Reliability Components of the WAMS Information Network

M.I. Uspensky[1]*

[1]ISE&EPN. Komi SC, Ural Division, RAS, Syktyvkar, Russia

Abstract: Power system modes can be controlled by use of a wide-area monitoring and control system (WAMS). It is based on the phasor measurement units (PMUs), connected by an information network covering a significant territory. The functioning reliability of such a network determines to a big extend the correct operation of the entire monitoring system. To assess its reliability, the one can be decomposed conveniently into four components: hardware or technical reliability, traffic reliability, software reliability, resistance to external negative impact on the transmitted information, and to consider each m independently. In this paper, the main attention is paid to assessment of the reliability and availability of the first three components in the information network.

The need for a correct assessment of the power system state has led to the creation of the Wide Area Measurement Systems (WAMS). It is based on the measuring technology of phasors (phase vectors), on the Phasor Measurement Unit (PMU) by the signal of global navigation systems, which ensures the simultaneous measurement of phasors [1]. WAMS includes measuring transformers, PMU, Phasor Data Concentrators (PDCs) and equipment of the local information network. They allow to control the power system behavior by continuous observation over systemic events. The WAMS operation reliability is determined by the element reliability of the monitoring system.

The paper considers the WAMS network structure, and proposes the assessment of their reliability based on the network links. A network failure is determined by the loss of terminal communication, and this concept includes not only the absence of such a connection, but also the distortion of the transmitted information. Then the network reliability includes four components, as fellows:

1) Hardware or technical reliability associated with the failure (destruction) of transmission channel elements or the integrity of communication lines;

2) Traffic reliability, determined by the temporary data loss or distortion without failure of the transmission channel element;

3) Software reliability due to errors in the development of exchange execution programs; and

4) The opposition to the external targeted influence on the transmitted information. This paper considers first three reliability components of the WAMS information network. The paper includes the example of an application for assessing the availability of a 10-bus system network [2] from the positions under consideration. Optical fiber or the high frequency channels through power lines are adopted as the carriers in the example.

The WAMS network hardware is network communications, the PMU and PDC electronics. Since the operation of the central processor units and the PDC communication interface during duplication is similar to the operation of these elements in the PMU, we use the reliability estimate of these units in [3], obtained from the Markov system of probability equations for state, taking into account different lengths of the main and backup communication channels. Then the network link availability from the duplicated information source (PMU, PDC or, if necessary, an intermediate amplifier) and the lines of the communication channel can be defined as

$$A_{ch} = A_{PDC} \cdot A_{com}, \tag{1}$$

where

$$A_{PDC} = \frac{\mu_{PDC}^2}{(\mu_{PDC}+\lambda_{PDC})^2}, \tag{2}$$

since PDCs are the same type, and

$$A_{com} = \frac{\mu_{lm} \cdot \mu_{lb}}{(\mu_{lm}+\lambda_{lm})(\mu_{lb}+\lambda_{lb})}. \tag{3}$$

Here A_{PDC} is the availability of the duplicated information source, λ_{PDC} and μ_{PDC} are the failure and recovery rates of the source, respectively. The physical availability of information carriers (twisted pair, optical fiber, high-frequency channel), each element of which is characterized by the length l_i, specific failure rate the main – λ_{lm} and backup – λ_{lb} lines, average recovery time of the main – r_{lm} and backup – r_{lb} lines per km, should also be included here. Since the reliability indicators of communication lines λ_{ln} and r_{ln} approximately linearly depend on the link length, and $\mu_{ln} = 1/r_{ln}$, then the working state probability of the information carrier element (communication availability for line *i*) is easy to evaluate as

$$A_{ln,i} = \frac{\mu_{ln,i}}{(\mu_{ln,i}+\lambda_{ln,i})} = \frac{1/(r_{ln,i} \cdot l_i)}{1/(r_{ln,i} \cdot l_i)+\lambda_{ln,i} \cdot l_i} = \frac{1}{1+\lambda_{ln,i} \cdot r_{ln,i} \cdot l_i^2}. \tag{4}$$

It should be noted that r_{ln} includes two components: the variable in the search for violations, depending on the distance; and the constant associated with the restoration. Since the second component has small values, we neglect it. Therefore, the communication line availability is inversely proportional to the square of line length. Unlike duplication in electronics, where the backup device usually repeats the main one, duplication of information carrier is provided most often by elements of various reliability in-

---

* Corresponding author: uspensky@energy.komisc.ru

dicators. This is because in normal mode the communication is provided via the shortest line in the communication network, and in the backup mode case the information goes through the remaining in the communication network, which can be significantly longer than the main one. Moreover, the approach in solving this problem is the same as at duplicating electronic components (2), only taking into account the different values of λ_j and μ_j for the j^{th} connection (3).

The algorithm for the calculation is as follows. After setting the initial data on the known link lengths of the information channels and the necessary reliability parameters, a table of the link participation in the formation of the main and backup channels is compiled (see the example of Table 1). Next, the link reliability characteristics (λ_j, μ_j and A_j for the j^{th} link) are calculated, the same parameters are determined for the main and backup information exchange channels and the availability and characteristics of channels with redundancy are calculated. At the same time, all changes are determined in the network configuration by the source data and the link participation table. The estimated part remains unchanged.

Table 1 Routes for the main and backup channels of information exchange

Source node	Main channel	Backup channel
1	1-7-4	1-9-8-6-4
2	2-7-4	2-9-7-4
3	3-4	3-5-4
5	5-4	5-6-4
6	6-4	6-5-4
7	7-4	7-6-4
8	8-6-4	8-9-7-4
9	9-7-4	9-8-6-4
10	10-2-7-4	-

Hardware reliability indicators were obtained for the test power system at the information network diagram in Fig. 1 and are given in [4]. Here we only note that with a complex network of information communications, it can find the backup connection from the server node to the node with the failed link, excluding the last one. To do this, we use the search algorithm first in depth and then in breadth, as proposed in [5]. It allows to take into account the failed links to find a backup route, if one exists, or to warn of its absence. When searching, the "Reserve channel" column of the Table 1 is built and the hardware found path reliability is evaluated. These backup routes are stored in Table 1 in the order of the decreasing reliability. A similar operation is performed in the process of network building. In a real mode, if necessary, a backup channel with operational connections and highest availability is used.

Traffic reliability lies in the information transmission in due time without losses and distortions associated with the loading of the exchange channel. Losses due to traffic are caused by an unacceptable delay or loss of some information due to an overload of the information channel, but are not associated with the element device failure of this channel, which is taken into account in hardware reliability. Therefore, the traffic reliability is determined by the choice of bandwidth, taking into account the delay of transmitted information.

The information frame from the generation unit or power line, formed by each PMU, combines 9 vector measurements: 3 currents and 3 voltages (magnitude and phase), 3 powers (active and reactive components); 2 analog values: generator excitation current and voltage; the PMU state and the state of the switching elements. In addition, the transmission package includes the frequency and speed of its change, the time stamp and the binding for interaction with the information network in standard C.37.118-2011. The structure of the data frame is given in Table 2.

Table 2 C37.118-2011 frame structure

Field	**Size**
Sync byte (SYNC)	2 bytes
Byte number of frame (FRAMESIZE)	2 bytes
Identifier PMU (IDCODE)	2 bytes
Second counting (SOC)	4 bytes
Fraction of a second/quality flag (FRACSEC)	4 bytes
Status flag (STAT)	2 bytes
Vectors (PHASORS)	$8 \cdot n$ bytes (floating point)
Frequency (FREQ)	4 bytes (floating point)
Frequency change rate (DFREQ)	4 bytes (floating point)
Analog data (ANALOG)	$8 \cdot m$ bytes (floating point)
Digital data (DIGITAL)	$2 \cdot l$ bytes (discrete values)
Cyclic Redundancy Check (CHK)	2 bytes

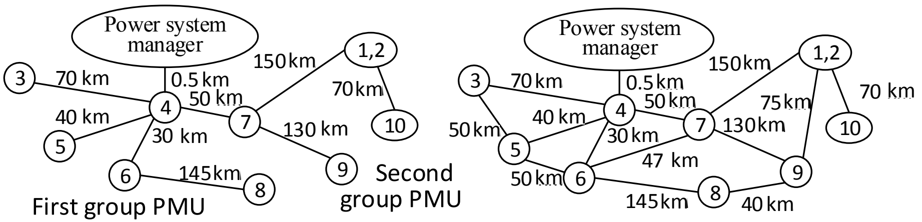
l – number of discrete information sources; *m* – number of analog information sources; *n* – synchronized vectors (magnitude and phase).

Then the amount of information from one PMU takes $b_{in} = 8 * 9 + 2 * 8 + 2 + 2 = 92$ bytes. The amount of additional information per frame of one bus is $b_{fr} = 6 + 8 + 8 + 2 = 24$ bytes. Depending on the PMU number - sources of measurement information and transmitted measurements per second, the packet volume often lies in the range of 100 - 400 bytes. The approximate channel bandwidth in Kbit/s is given in Table 3 depending on the number of source devices and the sampling rate taking into account a margin of 10%, [6]. In this case, 1Kbit = 1024 bits.

Table 3 Required channel bandwidth, Kbit/s

Samples per second	Number of PMU's			
	2	10	40	100
25	50	249	997	2392
50	100	499	1994	4984
100	200	997	3988	9969

The delay in information is related both with the type of the exchange channel and with the time of unloading its receive buffer. Packet delivery to a



a) b)

Fig. 1. Communication channels: a) without redundancy, b) with redundancy.

receiver requires time consuming, T_d, which is determined by the signal propagation time, T_{pc}, the packet transmission time over the communication line T_{pt} and the time of waiting for the packet in the queue in the communication unit T_{wp}.

$$T_d = T_{pc} + T_{pt} + T_{wp}. \tag{5}$$

The signal propagation time, T_{pc}, in most communication systems is determined by the propagation time of the optical or electric signal (electromagnetic field). The pulse delay in the optical fiber is (3.5–5) $*$ l (ns) [7], and in the copper wire 5 $*$ l (μs) [8], where l is the channel length in km.

The packet transmission time T_{pt} depends on the data transfer rate on the communication line v_{tr} (Kbit/s) and the volume or length of the packet L_p (Kbit)

$$T_{tp} = L_p/v_{tr}. \tag{6}$$

Obviously, the propagation speed depends only on the channel material; therefore, the propagation time on the channel is constant. Transmission time depends only on the packet length.

The main task in designing a data transmission network is to ensure the balance between traffic (request flow λ, in our case, measurement frequency), the amount of network resources (bandwidth) and the quality of service (service flow μ, request processing parameter). In solving this problem, two model levels of interaction for the open systems (OSI) are considered: network and channel layers.

Network layer. At the network layer traffic transit routes in the network are considered. For this, it is convenient to describe the communication network as the graph model [9] (in this case, non-oriented), in which the network nodes (routers) correspond to the graph vertices, and the communication lines to the graph arcs. The transmission time to the receiving node is the time that the packet spends on the network line. This time is random to a certain extent.

The intensity of the load on the network graph arcs ρ_{ij}, determined by the ratio λ_i/μ_j of the flow request intensity from the node-information source i to the flow service intensity by the receiver node j, depends on the number of devices and the amount of information from each device. In our case, the flow request intensity is determined by the measurement frequency in the power system bases: $\lambda = f_{msr} = \frac{1}{T_{msr}}$. The flow service intensity is the back volume of the packet delivery time: $\mu = \frac{1}{T_d} = \frac{1}{L_p/v_{tr}+T_{pc}}$, and since this time is less than the application period, then $T_{wp} = 0$. Otherwise, information will be lost. On the other hand, the receiver electronics creates an additional delay T_{re} on average of about 5 μs.

$$\rho_{ij} = \frac{L_p/v_{tr}+T_{pc}+T_{re}}{T_{msr}}\ . \tag{7}$$

Channel level. At this level, it is required to evaluate the necessary bandwidth of communication lines between network nodes. In the general case, an approximate formula can be used to estimate the probability of losses [10]

$$q_{ij} = \frac{1-\rho_{ij}}{1-\rho_{ij}^{N_j+1}}\rho_{ij}^{N_j}, \tag{8}$$

where N_j is the number of sections in the receiver accumulator j; ρ_{ij} is the load intensity of line ij. The absence of losses is defined as

$$p_{ij} = 1 - q_{ij}. \tag{9}$$

It is clear that such an assessment corresponds to one information line connecting two nodes. Taking into account the serial connection of channel links for two nodes passing through intermediate nodes, the overall assessment of the probability of information loss is defined as

$$P_\Sigma = \prod_{ij} p_{ij}. \tag{10}$$

Let us evaluate the WAMS information channels for a 10-bus test power system, which is given in detail in [2]. A map of information links with a distance scale is presented in [4], and a diagram of information links is presented above in Fig. 1. All information communications are made by fiber with a propagation delay of T_{pc} = 5 ns/km. Electronics Delay T_{re} = 5ms. Baud rate v_{tr} = 1 Mbps = 1048576 bps [11]. The measurement transmission frequency is 10 Hz or T_{msr} = 0.1 s. Since the power system manager is defined in the system bus 4, the information routes in the normal and failure mode of one information transmission line are given in Table 1, and the last column shows the connection of the node-source to node # 4 in the failure event of one component link along the route. Note that a communication failure of 10-2 leads to a complete loss of the information exchange with node 10. The initial data for the calculations are summarized in Table 4. Here in the third and fourth columns b_{in} and b_{fr}, the number is associated directly with the corresponding line, and Σb^{nr} and Σb^{em} are groups of bytes, including intermediate packets for the communication in question, both normal and emergency, associated with the failure of one of lines. N is determined by the maximum frames in normal mode and equals 5.

Table 4 Input data on the information network

Link	***l*, km**	b_{in}	b_{fr}	$\sum b_{in}^{nr}$	$\sum b_{fr}^{nr}$	$\sum b_{in}^{em}$	$\sum b_{fr}^{em}$
1-7	150	2	1	2	1	5	3
2-9	75	2	1	3	2	5	3
10-2	70	1	1	1	1	1	1
3-4	70	6	2	6	2	6	2
3-5	50	0	0	0	0	6	2
9-7	130	1	1	4	3	6	4
9-8	40	0	0	0	0	6	4
8-6	145	1	1	1	1	7	5
7-4	50	1	1	7	5	7	5
6-5	50	1	1	0	0	7	3
6-4	30	6	2	7	3	13	7
5-4	40	1	1	1	1	8	4
7-6	50	6	2	0	0	7	5
2-7	150	0	0	0	0	5	3
1-9	75	0	0	0	0	5	3

The simulation results are given in Tables 5 and 6, from which it is seen that with the calculated loads the probability of information loss is very low.

We consider the dependence of the loss information probability on the load intensity ρ using the example of a 7–4 connection under the remaining conditions. Using the same example, we consider the effect of the number of drive sections N, Table 8. It is clear that with N = 0, the probability of information loss equals 1, since there is simply nowhere to take it. As N increases, q it drops abruptly, turning almost to zero already at N = 10. It is also obvious that the greater is the load intensity ρ, the greater is the probability of information loss q, and the increase is quite fast, requiring an increase in the number of sections of the receiver's drive N.

Table 5 Loads and Probabilities of information loss for separate link

Link	$\rho_{ij}^{н}$	$q_{ij}^{н}$	ρ_{ij}^{a}	q_{ij}^{a}
1-7	0.01593	1.008E-09	0.04065	1.0643E-07
2-9	0.02477	9.099E-09	0.04064	1.0638E-07
10-2	0.00890	5.545E-11	0.00890	5.5455E-11
3-4	0.04583	1.929E-07	0.04580	1.9296E-07
3-5	–	–	0.04583	1.9289E-07
9-7	0.03363	4.154E-08	0.04949	2.8233E-07
9-8	–	–	0,04949	2.8221E-07
8-6	0.00891	5.557E-11	0.05835	6.3671E-07
7-4	0.05834	6.364E-07	0.05834	6.3645E-07
6-5	–	–	0,05468	4.6204E-07
6-4	0.05468	4.619E-07	0.10412	1.0961E-05
5-4	0.00890	5.541E-11	0.06353	9.6904E-07
7-6	–	–	0,05834	6.3644E-07
2-7	–	–	0,04065	1.0649E-07
1-9	–	–	0,04064	1.0638E-07

Table 6 Probabilities of no loss for route information

Route	$Q_{\Sigma M}^{nr}$	Route	$Q_{\Sigma M}^{em}$
1-7-4	6,37E-07	1-9-8-6-4	1,199E-05
2-9-7-4	6,87E-07	2-7-4	7,429E-07
3-4	1,93E-07	3-5-4	1,162E-06
5-4	5,54E-11	5-6-4	1,142E-05
6-4	4,62E-07	6-5-4	1,431E-06
7-4	6,36E-07	7-6-4	1,16E-05
8-6-4	4,62E-07	8-9-7-4	1,201E-06
9-7-4	6,78E-07	9-8-6-4	1,188E-05
10-2-7-4	6,37E-07	–	–

Failure of software is associated with its inconsistency with the tasks. There are many definitions of a software error. The definition [12] seems to be the most acceptable: *Software reliability is probability that the program will run for a certain period without failures, taking into account the degree of their influence on the output results*. The frequency of error occurrence from the statistical data, reduced to 100% errors, is given in Table 8 with the position "Incomplete or erroneous task" disclosed in more detail.

Software is not the subject to wear and tear; its reliability is determined only by development errors. Thus, this indicator should increase over time if the correction of the revealed errors does not introduce new errors.

For critical applications, which should include the WAMS software, the system delivered to the customer may contain from 4 to 15 errors per 100,000 lines of program code [13]. For clarity, we note that the number of lines of WINDOWS XP code is more than 45 million, NASA programs are 40 million, Linux 4.11 kernel is more 18 million. When evaluating the WAMS program with V = 10 million lines of code, the number of errors at the beginning of the program operation $E = (V/100000) \cdot 4 = 400$ errors. Then, using the formula for the mean time between failures of the software, we get

$$\lambda_{soft} = \beta\frac{E}{V} = 0.01\frac{400}{10^7} = 4\cdot 10^{-7}$$

or

$$t_{soft} = \frac{1}{\lambda_{soft}} = \frac{10^7}{4\cdot 8760} \approx 285 \text{ years},$$

where E is the number of errors per program accepted for operation, V is the program volume in lines of code, β is the program complexity coefficient, usually in the range 0.001 ... 0.01, λ_{soft} is the failure rate and t_{soft} is the mean time between failures of the software, 8760 is the number of hours in a year. With a value 1, an error per 1000 lines of code accepted for application software after testing with

Table 7 Influence of load intensity and number of sections on the probability of information loss q and error-free operation p for communication 7-4

#	ρ	N	p	q	#	ρ	N	p	q
1	0.01	0	0	1	5	0.3	7	0.9998469	0.0001531
2		1	0.99009901	0.00990099	6		10	0.999995867	4.13344E-06
3		3	0.99999901	9.9E-07	7		100	1	0
4		5	1	9.9E-11	1	0.5	0	0	1
5		7	1	9.88098E-15	2		1	0.666666667	0.333333333
6		10	1	0	3		3	0.933333333	0.066666667
7		100	1	0	4		5	0.984126984	0.015873016
1	0.05834	0	0	1	5		7	0.996078431	0.003921569
2		1	0.944874979	0.055125021	6		10	0.99951148	0.00048852
3		3	0.999813008	0.000186992	7		100	1	0
4		5	0.999999364	6.36452E-07	1	0.7	0	0	1
5		7	0.999999998	2.16628E-09	2		1	0.588235294	0.411764706
6		10	1	4.30211E-13	3		3	0.864587446	0.135412554
7		100	1	0	4		5	0.942856074	0.057143926
1	0.1	0	0.000000000	1.000000000	5		7	0.973782312	0.026217688
2		1	0.909090909	0.090909090	6		10	0.991354799	0.008645201
3		3	0.999099909	0.000900090	7		100	1	1.11022E-16
4		5	0.999990999	0.000009000	1	0.9999999	0	0	1
5		7	0.999999909	0.000000090	2		1	0.500000025	0.499999975
6		10	0.999999999	9.00007E-11	3		3	0.750000038	0.249999962
7		100	1.000000000	0.000000000	4		5	0.833333375	0.166666625
1	0.3	0	0	1	5		7	0.875000044	0.124999956
2		1	0.769230769	0.230769231	6		10	0.909090955	0.090909045
3		3	0.98094566	0.01905434	7		100	0.990099059	0.009900941
4		5	0.998297759	0.001702241					

Table 8 Frequency occurrence of errors for certain types

Cause of error	Frequency, %
Deviation from the task	12
Neglecting programming rules	10
Incorrect data sampling	10
Erroneous logic or sequence of operations	12
Erroneous arithmetic operations	9
Lack of time to resolve	4
Incorrect interrupt handling	4
Invalid constants or source data	3
Inaccurate recording	8
Incomplete or erroneous task	28

⇓

Errors in numeric values	12
Insufficient accuracy requirements	4
Erroneous characters or signs	2
Registration errors	15
Incorrect hardware description	2
Incomplete or inaccurate development basics	52
Ambiguity of requirements	13

the same amount of code lines E = 10,000 errors

$$\lambda_{soft} = \beta\frac{E}{V} = 0.01\frac{10000}{10^7} = 10^{-5}$$

or

$$t_{soft} = \frac{1}{\lambda_{soft}} = \frac{10^5}{8760} \approx 11.4 \text{ years}$$

or about one failure in 12 years.

Conclusion

The correct functioning of the WAMS local information network is ensured by four components of reliability.

Hardware reliability of the network is largely determined by the reliability of information carriers (optical fiber, radio waves, etc.) and by the devices providing their work - phasors meters, data concentrators. With the right organization of redundancy, the network hardware availability meets the requirements for the reliability of control systems.

Traffic reliability component is determined by the load intensity of each connection and the capabilities of receiving information, determined by the volume of the receiver's drive. The availability of the test network for traffic exceeds three nines after the decimal point.

In terms of software, the influence of code lines on the value of the reliability parameter is considered and its estimate is shown depending on the number of commands. For the example of a 10 million code lines of WAMS program, the mean time between failures should be 285 years.

Many works have been devoted to opposing the external negative impact on the transmitted information, for example, [15, 16], and they are not considered by this paper.

References

1. Phadke A. G. and Thorp J. S. *Synchronized Phasor Measurements and Their Applications*. New York: Springer, 2008, 260 p.
2. Uspensky M.I., Smirnov S.O. The Occurrence Reasons and Countermeasures to Power System Blackouts // Intern. J. of Energy Engineering, 2014, no. 1, pp. 1- 8.
3. Uspensky M.I. Functional reliability assessment of the phasor measurement unit // Relay protection and automation. 2017, no. 3, pp. 39-44. (In Russian).
4. Uspensky M. I. Reliability assessment of the WAMS communication network // Relay Protection and Automation, no. 1, 2019, pp.66-70. (In Russian).
5. Uspensky M.I., Kyzrodev I.V. Combined Method of a Distribution Network Reconfiguration for Power Supply Restoration // Proc. of the IEEE PowerTech, St. Petersburg, Russia, 27-30 June, ref. 33, 2005.
6. Real-Time Application of Synchrophasors for Improving Reliability 10/18/2010. [Electronic resource]. URL: http:// www.naspi.org (application date: 09.12.2019).
7. Tsukanov V.N., Yakovlev M.Ya. *Fiber optic technology. Practical Guide*. M.: Infra-Engineering, 2014, 304 p. (In Russian).
8. Davydov A.E., Smirnov P.I., Paramonov A.I. *Design of telecommunication systems and networks. Calculation of communication network parameters and traffic analysis*. St. Petersburg: University of IT-MO, 2016, 47 p. (In Russian).
9. Asanov M.O., Baransky V.A., Rasin V.V. *Discrete mathematics: graphs, matroids, algorithms*. M. PXD, 2001, 288 p. (In Russian).
10. N.B. Zeliger, O.S. Chugreev, G.G. Yanovsky. *Designing networks and systems for transmitting discrete messages*. M.: Radio and communications, 1984, 177 p. (In Russian).
11. Gordienko V. N. et al. *Optical telecommunication systems*. Textbook for high schools/ V. N. Gordienko, V. V. Krukhmalev, A. D. Mochenov, R. M. Sharafutdinov. M: Hotline – Telecom, 2011, 368 p. (In Russian).
12. Morozov Yu.M. *Reliability of hardware and software systems* / St. Petersburg, 2011, 136 p. (In Russian).
13. Chukanov V.O., Gurov V.V., Prokopyeva E.V. Methods of ensuring software and hardware reliability of computing systems / Presentation of the report at the seminar. - 44 p. (In Russian). [Electronic resource]. URL: http://www.mcst.ru/files/5357ec/dd0cd8/50af39/000000/seminar_metody_obespecheniya_apparatno-programmnoy_nadezhnosti_vy-chislitelnyh_sistem.pdf (application date: 11.02.2020).
14. Shklyar V.N. *Reliability of control systems*. Tomsk: Publishing House of Tomsk Polytechnic University, 2009, 126 p. (In Russian).
15. Zhang Y. etc. Cyber Physical Security Analytics for Transactive Energy Systems / Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn and S. Suresh // IEEE Trans. on Smart Grid, **11**, no. 2, March, 2020, pp. 931-941.
16. Martel E., Kariger R., Graf P.-A. *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards* / Center for Cybersecurity and Electricity Industry Community. January, 2019, 29 p. [Electronic resource]. URL: http://www3.weforum.org. (application date: 03.03.2020).