Resilience Assessment of the State Estimation Software under Cyber Attacks

*Nikolai*Voropai[1], *Irina*Kolosok[1],and *Elena*Korkina[1]*

[1]MelentievEnergy Systems Institute, Irkutsk, Russia

Abstract. Taking into account Smart Grid creation, cyber security appears as critical problem. In spite of wide set of technical tools and organisational decisions, which use for protection of electrical objects against cyber attacks, it is impossible to prevent them completely. Therefore, the ability of Smart Grid to resist cyber attacks is important and necessary property. Thus, the cyber resilience is ability of complicate technical-information system to keep operable state under contingencies including cyber attacks. This paper deals with general problem of electric power system resilience and its cyber resilience, determination methods to calculate quantitative measure of Smart Grid resilience. The state estimation software resilience under cyber attacks is discussed.

1 Some terminology considerations

Present-day electric power systems (EPSs) are most complicated technical man-made objects, when using innovative technologies to generate, transmit, deliver and store electric power. They permanently develop affected by many objective factors. During EPS development, their properties vary, there is a necessity to study new properties of transforming EPSs and new problems in operation of these systems, and, accordingly, a necessity to use new tools to maintain EPS normal operation.

Recently, in English publications, a new term, resilience, reflecting EPS property transformation has been actively discussed [1-6 etc.]. The most comprehensive definition of the term "resilience" is given in [2], where it is defined as "as the ability of the system or systems-of-systems (SoS) to withstand a change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability)." It is important to note that this definition refers to any systems irrespective of their nature. In [4], the discussed property is also represented for systems of any nature, and it is addressed as complex, including ecological, organizational, and system components. Herewith, the latter features as an ability to minimize the value and duration of deviations from target metrics of a system.

Studies [1, 3, 5, 6] address this property with reference to EPSs, and in [3, 5], the focus is on external extreme perturbations (for example, hurricanes, etc.). Over the recent years, researchers actively investigate the problem of cyber attacks as potential external disturbances affecting the information-communication subsystem of present-day cyber-physical EPSs [7-9, etc.]. At the same time, in the review [3] - besides external extreme disturbances, and in [1, 6] – exclusively, it is a problem of resilience in relation to the cascade system collapses. Herewith, in [1], to corroborate the trend of growing importance of the addressed property, there is information on the increase in scales of after effects of the cascade system failures for users in time based on the statistics about the USA EPS over 1991-2005 This legitimacy of growth of scales of after effects of system collapses features any developing EPS.

The Russian term corresponding to the notion resilience is survivability. Applicable to EPS, survivability is a property of a system to withstand disturbances without allowing their cascade development with a mass interruption of supply to users, and to recover the system initial state, or the one close to it [10]. From this definition, one can see that, in the survivability property, shown are the absorptive and adaptive abilities of a system noted in [2], as well as its ability to recover.

In the English literature [e.g., 11] the term vulnerability is used instead of survivability. At that, vulnerability is related to dynamic mode of reliability, to dynamic security. The differences between the terms survivability and vulnerability are obvious: survivability assumes a certain "activity" of a system when resisting perturbations due to a rationally organized structure, expedient operation modes, and efficient control. Vulnerability reflects as if a "passive" response of a system to perturbations. Taking this into account, vulnerability is a complementary (opposite) property of a system as compared with survivability [10, 12].

It is expedient to note some nuances related to the PES survivability concept. Those nuances are reflected in Figure 1, where 1 is the system operational capacity normal level φ, 2 is the limiting state (for details, see

[*] Corresponding author: korkina@isem.irk.ru

[10, 12, 13]), 7 is the restoration stage. According to the figure, there are two cases possible. In the first case, an emergency process starts with an ordinary perturbation, and then, due to failures of control units and staff mistakes, there occurs a cascade development of emergency 3. At each stage of such a development, the emergency control system attempts to interrupt the emergency cascade development 6. Upon reaching the limiting state 2, the emergency cascade development becomes non-reversible 4, an avalanche process develops rapidly, the emergency control schemes either have no time to response, or have already exhausted their possibilities by this stage. It is this case that the resilience property is addressed in [1, 6]

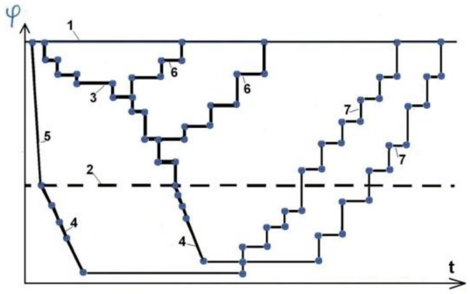


Fig. 1. Illustration for a EPS behavior in terms of survivability.

The other case applicable to the survivability property is related to an extreme non-ordinary initial disturbance 5 (hurricanes, tornadoes, etc. refer to such disturbances [3, 5], as well as cyber attacks (CAs) [7-9]), after which the system appears below the limiting state, and there occurs an avalanche uncontrollable development of an emergency process 4.

2 Smart Grid cyber resilience

Creating Smart Grids (SG) provides:

- using new technologies widely and gages to measure mode parameters (digital measuring transformers and converters, devices to measure vector values -phasor measurement units (PMU), and so forth),
- creating wide area measurement systems (WAMS), protection systems (WAPS), and control systems (WACS) based on the high-precision synchronized phasor measurements.
- present-day means of communication that principally change the processes of data acquiring, processing, and transmitting,
- substation digitization and automation,
- changing properties of the observational object (power system) due to a grid saturation with active elements (FACTS, HVDC),
- using technologies of a distributed computing,
- high-performance hardware.

Introducing obvious advantages of using such technologies and hardware, a Smart Grid also has its defects: higher vulnerability of the entire Smart Grid and its local infrastructures to cyber attacks, due to which introducing new technologies should be accompanied by allowance for requests of the Smart Grid information protection from adverse external effects. Therefore, there emerge problems of providing Smart Grid cyber security, along with traditional problems of raising the efficiency of production, transformation, transmission, and power distribution, Smart Grid reliability, security, and survivability. Solving the Smart Grid cyber security problems requires supplementing and expanding the "reliability" property with new concepts, such as "vulnerability," "survivability," "cyber resilience," etc., which is necessary for revealing and assessing mechanisms for cyber attack effect on electric power industry objects.

In the Russian sources [9, 14], the term durability is used and its interpretation is provided: 1) ability of Smart Grid and its elements to withstand external effects and to operate in the normal mode under cyber attacks; 2) ability to maintain normal operation (in standard modes or those close to the latter) during and after disruptive events (DEs), including cyber attacks.

In [15], the author, based on the analysis of situation in cyber security over the last 2-3 years, notes that cyber resilience is the property of an information system enabling it to exist under continuous or constant attacks. The term survivability prompts us that, to solve the problems set before the system, it is not necessary to attempt to protect everything. It is sufficient to focus on the critical components, providing their redundancy, duplication, staff qualification, and other problems that, applicable to information systems, may be taken from the reliability theory.

Apparently, the Smart Grid survivability principles may and should be used when studying the Smart Grid cyber resilience problem. On the other hand, it is obvious that providing cyber resilience entirely and immediately is difficult; therefore, it is necessary to solve this problem systemically, starting the phase of developing preventive measures and ending with the restoration phase after a cyber attack.

3 Main regularities of stable behaviour of the system

The concept of resilience has been developed and investigated in various fields, but there has been no uniform standard definition so far. Like shown in Section 1, under the effect of external disturbances, a system should have abilities to absorb effects, adapt to the latter, and restore. These abilities may be regarded as three essential properties of a system resilience: enhancing any of them will enhance the system resilience.

Figure 2 borrowed from [16] shows the main regularities of the system steady and unstable behaviour under effects of damage factors. Apparently, the system behaviour character shown on Figure 2 is similar, in many respects, to the EPS behaviour illustrating the survivability property (Figure 1).

Depending on the EPS ability to adapt, self-organize, and restore, possible are different versions of final restoration:1) by the mode not different from pre-emergency state (robust behaviour), 2) incomplete recovery with the mode relaxed parameters (flexible behaviour), 3) transition to the non-operable state (destructive behaviour), 4) with the mode parameters surpassing those of the pre-emergency mode (recovery with adaptation).

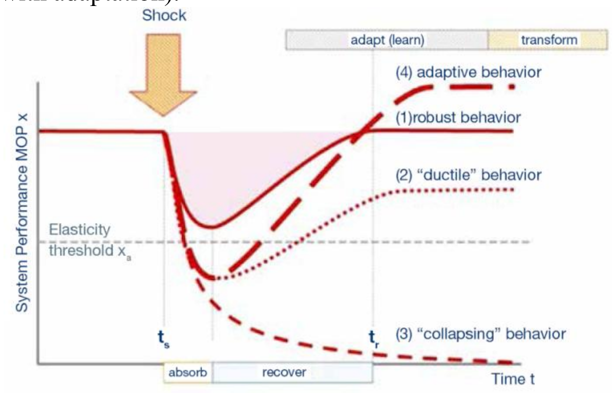


Fig. 2. Main regularities of the system stable and unstable behaviours.

4 Quantitative measure of resilience

Assessing the EPS resilience helps find the best strategy to restore the system operation and minimize originating losses. Over the last decade, various methods to quantify the assessment of resilience to external disturbances have been offered.

In the reliability theory, developed were some approaches to assess the reliability quantity indicators. The main of the latter is – failure-free operation - is the property of an object to keep operable state for a certain time.

To assess reliability, important is the duration under operational loads, i.e., the time factor. To assess the resilience to external disturbances, important is the effect level, at which there can occur a failure, i.e. the kind of disturbance and its intensity.

Resilience to external disturbances has a non-linear nature of a threshold kind: the action of the disruptive mechanism manifests itself only after the disturbance level exceeds a threshold value, the limiting condition of the system shown in Figures 1 by line 2 or the elasticity threshold Xs in Figure 2. An increase in the main characteristic of the system resilience - the time to reach the limiting condition - enables to decrease the risk of developing critical (emergent) situation and to provide security.

In foreign studies, proposed was the General resilience metric (GR) to determine quantity resilience indicator with a possibility to take into account the criteria of individual properties.

To illustrate this parameter, we use Figure 3 from [2] that shows the main phases and transitions when analysing the system resilience to external disturbances.
The Y-axis represents the measure of performance (MOP).

The first phase is the initial steady phase (t<td), at which the system performance assumes its target value.

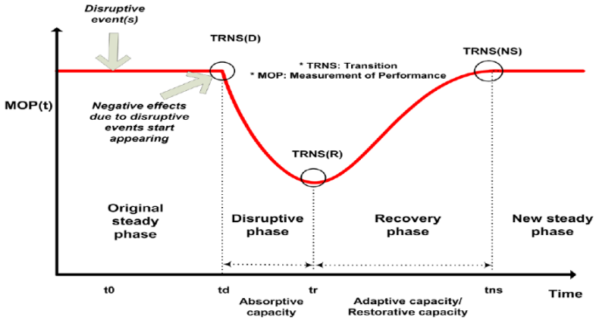


Fig. 3. System phases and transitions at a DE effect [2].

The second phase is the destructive (disruptive) phase ($t_d \leq t < t_r$), at which the system performance starts dropping, until it reaches the lowest level at time tr. During this phase, one can assess the system absorptive capability. Robustness (R) is the measure that enables to assess this ability being the MOP minimal value.

The third phase is the restoration phase ($t_r \leq t < t_{ns}$), at which the system performance starts to increase to a new steady level. During this phase, one can assess the system adaptive and restorative capabilities by introducing the corresponding measures: $RAPI_{DP}$ (rapidity) and TAPL (time averaged performance loss). The reached new steady level may be equal to the previous one, but it can be lower or higher than that level. To take this into account, developed was a quantitative measure - Recovery Ability (RA).

Considering these measures, a formula was obtained to calculate the integrated metric for the system resilience to external disturbances (GR):

$$GR = f\,(R, RAPI_{DP}, RAPI_{RP}, TAPL, RA) =$$

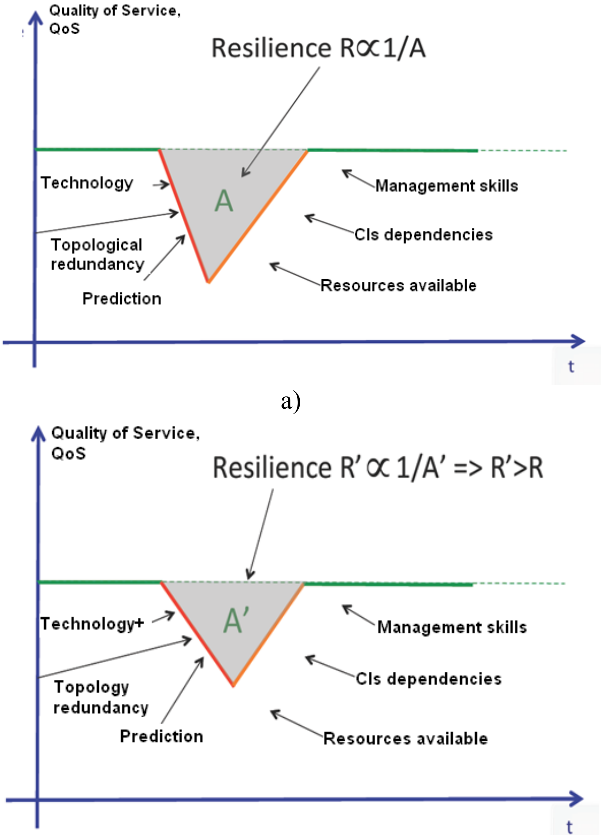
$$= R\left(\frac{RAPI_{DP}}{RAPI_{RP}}\right)(TAPL)^{-1}\ RA$$

where: R is the robustness (MOP minimal value of),
$RAPI_{DP}$ is the disruptive phase rapidity,
$RAPI_{RP}$ is the restoration phase rapidity,
TAPL is the time averaged performance loss,
RA is the recovery ability.

The GR metric is dimensionless and is an extremely useful measure to compare resilience of engineering systems. For example, it may be used to compare the resilience of different systems to the same DE. For more resilient system, a value of this metric will be higher. This metric may be also used to compare the resilience of the same system to different DEs. A higher GR indicates that the system is more resilient to certain DEs. Besides, the GR metric may be used to compare various versions and develop more resilient system to a certain DE as per various mitigation and protection strategies.

Yet, to calculate this metric, one should have statistics on the number of CAs over a certain time interval, and on the duration of individual phases of effect and restoration. Therefore, in a number of studies, for example, in [17], proposed were some simplified versions to measure a similar metric. We term it the cyber resilience index (CRI). Figure 4 shows two versions of the figure from [17], similar to Figure 2, but in a simpler view.

From this figure, one can see that the CRI value (R in the figure) is inversely proportional to the A triangle area restricted by the system normal performance line, by the line of the performance drop at the destructive phase, and by the line of the performance growth at the restoration phase. Also, from the figure, one can see that, in the b-case, the system CRI is higher, than that in the a-case.



a)

b)

Fig. 4. Illustration for the cyber resilience index (CRI).

5 Case study

As a case study, we assessed the cyber resilience for the OTSENKA (State Estimation) software developed at the Melentiev Energy Systems Institute of the Siberian Branch of the Russian Academy of Sciences [18].
The primary problems solved at the EPS state estimation:

- forming the current scheme from the SCADA;
- checking the observability;
- bad data detection (BDD) in SCADA-measurements;
- filtering random SCADA errors (obtaining SCADA estimates and calculating non-measured parameters).

In a reliable state estimation software, all these functions should be doubled. Thus, in the OTSENKA software, checking the observability of the scheme is executed twice: based on the topological method until solving the state estimation problem (estimation calculation) and during the estimation calculation at the Jacobian matrix triangular resolution. BDD is done a priori, i.e. prior to solving the state estimation problem through the Test Equation method [18], or during calculating the estimates by non-quadric (robust) criteria, or after the state estimation by estimate residuals. Estimating may be performed through state estimation linear algorithms, if the scheme is observable through PMU-measurement, non-linear algorithms through the weighed least square method from the SCADA and PMU data, or by using robust criteria to suppress erroneous measurements.

Figure 5 illustrates the state estimation software resilience under cyber attacks.

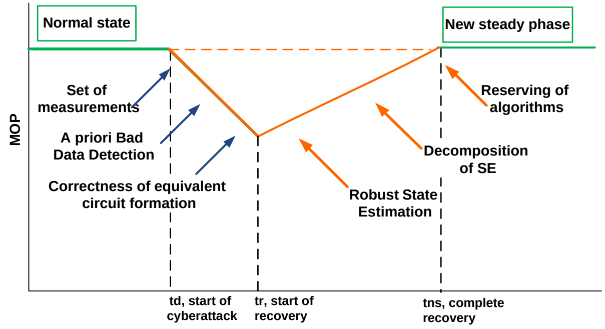


Fig. 5. EPS state estimation software cyber resilience.

The curve length and inclination within the [t_d; t_r] interval depend on the composition of the processed measurements, on the aprioristic BDD efficiency, on the Jacobian matrix conditionality, and on other factors. The curve length and inclination within the interval [t_r; t_{ns}] interval (restoration phase) depend on the possibility to duplicate the applied algorithms.

Figures 6-8 show the analyses of probable state estimation software attacks.

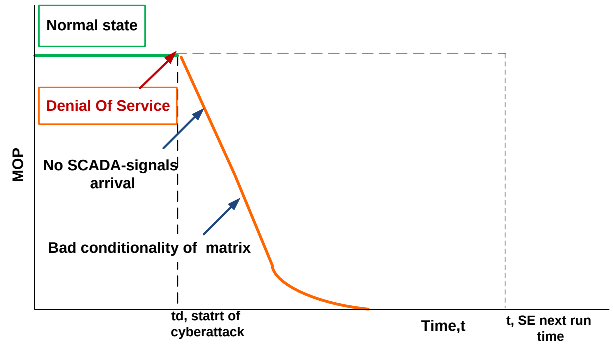


Fig. 6. Impossibility to recover SE software due to a denial of service (DoS) attack.

With no SCADA signals due to a DoS attack, the scheme is impossible to correctly design (Figure 6). The generated matrix thereof has a bad conditionality, the iterative process diverges. There emerges an issue to develop special alarms for such cases.

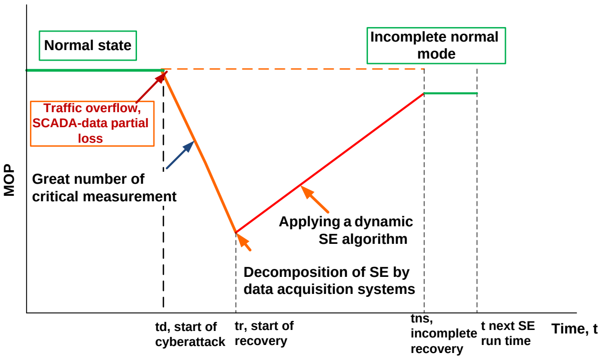

Normal state
Incomplete normal mode
Traffic overflow, SCADA-data partial loss
MOP
Great number of critical measurement
Applying a dynamic SE algorithm
Decomposition of SE by data acquisition systems
td, start of cyberattack
tr, start of recovery
tns, incomplete recovery
t next SE run time
Time, t

Fig. 7. State estimation software restoration under a man-in-the-middle (MITM) attack.

Figure 7 shows the consequences of a MITM attack: the attacker is inside the network and by repeated sending of the same packages overwhelms the traffic. Therefore, the transmission of other necessary packages is blocked. A scheme part becomes unobservable. The state estimation software performance persists due to the decomposition algorithm from SCADA and WAMS measurements [19] and due to using the estimations of the unobservable scheme part the previous cycle.

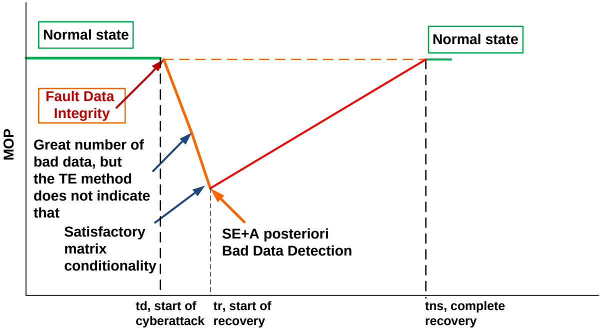

Normal state
Normal state
Fault Data Integrity
MOP
Great number of bad data, but the TE method does not indicate that
Satisfactory matrix conditionality
SE+A posteriori Bad Data Detection
td, start of cyberattack
tr, start of recovery
tns, complete recovery

Fig. 8. State estimation software recovery under a fault data integrity (FDI) attack.

Figure 8 shows the consequences of an FDI attack: the attacker injects false data that cannot be detected through the Test Equation method. The state estimation software performance resilience persists due to a posteriori BDD.

6 Conclusions

Resilience is the ability of a system to withstand the effect of disruptive events (cyber attacks), to reduce initial negative effects, to adapt to the latter, and to restore after them.

This concept supplements and expands such EPS (Smart Grid) properties, as "reliability," "security," "flexibility," "vulnerability," etc.

Resilience has a non-linear nature of a threshold kind. To assess a degree of a PES resilience, one should develop quantitative metrics.

Proposed was a general resilience metric (GR) to quantify resilience. The GR takes into account the absorptive, adaptive, and restoration capabilities of a system.

It is important to study the Smart Grid resilience problems systemically, i.e., by considering all its capabilities and possible cyber attacks, in order to solve the problem completely and not to admit negative effects of cyber attacks on the Smart Grid vulnerability.

This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (№ AAAA-A17-117030310438-1).

References

1. Massoud A. Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid // IEEE PES General Meeting, Pittsburg, USA, July 20-24, 2008, 5 p.
2. Cen Nan, Sansavini G., Kroeger W. Building an integrated metric for quantifying the resilience of interdependent infrastructure systems // 9th Intern. Conf. on Critical Information Infrastructure Security, Limassol, Cyprus, October 13-15, 2014, 12 p.
3. Yezhou Wang, Chen Chen, Jianhui Wang, Baldick R. Research on resilience of power systems under natural disasters - A review // IEEE Trans. Power Syst., 2016, Vol. 31, No. 2, pp. 1604-1612.
4. Zhonglin Wang, Nistor M.S., Pickl S.W. Analysis of the definitions of resilience // 20th IFAC World Congress, Toulouse, France, July 9-14, 2017, pp. 11136-11144.
5. Panteli M., Mancarella P., Trakas D.N., Kyriakides E., Hadziargiriou N.D. Metrics and quantification of operational and infrastructure resilience in power systems // IEEE Trans. Power Syst., 2017, Vol. 32, No. 6, pp. 4732-4741.
6. Kezunovic M., Overbye T.J. Off the beaten path: Resiliency and associated risk // IEEE Power and Energy Magazine, 2018, Vol. 16, No. 2, pp. 26-35.
7. Mehrdad S., Mousavian S., Madraki G., Dvorkin Yu. Cyber-physical resilience of electrical power systems against malicious attacks: A review // Current Sustainable / Renewable Energy Reports, <https://doi.org/10.1007/s40518-018-0094-8>
8. Kolosok I.N., KorkinaE.S., and GurinaL.A. Analyzing security of state estimation results from PMU under WAMS cyberattacks // Methodical issues of studying reliability of the bulk energy systems. Issue 66. Minsk: BNTU, 2015, P. 66 - 75, in Russian.
9. Papkov B.V., Kulikov A.L., and OsokinV.L. Cyber threats and cyber attacks in electric power industry.Nizhnii Novgorod: NRU RAE&PS, 2017, P. 80, in Russian.
10. Reliability of energy systems (Collection of recommended terms). Moscow: Energiya (Energy) Publ., 2007, P. 152, in Russian.
11. Fouad A.A., Zhou Qin, Vittal V. System vulnerability as a concept to access power system dynamic security // IEEE Trans. on PS, Vol. 9, No. 2, pp.1009 - 1015.
12. Voropai N.I. EPS Survivability: methodical bases and methods of research // Izvestiya (Bulletin) of the

USSR AS. Energetics and Transport, 1991, No. 6, Pp. 52 - 59, in Russian.

13. Antonov G. N, Cherkesov G.N., Krivorutskiy L.D., et al. Methods and models for studying survivability of energy systems. Novosibirsk: Nauka (Science) Publishers, 1990, P. 285, in Russian.

14. Bakulin V.M, MalkovS.Yu., Goncharov V.V., and Kovalyov V.I. Managing the provision of complex engineering system durability. Moscow: FIZMATLIT (Physical-Mathematical Literature) Publishers, 2006, P. 304, in Russian.

15. Lukatskiy A. Cyber resilience, cyber survivability, cyber reliability, cyber continuum. https://www.securitylab.ru/blog/personal/Business_without_danger/342751.php, in Russian.

16. Heinimann H.R. Future resilient systems. Singapore-Zurich: ETH Risk Center, 2014, 600 p.

17. Tofani A., Alessandroni S., D'Agostino G., Di Pietro A., Onori G., Pollino M. and Rosato V. Operational Resilience Metrics for a Complex Electrical Networks // Intern. Conf. on Critical Information Infrastructure Security CRITIS 2017, Lucca – Italy.

18. Gamm A.Z., and Kolosok I.N. Detecting bad data of SCADA-measurements in power systems. Novosibirsk: Nauka (Science) Publishers, 2000, P. 152, in Russian.

19. Kolosok I.N., Korkina E.S. Decomposition of power system state estimation problem as a method to tackle cyberattacks // The1st IEEE Intern. Conf. ICPS-2018, Saint-Petersburg, 15-18 May 2018, SF-004928