ORIGINAL CYBER SECURITY INDEXES (RATINGS) OF INTERNATIONAL CYBER SECURITY UNIVERSITY (ICU)

1. Cybersecurity Indices (Global Report)

CIGBR_ICU_Cybersecurity Indices Global Brief Report_International Cybersecurity University

Cybersecurity indices (global report).
Type - global.
Category - report.

Other parameters of the index are determined by its version. The format of the index version is CIGBR.XX.YY, where XX is the last two digits of the year, YY is the version number. The following is a description of the CIGBR.21.01 version.

The developer of the index is the *International Cybersecurity University* (ICU, website https://www.icu-ng.org/), Kyiv (Ukraine). ICU is a non-governmental public organization founded in 2019. The purpose of the organization's activity is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. ICU cooperates on a regular basis with 10 central executive bodies in Ukraine (including the State Service for Special Communications and Information Protection, the Ministry of Internal Affairs, the Ministry of Energy), and other market participants in the field of information security and cybersecurity. In 2020, the ICU established a research and training research center, and the organization - a scientific expert council in the field of information security and cybersecurity. The thematic areas of research, scientific and technical development, teaching and educational activities of the organization include information and communication technologies, energy and energy efficiency, environmental management, life sciences, new technologies for prevention and treatment of common diseases, new substances, and materials.

ICU_CIGBR contains a list, classification, and analysis of 65 global, international, and corporate indices (indexes) and ratings in the field of information security and cybersecurity. The report contains detailed information on indices, including their indicators (components, domains, sub-indices, *objectives*), methodologies and sources of development (formation). The first issue of the report as of June 1, 2021 in Ukrainian has been prepared. It is planned to update the first issue in English and launch the web portal ICU_CIGBR during 2021 - the first half of 2022.

The cybersecurity indices in the report are divided into:

- by types:
    - global;
    - international;
    - corporate;
- by categories:
    - reports;
    - expert;
    - network;
    - data sets;
    - financial (exchange);
    - combined;

- by organization of access or other indicators:

    - platforms;
    - questionnaires;
    - libraries;
    - applications;
    - automatic (or automated);
    - normative;
    - technical;
    - marketing.

The report does not contain statistics (rating information) but contains links to their sources.
Other indicators of cybersecurity indices presented in the report include:

- full and abbreviated name, country of developer (publisher);
- year of first release, frequency of publication;
- indicators;
- number of indexing subjects (entities);
- Ukraine's place in global and international rankings (if any);
- references to sources of development (formation) and methodology.

Methodology

The report is formed in accordance with the specified indexing deadlines. The subject or object of indexing is defined separately for each cybersecurity index. Indexing means any method of evaluation, usually with subsequent comparison of estimates with each other.

The subject of indexing includes:

- activities of indexing entities in the areas of information security and cybersecurity;
- state of information security and cybersecurity of indexing subjects (rating);
- the level of protection of indexing subjects (rating) from information security and cybersecurity threats;
- certain indicators of information security and cybersecurity, as well as protection against relevant threats;
- some indicators of the harmful effects of implemented threats.

The methodology of report formation is based on the method of expert assessments.

2. Local cybersecurity index

LCSI_ICU_Local CyberSecurity Index_International Cybersecurity University

Local CyberSecurity Index_Local CyberSecurity Index.

Type - corporate (corporative).

Category - combined.

Other parameters of the index are determined by its version. The format of the index version is LCSI.XX.YY, where XX is the last two digits of the year, YY is the version number. The following is a description of LCSI version.21.01.

The developer of the index is the *International Cybersecurity University* (ICU, website https://www.icu-ng.org/), Kyiv (Ukraine). ICU is a non-governmental public organization founded in 2019. The purpose of the organization - to create conditions for the safe operation of cyberspace, its use in the interests of the individual, society and the state. ICU cooperates on a regular basis with 10 central executive bodies in Ukraine (including the State Service for Special Communications and Information Protection, the Ministry of Internal Affairs, the Ministry of Energy), and other market participants in the field of information security and cybersecurity. In 2020, the ICU established a research and training research center, and the

organization - a scientific expert council in the field of information security and cybersecurity. The thematic areas of research, scientific and technical development, teaching and educational activities of the organization include information and communication technologies, energy and energy efficiency, environmental management, life sciences, new technologies for prevention and treatment of common diseases, new substances and materials.

As of June 1, 2021, pilot projects are underway to implement the index in the public sector and the energy sector.

Indexing objects (rating)

Object of indexing (subjective level) - the object of critical information infrastructure of the object of critical infrastructure, public authority, enterprise, institution, organization.

Indexing object (industry level) - critical information infrastructure, information, communication, network resources or a set of indexing objects (subject level) of critical infrastructure, industry, sector of the economy.

Indexing object (national level) - critical information infrastructure or set of indexing objects (sectoral level) of the country, information, communication, network resources of critical infrastructure of state and economic authorities, security and defense bodies, state registers, state electronic services or other electronic services used by more than 10% of the country's population.

Methodology of LCSI_ICU formation

The methodology for forming the LCSI.21.01 version of the index is based on the method of expert assessments. The formation of the following versions of the index will be additionally based on:

- index method of mathematical statistics;
- mathematical theory of ratings;
- game-theoretic cooperative resource model.

Indicators (subindexes) LCSI_ICU:

- Survey *Indicator* (*Indicator of the Survey* , abbr. - IS);
- Value of Audit (*Audit Indicator* , abbr. - AI);
- Indicator Monitoring Network (*Network Monitoring Indicator* , abbr, - NMI);

The IS survey indicator is formed by providing answers (filling in offline or online survey forms) by the owner (manager, trustee) of the indexing object.

The questions for the questionnaire for the LCSI.21.01 index version are formed taking into account (or in accordance with) up to:

- requirements of normative documents (ISO 27000, NIST CSF, CIS, ND TZI, Resolution of the Cabinet of Ministers of Ukraine № 518 of June 19, 2019);
- industry (corporate) requirements (requirements of organizations) for information security (network security, cybersecurity) of the indexing object;
- analyzed answers to questionnaires received earlier.

The version of the list of normative documents (standards), the requirements of which are used to form questionnaires, corresponds to the version of the index.

The AI audit indicator is formed by conducting an independent (state, mandatory, other) internal or external information security audit. The scope of audit tasks is determined by the owner (manager) of the indexing object, taking into account or in accordance with the requirements of regulatory documents.

As a rule, the following are subject to audit:

- questions mentioned in the questionnaire;
- thoroughness and depth of implementation of measures indicated in the questionnaire;
- processes and management of information security organization (network security, cybersecurity) .

The NMI network monitoring indicator is formed by analyzing:

- network traffic to detect cyberattacks and malicious activity from external vendors;
- internal network traffic and malicious activity within the perimeter;
- security of web resources;
- the results of a remote vulnerability scan.

The value of the LCSI_ICU index is calculated by the formula:

$$LCSI = (K_{is} * IS + K_{ai} * AI + K_{nmi} * NMI) / K_{norm}$$

where K_{is} - weighting factor IS;

K_{ai} - weighting factor AI;

K_{nmi} - weighting factor NMI;

K_{norm} - normalization factor to bring LCSI to a certain numerical scale.

All weights are dynamic, multifactorial and self-consistent. A detailed method of calculating the components of the index is developed separately in each case using the above methods.

LCSI_ICU version

The methodology of forming the LCSI version assumes the versioning of the index. For different versions of the index may change:

- number and list of index indicators;
- the number and list of components of the index;
- method of calculation (formation) of weight and other coefficients of the index;
- list and content of formation methods;
- scales for evaluating indicators (sub-indices) (the scale for evaluating the general index should be universal).

Requirements for the indexing object

Each of the requirements is unique. The calculation of the index can be based on any number of any of its indicators. (even on one indicator). Increasing the number of indicators and the quality of evaluation should only improve the indexing procedure.

Requirements for the indexing object:

- readiness to discuss the conditions of information exchange (sensitive information) and participation in indexing (rating);
- willingness to provide answers to questionnaires;
- readiness to pass the internal (external) information security audits provided by the method;
- readiness to receive and use network monitoring information from external suppliers and internal sources;
- availability of sensors at the entrance to the corporate network or data on network activity from partners (external suppliers);
- readiness to transfer open information about the value of the general index to the public sphere.