ОРИГІНАЛЬНІ ІНДЕКСИ (РЕЙТИНГИ) КІБЕРБЕЗПЕКИ МІЖНАРОДНОГО УНІВЕРСИТЕТУ КІБЕРБЕЗПЕКИ» (ICU)

1. Індекси кібербезпеки (глобальний звіт)

CIGBR_ICU_Cybersecurity Indices Global Brief Report_International Cybersecurity University

Індекси кібербезпеки (глобальний звіт).

Тип – глобальний (global).

Категорія – звіт (report).

Інші параметри індексу визначаються його версією. Формат версії індексу – CIGBR.XX.YY, де XX – останні дві цифри року, YY – номер версії. Нижче міститься опис версії CIGBR.21.01.

Розробник індексу – Міжнародний університет кібербезпеки (*International Cybersecurity University*, скор. – ICU, веб-сайт https://www.icu-ng.org/), Київ (Україна). ICU – неурядова громадська організація заснована у 2019 році. Мета діяльності організації – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. ICU на постійній основі співпрацює з 10 центральними органами виконавчої влади в Україні (у т. ч. Державною службою спеціального зв'язку та захисту інформації, Міністерством внутрішніх справ, Міністерством енергетики), іншими учасниками ринку у сфері інформаційної безпеки та кібербезпеки. У 2020 році в ICU створено науково-навчальний дослідницький центр, а при організації – наукову експертну раду в сфері інформаційної безпеки та кібербезпеки. До тематичних напрямів наукових досліджень, науково-технічних розробок, навчальної та освітньої діяльності організації належать інформаційні та комунікаційні технології, енергетика та енергоефективність, раціональне природокористування, науки про життя, нові технології профілактики та лікування поширених захворювань, нові речовини і матеріали.

ICU_CIGBR містить перелік, класифікацію та аналіз 65 глобальних, міжнародних і корпоративних індексів і рейтингів у сфері інформаційної безпеки та кібербезпеки станом. Звіт містить розгорнуті відомості про індекси, включаючи їх показники (складові, домени, субіндекси, *objectives*), методології та джерела розробок (формування). Підготовано перший випуск звіту станом на 01.06.2021 р. українською мовою. Заплановано оновлення першого випуску англійською мовою та запуск веб-порталу ICU_CIGBR протягом 2021-го - першої половини 2022-го року.

Індекси кібербезпеки у звіті поділяються:

- за типами:
  - глобальні;
  - міжнародні;
  - корпоративні;
- за категоріями:
  - звіти;
  - експертні;
  - мережеві;
  - набори даних;
  - фінансові (біржові);

    - комбіновані;
- за організацією доступу або іншими показниками:
    - платформи;
    - опитувальники;
    - бібліотеки;
    - додатки;
    - автоматичні (або автоматизовані);
    - нормативні;
    - технічні;
    - маркетингові.

Звіт не містить статистичних даних (рейтингових відомостей), але містить посилання на їхні джерела.

До інших показників індексів кібербезпеки, наведених у звіті, належать:

- повна та скорочена назва, країна розробника (видавника);
- рік першого релізу, періодичність видання;
- показники (objectives);
- кількість суб'єктів індексування;
- місце України у глобальних та міжнародних рейтингах (за наявністю);
- посилання на джерела розробки (формування) та методологію.

Методологія

Звіт формується у відповідності до визначених термінів індексування. Предмет або об'єкт індексування визначається окремо для кожного індексу кібербезпеки. Під індексуванням розуміється будь-який спосіб оцінювання, як правило, з подальшим порівнянням оцінок між собою.

Предмет індексування включає:

- діяльність суб'єктів індексування в сферах інформаційної безпеки та кібербезпеки;
- стан інформаційної безпеки та кібербезпеки суб'єктів індексування (рейтингування);
- рівень захищеності суб'єктів індексування (рейтингування) від загроз інформаційної безпеки та кібербезпеки;
- окремі показники інформаційної безпеки та кібербезпеки, а також захищеності від відповідних загроз;
- окремі показники шкідливого впливу реалізованих загроз.

Методологія формування звіту базується на методі експертних оцінок.

2. Локальний індекс кібербезпеки

LCSI_ICU_Local CyberSecurity Index_International Cybersecurity University

Локальний індекс кібербезпеки_Local CyberSecurity Index.

Тип – корпоративний (corporative).

Категорія – комбінований (combined).

Інші параметри індексу визначаються його версією. Формат версії індексу – LCSI.XX.YY, де XX – останні дві цифри року, YY – номер версії. Нижче міститься опис версії LCSI.21.01.

Розробник індексу – Міжнародний університет кібербезпеки (*International Cybersecurity University*, скор. – ICU, веб-сайт https://www.icu-ng.org/), Київ (Україна). ICU

– неурядова громадська організація заснована у 2019 році. Мета діяльності організації – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. ICU на постійній основі співпрацює з 10 центральними органами виконавчої влади в Україні (у т. ч. Державною службою спеціального зв'язку та захисту інформації, Міністерством внутрішніх справ, Міністерством енергетики), іншими учасниками ринку у сфері інформаційної безпеки та кібербезпеки. У 2020 році в ICU створено науково-навчальний дослідницький центр, а при організації – наукову експертну раду в сфері інформаційної безпеки та кібербезпеки. До тематичних напрямів наукових досліджень, науково-технічних розробок, навчальної та освітньої діяльності організації належать інформаційні та комунікаційні технології, енергетика та енергоефективність, раціональне природокористування, науки про життя, нові технології профілактики та лікування поширених захворювань, нові речовини і матеріали.

Станом на 01.06.2021 р. тривають пілотні проєкти з впровадження індексу в державному секторі та галузі енергетики.

Об'єкти індексування (рейтингування)

Об'єкт індексування (суб'єктний рівень) – об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури, органу державної влади, підприємства, установи, організації.

Об'єкт індексування (галузевий рівень) – критична інформаційна інфраструктура, інформаційні, комунікаційні, мережеві ресурси або сукупність об'єктів індексування (суб'єктний рівень) критичної інфраструктури, галузі, сектору економіки.

Об'єкт індексування (національний рівень) – критична інформаційна інфраструктура або сукупність об'єктів індексування (галузевий рівень) країни, інформаційні, комунікаційні, мережеві ресурси критичної інфраструктури органів управління державою та економікою, органів безпеки та оборони, державних реєстрів, державні електронні сервіси або інші електронні сервіси, якими користуються більше 10% населення країни.

Методологія формування LCSI_ICU

Методологія формування версії LCSI.21.01 індексу базується на методі експертних оцінок. Формування наступних версій індексу додатково базуватиметься на:

- індексному методі математичної статистики;
- математичній теорії рейтингів;
- теоретико-ігровій кооперативній ресурсній моделі.

Показники (субіндекси) LCSI_ICU:

- Показник опитування (*Indicator of the Survey*, скор.– IS);
- Показник аудиту (*Audit Indicator*, скор. – AI);
- Показник мережевого моніторингу (*Network Monitoring Indicator*, скор, – NMI);

Показник опитування IS формується шляхом надання відповідей (заповнення офлайн або онлайн форм опитування) власником (розпорядником, довіреною особою) об'єкту індексування.

Питання для опитувальника для версії LCSI.21.01 індексу формуються з врахуванням (або у відповідності) до:

- вимог нормативних документів (ISO 27000, NIST CSF, CIS, НД ТЗІ, Постанова КМУ № 518 від 19.06.2019);
- галузевих (корпоративних) вимог (вимог організацій) до інформаційної безпеки (мережевої безпеки, кібербезпеки) об'єкту індексування;

- проаналізованих відповідей на питання опитувальників, отриманих раніше.

Версія переліку нормативних документів (стандартів), вимоги яких використовуються для формування опитувальників, відповідає версії індексу.

Показник аудиту AI формується шляхом проведення незалежного (державного, обов'язкового, іншого) внутрішнього або зовнішнього аудиту інформаційної безпеки. Обсяг завдань аудиту визначається власником (розпорядником) об'єкту індексування з урахуванням або у відповідності до вимог нормативних документів.

Аудиту, як правило, підлягають:

- питання, зазначені в опитувальнику;
- ґрунтовність та глибина реалізації заходів, зазначених в опитувальнику;
- процеси та менеджмент організації забезпечення інформаційної безпеки (мережевої безпеки, кібербезпеки).

Показник мережевого моніторингу NMI формується шляхом аналізу:

- мережевого трафіку на виявлення кібератак та зловмисної активності від зовнішніх постачальників;
- внутрішнього мережевого трафіку та зловмисної активності всередині периметру;
- захищеності веб-ресурсів;
- результатів віддаленого сканування на вразливість.

Значення індексу LCSI_ICU розраховується за формулою:

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

де K_{is} – ваговий коефіцієнт IS;

K_{ai} – ваговий коефіцієнт AI;

K_{nmi} – ваговий коефіцієнт NMI;

K_{norm} – коефіцієнт нормалізації для приведення LCSI до певної числової шкали.

Усі вагові коефіцієнти є динамічними, багатофакторними та такими, що узгоджуються власне з собою. Деталізована методика розрахунку складових індексу розробляється окремо у кожному випадку з використанням наведених вище методів.

Версійність LCSI_ICU

Методологія формування версії LCSI передбачає версійність індексу. Для різних версій індексу можуть змінюватися:

- кількість та перелік показників індексу;
- кількість та перелік складових показників індексу;
- методика розрахунку (формування) вагових та інших коефіцієнтів індексу;
- перелік та зміст методів формування;
- шкали оцінок показників (субіндексів) (шкала оцінки загального індексу має бути універсальною).

Вимоги до об'єкту індексування

Кожна з вимог є невинятковою. Розрахунок індексу може відбуватися по довільної кількості будь-яких його показників. (навіть по одному показнику). Збільшення кількості показників та якості оцінювання має лише вдосконалювати процедуру індексування.

Вимоги до об'єкту індексування:

- готовність до обговорення умов обміну відомостями (чутливою інформацією) та участі у індексуванні (рейтингування);

- готовність надавати відповіді на питання опитувальників;
- готовність проходити передбачені методикою внутрішні (зовнішні) аудити інформаційної безпеки;
- готовність на отримання та використання відомостей мережевого моніторингу від зовнішніх постачальників та внутрішніх джерел;
- наявність сенсорів на вході до корпоративної мережі або даних про мережеву активність від партнерів (зовнішніх постачальників);
- готовність на передачу відкритої інформації про значення загального індексу до публічної сфери.