# METROLOGY, QUALITY, STANDARDIZATION AND CERTIFICATION

## GENERALIZED RISK ASSESSMENT PROCEDURE FOR SOFTWARE TESTING OF LEGALLY REGULATED MEASURING INSTRUMENTS

***Valentyn Gaman, Serhii Kursin, PhD, Oleh Velychko, Dr. Sc., Prof.,***
*SE “Ukrmetrteststandard”, Ukraine;*
*e-mail: vgaman@ukrcsm.kiev.ua*

**Abstract.** The legal metrology covers measuring instruments (MI), the measurement results of which are used in calculations for consumed energy resources, in the fields of information protection, security, environmental protection, etc. Most modern MIs use microcontrollers or are controlled by computers. The software (SW) of such MIs provides an opportunity not only to automate the processes of measurement and calculation of results but also to ensure long-term storage and data transfer. The manufacturer is responsible for investigating and assessing all possible risks related to the MI SW. The task of the conformity assessment body is to assess the conformity of MIs adequately in general and software, in particular, to the established requirements based on the analysis of risk classes. Standards for information security risk management, information technology security assessment, and information technology security assessment criteria consider only general issues of software security and risk assessment without taking into account the scope of its application. The existing regulatory documents on software risk management were considered. Modern methods of assessing the risks of the MI SW were studied. To assess the risks of software of legally regulated MIs, a general classification of threats and vulnerabilities of MI SW was made. For choosing threats that affect functionality, only those that affect metrological characteristics during measurement are taken into account. Possible manifestations of the impact of threats on stored data can be their distortion or destruction, and transmissions of data can be data distortion during transmission or data loss due to a break in the telecommunications connection. A proposed simplified risk assessment methodology for assessing the compliance of MI SW without statistical data on the probabilities of threats and the amount of harm from the implementation of threats is presented. Risk is defined as the probability of harm due to a certain vulnerability, taking into account the conditional amount of harm.

**Key words:** Software, measuring instruments, risk assessment, assessing compliance

### 1. Introduction

Legal metrology includes measuring instruments, which measurement results are used in the calculations for consumed energy resources, information security, environmental protection, etc. Most modern MIs use microcontrollers or are controlled by computers. Software (SW) of such MIs provides an opportunity not only to automate the processes of measurement and calculation of results but also to ensure long-term storage and data transmission, including through public networks, to ensure automatic download of updates, etc. All this significantly increases the risks of economic losses due to distortion of measurement results, risks to life and health safety, and risks of disclosure of personal information due to intentional interference. The examination levels of both the MI itself and SW are selected following the identified risks.

The Technical Regulation on MIs [1] and the Technical Regulation on legally regulated MIs [2] require that the technical documentation submitted to conformity assessment bodies, in particular for assessment modules A, A2, B, D1, E1, F1, G, H, H1, when testing MIs contained information on adequate analysis and assessment of possible risks of using such MIs. It is the responsibility of the manufacturer to investigate and assess all possible risks. The task of the conformity assessment body is to assess the conformity of MIs adequately in general and software, in particular, to the established requirements based on the analysis of risk classes. The WELMEC Guide 7.2 [3] assigns software risk classes for MI groups covered by the MID Directive (2014/32/EU) [4], to which the MI Technical Regulation [1] corresponds. For other groups of legally regulated MIs [2], software risk classes are not established, and it requires a personal approach to each MI to establish the required examination levels. Therefore, there is a need to define risk classes for all groups of legally regulated MIs with SW.

### 2. Disadvantages

Standards for information security risk management [5], security assessment in the field of information technologies [6], and assessment criteria of information technology security [7] consider general issues of software security and risk assessment without taking into account the scope of its application. In addition, [5] provides the basic principles of risk assessment, which are reduced to 3 procedures. Risk identification is the procedure of determining undesirable events, or so-called threats. Risk analysis is a procedure of giving threats quantitative or qualitative assessments as a whole. Risk evaluation is a procedure for calculating risks for a specific software application.

Special methods have been developed to assess risks related to MI SW. In [8], an algorithmic approach to risk assessment of MI SW is proposed, a specific set of functional capabilities and related security properties for measuring devices is defined, and a list of threats is proposed. However, this work considers only some types of MIs.

There are methods of risk assessment using the attack probability tree, specially adapted for risk assessment procedures of MI SW in legal metrology. An example of an algorithm for such an analysis for taximeters is given in [9]. It is shown that it is impossible to assess risks based only on technical data without taking into account the motivation of the thief. Also, there are risk assessment methods using a protection probability tree, which involve the construction of protection algorithms based on attack probability trees. In [10], a practical example shows such a procedure for the threat of reading memory cores by an unprivileged software user. A simplified method of risk assessment (both by manufacturers and assessment bodies) of only some threats of an idealized MI is proposed [11]. In [12], a generalized methodology is provided for risk assessment of non-automatic weighing devices and FTAs, to which the recommendations [3] are applied.

In [13–15], a comparative analysis of the general requirements in the documents and guidelines of the international and regional organizations of legislative metrology OIML and WELMEC regarding software testing for MI was carried out. An analysis of the regulatory framework for testing software for MIs at the national level was carried out to establish its suitability for compliance assessment. The main indicators for software of MI with built-in and universal computer, which have the greatest impact on the results of conformity assessment, are determined. At the same time, in these works, the assessment of the risks of software application in various categories of MIs is paid attention only in a general way.

From the conducted analysis, it can be concluded that there are significant developments in the field of risk assessment methodology and its active implementation in the procedures for assessing compliance for MIs. However, the determination (identification) of possible vulnerabilities, corresponding threats, and risks for legally regulated MIs, which are not covered by the WELMEC Guide 7.2, is an actual task.

## 3. Goal

The purpose of the study is to develop a classification of software security vulnerabilities, considering the areas of application of legally regulated metrological instruments and to develop the methodology for assessing the risks of their application.

## 4. Peculiarities of the legally regulated metrology spheres

Under the current legislation on metrology and metrological activities, the sphere of legally regulated metrology includes activities where the inadequate quality of MIs and the consequences of their incorrect use can be critical. In addition to payments for goods consumed, these types of activities can include:

- ensuring the protection of the life and health of citizens;
- quality and safety control of food products and medicines;
- control of the state of the natural environment;
- safety control of working conditions;
- control of road safety and technical condition of vehicles;
- work on ensuring technical protection of information following legislation.

The list of categories of legally regulated measuring equipment subject to periodic verification [16] contains groups of MIs that can be used in the above types of activities. We will list some of them:

1. *To ensure the protection of life and health of citizens* (this group also may include quality and safety control of food products and medicines, control of the state of the environment, control of the safety of working conditions): analyzers of indicators of agricultural and food products (milk, grains, sugar beets, oil crops and their processing products); ionizing radiation detection units; measuring antennas and receivers; measuring channels of radiation control systems; meters of electromagnetic field parameters; gas analyzers (including exhaust gas analyzers), gas detectors; alpha, beta, gamma radiation spectrometers.

2. *To control road safety and the technical condition of vehicles:* remote speed meters of vehicles; remote meters of space-time parameters of the location of vehicles; alcohol content meters in blood and exhaled air.

3. *For technical protection of information*: spectrum and characteristics of communication systems analyzers; power and radio interference meters; selective voltmeters; measuring antennas and receivers.

Manufacturers should analyze and assess the risks associated with the use of submitted for conformity assessment MI. However, not all threats related to the operation of the MI concern its SW. The adequacy of the scope of tests in assessing the conformity of measuring equipment depends on the correct assessment of the SW risk class.

## 5. Risk assessment during software testing of legally regulated measuring equipment

The classification of software threats proposed in [5] can be divided into two main groups: purposely (P) and accidental (A). At the same time, threats related to the human factor can be both intentional and accidental, while environmental threats are only accidental.

From the proposed types of threats, we will select those that relate directly to the MI SW and such legally regulated functions as operation, storage, and data transfer (Table 1). When choosing threats that affect functioning, only those that affect metrological characteristics during measurement (distortion of the measurement result) are taken into account. Possible manifestations of the impact of threats on stored data can be their distortion or destruction. Possible manifestations of the impact of threats during data transmission may be data distortion during transmission or data loss due to a break in the telecommunications connection.

**Table 1.** Threats to the software of legally regulated MIs and their manifestation

| Type of harm | Sources of threat | Threat group | A possible manifestation * |
|---|---|---|---|
| Physical damage | Fire | P, A | LD, DC |
| | Destruction of equipment or media | P, A | LD, DC |
| Natural events | Climatic phenomena | A | LD, DC |
| Loss of necessary services | Loss of power supply | P, A | LD, DC |
| | Failure of telecommunications equipment | P, A | DC |
| Malfunctions due to radiation | Electromagnetic radiation | P, A | LD, DC |
| | Electromagnetic pulse | P, A | LD, DC |
| Information compromising | Intercepting and sending a compromised signal | P | DT |
| | Theft of data carriers | P | LD |
| | Theft of equipment | P | DC |
| | Hardware tampering | P | DD, DT, DC |
| | Tampering with software | P | DM |
| Technical failures | Equipment failure | A | LD, DC |
| | Equipment halting | A | LD, DC |
| | Software crash | A | DM, LD, DC |
| Unauthorized actions | Data distortion | P | DD, DT |
| Compromising of functions | Error in use | F | LD, DC |
| | Abuse of rights | P, A | LD, DC |
| | Falsification of rights | P | DD, LD, DT |
| | Denial of action | P | LD, DC |

* Note: LD is data loss; DC is disconnection of the communication line; DT is distortion during data transmission; DD is data distortion; DM is distortion of measurement results.

It is recommended to pay special attention to the sources of threats related to the human factor since the motivation can be: rebellion, ego, status, money, blackmail, and revenge. As part of software testing, it is advisable to take into account the vulnerabilities associated with obtaining unreliable (distorted) measurement results, in contrast to the risk assessment of vulnerabilities of the type of failure, failure, etc. Distorted results of MIs measurement used in critical areas can lead to catastrophic consequences. Thus, based on the given examples of vulnerabilities [5], it is possible to create the following classification of vulnerabilities concerning the distortion of the results of MIs with SW, presented in Fig. 1.

The maximum number of vulnerabilities should be taken into account by the manufacturer of MI to ensure adequate protection of the device, measurement results, and data from possible threats. Each unaccounted vulnerability or insufficiently assessed vulnerability increases the risk of exposure to this or that threat.

Risk is defined as the probability of harm due to certain vulnerabilities, taking into account the conditional amount of harm. Numerically, the risk of a separate vulnerability is determined by the expression:

$$R(x) = P(x)\cdot A(x), \tag{1}$$

where P(x) is the probability of a threat occurring due to a certain vulnerability x; A(x) is the expected amount of damage (loss harm) that the realized threat can cause.

Since probability is a dimensionless quantity, risk must be measured in units of damage (loss) caused by the hazard. The amount of damage is determined by the financial losses of the supplier of the good or the consumer for measuring devices used to calculate consumer goods. For other devices the quantitative expression of damage can be: the number of dead, the number of wounded, or sick, the area of the affected territory, the value of damaged vehicles, etc. Therefore, determining the amount of damage for such MIs is a difficult task. For the development of a general method of risk assessment concerning MI SW, it is possible to use conditional units (points), which will generally characterize the extent of possible damage due to certain threats.

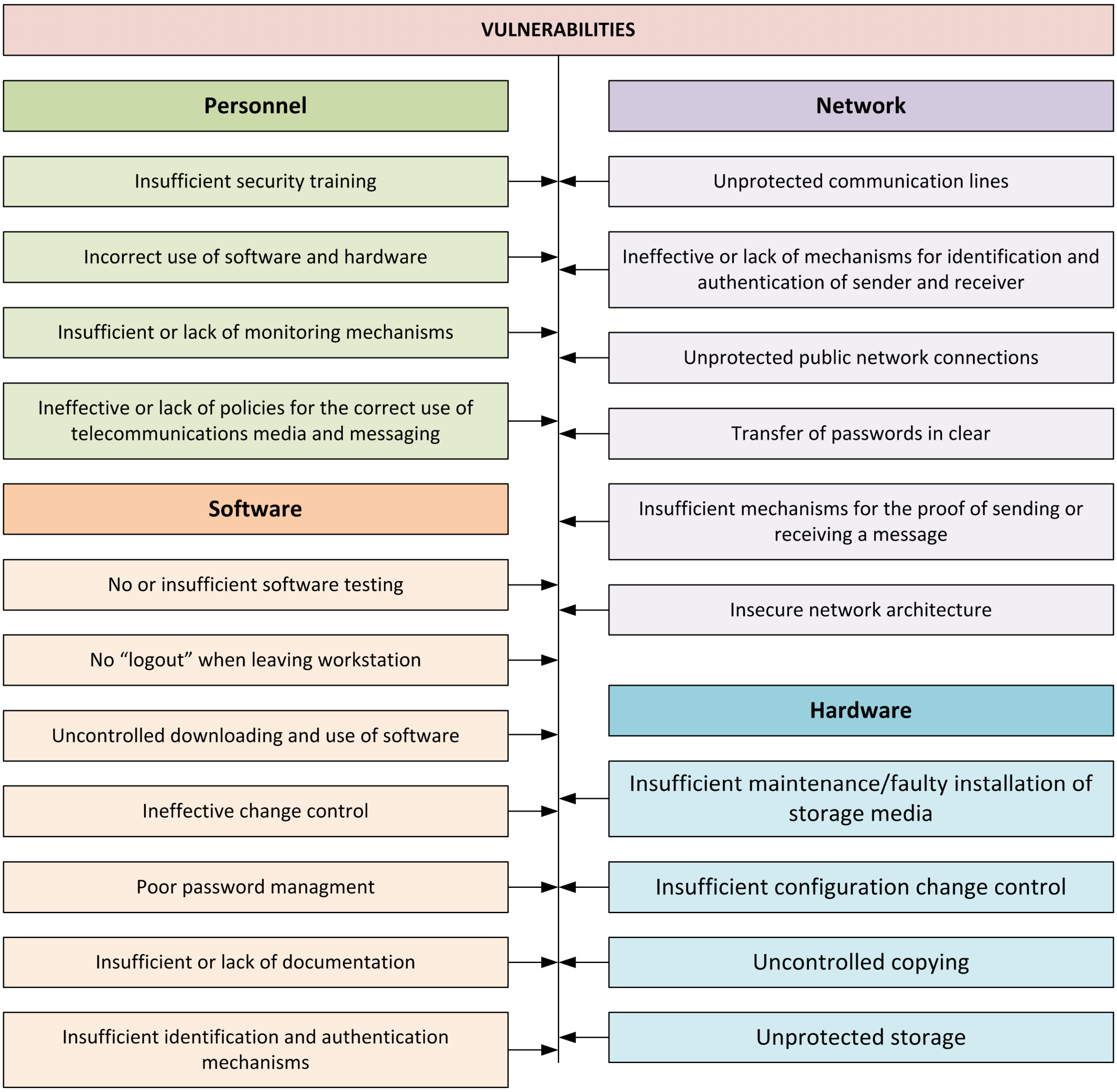
VULNERABILITIES
Personnel
Insufficient security training
Incorrect use of software and hardware
Insufficient or lack of monitoring mechanisms
Ineffective or lack of policies for the correct use of telecommunications media and messaging
Software
No or insufficient software testing
No “logout” when leaving workstation
Uncontrolled downloading and use of software
Ineffective change control
Poor password managment
Insufficient or lack of documentation
Insufficient identification and authentication mechanisms
Network
Unprotected communication lines
Ineffective or lack of mechanisms for identification and authentication of sender and receiver
Unprotected public network connections
Transfer of passwords in clear
Insufficient mechanisms for the proof of sending or receiving a message
Insecure network architecture
Hardware
Insufficient maintenance/faulty installation of storage media
Insufficient configuration change control
Uncontrolled copying
Unprotected storage

*Fig. 1 Classification of software vulnerabilities of MI*

The value of the probability can be estimated taking into account statistical data on the occurrence and implementation of certain threats for specific types of MIs or their classes. If there is no such data, it is possible, using subjective assessments, regarding the probability of occurrence of the threat of accidental events, the presence of malicious intent for purposely events, to divide the probability of threats into three groups: low (L); medium (M); high (H). Similarly, it is possible to distribute the amount of damage.

Since there can be several software vulnerabilities, the total risk consists of the sum of the risks of each vulnerability:

$$R_{\Sigma} = \sum_{x=1}^{N} R(x) = \sum_{x=1}^{N} \left[ P(x) \cdot A(x) \right] \qquad (2)$$

To assess the general risk class of MI SW, it is necessary to determine conditional points for probabilities and values of possible damage. For example, for probability groups: P1 – low, P2 – medium, P3 – high; for the amount of damage – A1, A2, A3, respectively.

For a finite number of threats N, it is possible to determine the limits of the interval of risk classes. Thus, the lower bound of *RL* will have the expression:

$$RL = N \cdot \left( P_1 \cdot A_1 \right) \quad (3)$$

The upper limit of *RH* will have the expression:

$$RH = N \cdot \left( P_3 \cdot A_3 \right) \quad (4)$$

Dividing the obtained range into three parts, we will get the corresponding ranges for the conditional risk levels:

$$R_{lvl} \equiv \begin{cases} Low\ Risk & , \quad if\ RL \le R < \frac{1}{3}RH \\ Middle\ Risk & , \quad if\ \frac{1}{3}RH \le R \le \frac{2}{3}RH \\ High\ Risk & , \quad if\ \frac{2}{3}RH < R \le RH \end{cases} \quad (5)$$

A visual example of the risk calculation and assessment procedure is presented in Fig. 2.

In Fig. 2 in the first column, a dotted line shows the maximum possible value of risks Risk 1 – Risk 14, which is a rectangle with sides that are equal to the maximum values of probability (P3) and possible damage (A3). The areas of the shaded rectangles correspond to the calculated risk values. The second column is formed from rectangles, the area of which corresponds to the calculated value of the corresponding risks at a fixed width corresponding to the maximum value of the damage size (A3). The third column is the result of adding all the resulting rectangles. The height of the third column is used to determine the risk class.

The obtained risk levels can be correlated with risk classes B, C, and D according to WELMEC 7.2 [3], which are listed in the Table. 2.

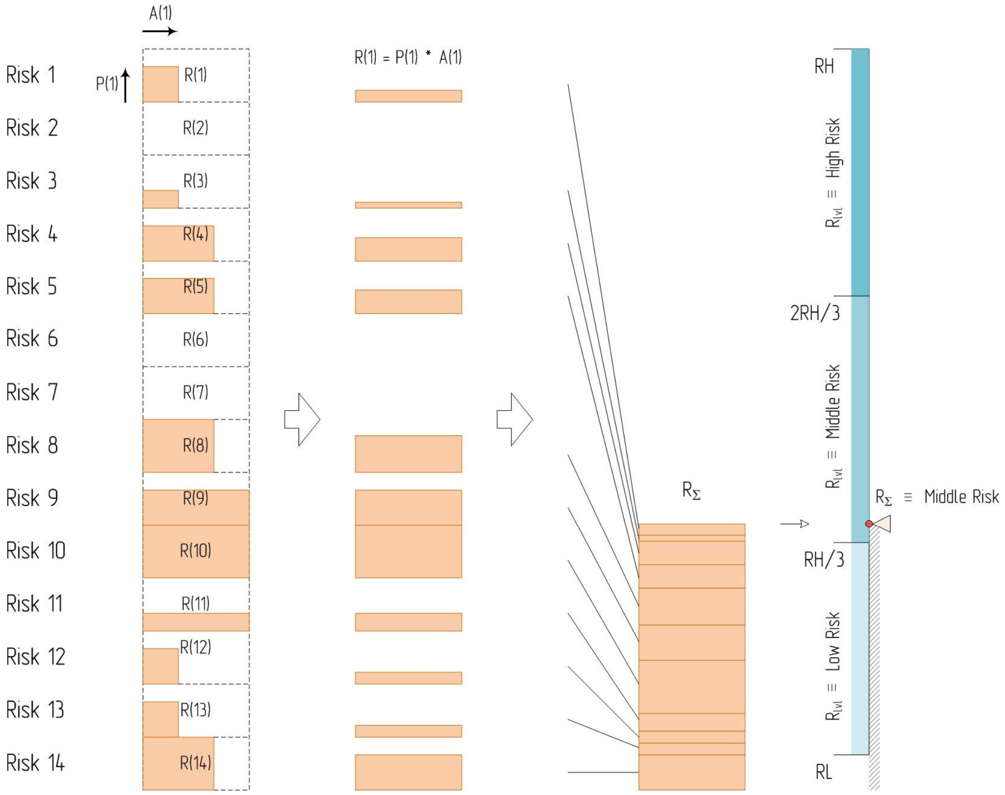

*Fig. 2 An example of the procedure for calculating and assessing the risks of FTA software*

**Table 2.** Definition of risk classes for software of MI according to WELMEC 7.2

| Risk class | Software protection level * | Software testing level * | Software compliance level * |
|---|---|---|---|
| A | L | L | L |
| B | M | M | L |
| C | M | M | M |
| D | H | M | M |
| E | H | H | M |
| F | H | H | H |

* Note: L is low level; M – meddle level; H - high level.

It should be noted that the number of possible threats for all types of MI under analysis is set to be the same, and for each specific type of MI, the total software risk is calculated according to expression (2). The level of risk for this MI SW is determined depending on the obtained value of the total risk under the distribution according to the expression (5).

## 6. Conclusions

For legally regulated MIs used in critical areas and for which WELMEC recommendation 7.2 does not apply, a generalized procedure for assessing risk classes was developed to determine the test level during the assessment of the compliance of MI SW. In the absence of statistical data on the probability of threat occurrence and data on the possible amount of damage from the implementation of these threats, it is suggested to use a subjective assessment to divide the probabilities and amount of damage into three groups (low, medium, high) with the assignment of conditional points. Conditional points are used to calculate and assess the total risk class for all threats.

Classifications of possible threats and vulnerabilities of MI SW related to such legally regulated functions as receiving, saving, and transmitting measurement data have been developed.

## 7. Gratitude

The authors express their gratitude to the Staff members of the Department of Information-Measuring Technologies of Lviv Polytechnic National University.

## 8. Mutual claims of authors

The authors declare the absence of any financial or other potential conflict related to this work.

## References

[1] Technical regulation of measuring equipment. Resolution of the Cabinet of Ministers of Ukraine, 24.02.2016, № 163. – Available at: https://zakon.rada.gov.ua/laws/show/163-2016-%D0%BF#Text.

[2] Technical regulation of legally regulated measuring equipment. Resolution of the Cabinet of Ministers of Ukraine, 13.01.2016, № 94. – Available at: https://zakon.rada.gov.ua/laws/show/94-2016-%D0%BF#Text.

[3] WELMEC 7.2:2021. Issue 9. Software Guide (Measuring Instruments Directive 2014/32/EU1). – WELMEC, 2021. – 148 c. https://www.welmec.org/welmec/documents/guides/7.2/2021/WELMEC_Guide_7.2_v2021.pdf.

[4] Directive 2014/32/EU of 26 February 2014 on the harmonization of the laws of the Member States relating to the making available on the market of measuring instruments (recast). – Available at: https://eur-lex.europa.eu/eli/dir/2014/32/oj.

[5] ISO/IEC 27005:2022, "Information technology – Security techniques – Information security risk management", ISO, 2022.

[6] ISO/IEC 18045:2008, "Common Methodology for Information Technology Security Evaluation", ISO, 2008.

[7] ISO/IEC 15408:2012, "Common Criteria for Information Technology Security Evaluation", ISO, 2012.

[8] M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology", 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, 2015, pp. 1113-1123, doi: 10.15439/2015F127.

[9] M. Esche, F. G. Toro, and F. Thiel, "Representation of attacker motivation in software risk assessment using attack probability trees", 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 2017, pp. 763-771, doi: 10.15439/2017F112.

[10] M. Esche and F. G. Toro, "Developing Defense Strategies from At-tack Probability Trees in Software Risk Assessment", 2020 15th Conference on Computer Science and Information Systems (FedCSIS), Sofia, Bulgaria, 2020, pp. 527-536, doi: 10.15439/2020F21.

[11] F. G. Toro, M. Koval, M. Esche, "Proposal for simplified implementation of risk assessment method for measuring instruments", 2018 Federated Conference on Computer Science and Information Systems (FedCSIS), Poznan, Poland, 2018, pp. 43-47. doi:10.15439/2018F377.

[12] WELMEC Guide 7.6, "Software Risk Assessment for Measuring Instruments", WELMEC, 2021. – Available at: https://www.welmec.org/welmec/documents/guides/7.6/2021/WELMEC_Guide_7.6_v2021.pdf.

[13] O. Velychko, T. Gordiyenko, and O. Hrabovskyi, "Testing of measurement instrument software on the national level", Eastern-European Journal of Enterprise Technologies. Information and control systems, 2018, № 2/9 (92), pp. 13–20. doi: 10.15587/1729-4061.2018.125994.

[14] O. Velychko, V. Gaman, T. Gordiyenko, and O. Hrabovskyi, "Testing of measurement instrument software with the purpose of conformity assessment", Eastern-European Journal of Enterprise Technologies. Information and control systems, 2019, № 1/9 (97), pp. 19–26. doi: 10.15587/1729-4061.2019.154352.

[15] O. Velychko, O. Hrabovskyi, and T. Gordiyenko, "Quality assessment of measurement instrument software with analytic hierarchy process", Eastern-European Journal of Enterprise Technologies. Information and control systems, 2019, № 4/9 (100), pp. 35–42. doi: 10.15587/1729-4061.2019.175811.

[16] List of categories of legally regulated measuring equipment subject to periodic verification. Resolution of the Cabinet of Ministers of Ukraine, 04.06.2015. № 374. – Available at: https://zakon.rada.gov.ua/laws/show/374-2015-%D0%BF#Text.