined (using the methods of group expert evaluation).

Once this final stage is completed, the model of the evaluation (assessment) system can be considered fully constructed.Now, based on this model, which is the structure of interconnected factors of different significance, it is possible to determine the relative value of the estimate by the main criterion.

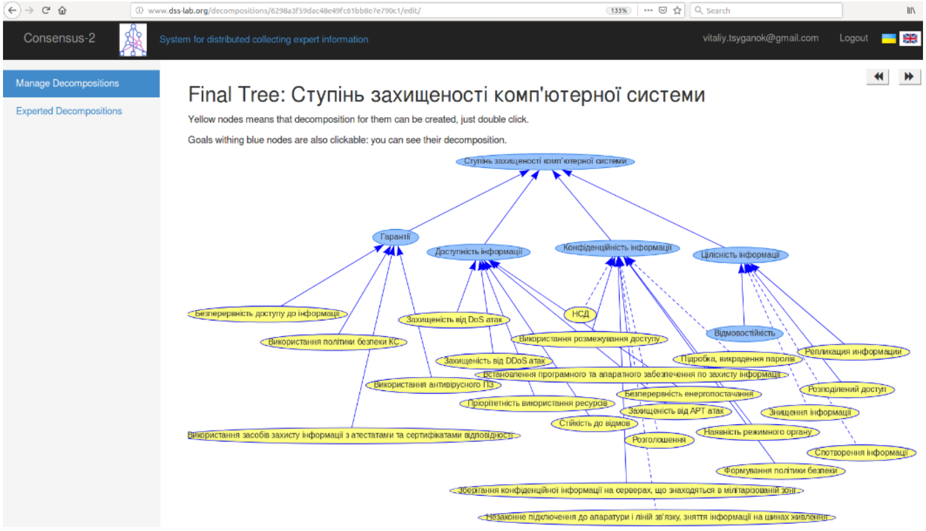
5.2 Anexample of power grid cyber-vulnerability state assessment

Let us illustrate the application of technology and the functioning of the systembythefollowing hypothetical example.

Let us assume, the knowledge engineer (a user, registered in the "Consensus-2" system, with authority given by the expertise organizer (decision-maker)), formulated the main criterion for assessing the state of cyber-vulnerability of electric powergrid as "The level of protection of the cybernetic component of the power grid". The examination organizer, having appropriate rights in the system, authorizes a group of users to work as experts.

After proper authentication, each expert, in accordance with his / her pertinent knowledge level, formulates a list of the most important factors that influence the level of protection of the cybernetic component of the power grid. Following the mutual harmonization and unification (generalization) of the knowledge, provided by the experts, the following formulations of the criteria-components of the evaluation system are selected as the most appropriate ones: "preserving the integrity of information", "protecting the confidentiality of information", and "ensuring the availability of information". At this stage, the knowledge engineer has the opportunity to identify these components of the system without consulting the experts, since such a decomposition is provided in guidance documents on the organization of cyber defense [3].

Next, each of the above-listed criteria is decomposed by a separate group of experts. As a result, decomposition is completed. Within the graphical interface of the expert session organizer the decomposition result might look as shown on Fig.3.



Final Tree: Ступінь захищеності комп'ютерної системи

Yellow nodes means that decomposition for them can be created, just double click.

Goals withing blue nodes are also clickable: you can see their decomposition.

www.dss-lab.org/decompositions/6298a3f59dac48e49fc61bb8e7e790c1/edit/
133%
Search
Consensus-2
System for distributed collecting expert information
vitaliy.tsyganok@gmail.com
Logout
Manage Decompositions
Experted Decompositions
Ступінь захищеності комп'ютерної системи
Гарантії
Доступність інформації
Конфіденційність інформації
Цілісність інформації
Безперервність доступу до інформації
Захищеність від DoS атак
НСД
Використання політики безпеки КС
Використання розмежування доступу
Відмовостійкість
Підробка, викрадення паролів
Репликация информации
Захищеність від DDoS атак
Встановлення програмного та апаратного забезпечення по захисту інформації
Використання антивірусного ПЗ
Безперервність енергопостачання
Розподілений доступ
Пріорітетність використання ресурсів
Захищеність від APT атак
Знищення інформації
Стійкість до відмов
Використання засобів захисту інформації з атестатами та сертифікатами відповідності
Розголошення
Наявність режимного органу
Спотворення інформації
Формування політики безпеки
Зберігання конфіденційної інформації на серверах, що знаходяться в мілітарізованій зоні
Незаконне підключення до апаратури і ліній зв'язку, зняття інформації на шинах живлення

Fig. 3. Visual representation of the developed evaluation system modelwithin the interface of "Consensus-2"system

Once the weights of the arcs in the graph are obtained (as values of relative impact coefficients, determined through group expert evaluation), we get a weighted hierarchy of criteria – a complete model for assessing the cyber-vulnerability of power grids.

At the lower levels of the hierarchy of criteria, we have objective parameters(indicators) of the system that the expert groups have identified as decisive, basic ones for this evaluation. If we take such indicators for existing systems, and perform calculations using available complex target-oriented dynamic alternative evaluation methods [13], we obtain the relative indices of the state of cyber-vulnerabilities of specific power grids. For the case when we have to evaluate one single power grid, the evaluation is conducted in comparison with the established standard (benchmark) – a hypothetical ideally protected system.

The described hierarchical network models allow us not only to perform comparative assessment of the state of cyber-vulnerabilities in power grids, but also to optimize allocation of resources, targeted at implementation of measures to improve cyber-security of systems, and to build long-term cyber-defense organization plans for critical infrastructures [14, 15].

Conclusions

An original approach to the development of a procedure for assessing the state of cyber-security of power grids is proposed. The approach is based on knowledge of the level of actual threats and the peculiarities of the management processes in these systems.It is also based on real-time cyber-protection models and the system of cyber-security state assessment, developed in the process of research.The models allow us to classify the complexity of assessment procedures for different objects according to the following properties:

- Cybernetic component content;
- Information of assessment procedure and its semantic meaning;
- Time of assessment procedure information updating.

Based on the suggested approach, we can define the structure and content of cyber-security assessment of a specific power grid, and verify the correctness of information forming in assessment procedures.For instance, in grids, where cyber-component includesreal-time protection system, information on system state should be formed and processed with automation means (based on objective data, generated without experts' participation).However, experts can still participate in the formation of estimation scale and criteria.

For performing assessment,we provide an opportunity to use group decomposition technology, implemented within a distributed decision support system. The technology allows us to utilize the subjective experience of the experts.

References

1. NISTIR 7628 Revision 1. Guidelines for Smart Grid Cybersecurity. National Institute of Standards and Technology Interagency Report 7628 Rev. 1, Vol. 1 290 pages (September 2014).
2. Yuning Jiang; Manfred Jeusfeld; YacineAtif; Jianguo Ding; ChristofferBrax; Eva Nero. "A Language and Repository for Cyber Security of Smart Grids", 22nd IEEE Enterprise Computing Conference", 2018 10. 16-18, Stockholm, Sweden.
3. Stouffer Keith, Falco Joe, ScarfoneKaren Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology.*NIST Special Publication 800-82*Rev. 2 (as of August 12, 2015)accessed onhttp://dx.doi.org/10.6028/NIST.SP.800-82r2 .
4. IhorYakoviv, "The communication channel from the position of attributive-transfer nature of the information", *Information technology and security*, vol. 1, iss. 2, pp. 84-96, 2012. Kyiv, Ukraine: Institute of special communications and information security NTUU "Igor Sikorsky KPI". [Online]. Available: http://its.iszzi.kpi.ua/issue/view/2838 .

5. ND TPI 2.5-004-99 Criteria for assessing the security of information in computer systems from unauthorized access. Approved by order of DSTSZI of the Security Service of Ukraine dated April 28, 1999 No. 22. (in Ukrainian НДТЗІ 2.5-004-99)
6. ND TPI 2.5-005-99 Classification of automated systems and standard functional profiles of protection of the processed information from unauthorized access. Approved by order of DSTSZI of the Security Service of Ukraine dated April 28, 1999 No. 22. (in Ukrainian НДТЗІ 2.5-005-99)
7. Igor Yakoviv, Fundamentals of building a comprehensive information security system for the information and telecommunication system. Tutorial. - Kyiv: National Technical University of Ukraine "KPI named after Igor Sikorsky", 2016 – 88p. (in Ukrainian)
8. Igor Yakoviv, "The base model of informational processes of management and safety criteria for cybernetic systems", *Information technology and security*, vol. 3, iss.**1**(4), pp.68-73, 2015. Kyiv, Ukraine: Institute of special communications and information security NTUU "Igor Sikorsky KPI". Available: http://its.iszzi.kpi.ua/article/view/57735/53977 .
9. IhorYakoviv, "Infocommunication system, conceptual model of cyberspace andcybersecurity".*Information technology and security*, vol. 7, iss.1(4), pp.68-73, 2017. Kyiv, Ukraine: Institute of special communications and information security NTUU "Igor Sikorsky KPI". Available: http://its.iszzi.kpi.ua/article/view/57735/53977 .
10. Saaty T.L. The Analytic Hierarchy Process: planning, priority setting, resource allocation / N.Y.: McGraw Hill. – 1980. – 287 p.
11. Свідоцтво про реєстраціюавторського права на твір №75023. Комп'ютернапрограма „Система розподіленогозбору та обробкиекспертноїінформації для систем підтримкиприйняттярішень – «Консенсус-2»" / Циганок В.В., Роїк П.Д., Андрійчук О.В., Каденко С.В. // від 27/11/2017.
12. Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / ИПРИ НАНУ. – К.: Наукова думка, 2002. – 382с.
13. Циганок В.В. Удосконалення методу цільовогодинамічногооцінювання альтернатив та особливостійогозастосування.*Реєстрація, зберігання і обробкаданих*. 2013. т.15, №1.– С.90-99.
14. Tsyganok V, Kadenko S, Andriychuk O, Roik P. Usage of multicriteria decision-making support arsenal for strategic planning in environmental protection sphere. *J. Multi-Crit.Decis. Anal.* 2017; pp. 227–238.
15. Tsyganok V.V., Kadenko S.V. &Andriichuk O.V. Using different pair-wise comparison scales for developing industrial strategies.*International Journal of Management and Decision Making*. – 2015. – vol. 14, issue 3. – P. 224-250.