УДК 004.7

Mykola Khudyntsev, Candidate of Physical and Mathematic Science, Associated Professor of the Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine
ORCID ID: https://orcid.org/0000-0002-9324-6901
e-mail: nh@te.net.ua

Igor Palazhchenko, postgraduate of the Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine
ORCID ID: https://orcid.org/0009-0000-0491-7068
e-mail: palazhchenko.ihor@gmail.com

Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

CYBERSECURITY MATURITY MODELS FOR CYBERSECURITY ASSESSMENT IN CRITICAL INFRASTRUCTURE

Abstract. *The paper includes a list of existing maturity models (cybersecurity maturity) and an analysis of the application of these models for assessing cybersecurity, the level, and maturity of cyber security, the maturity of systems and processes for ensuring cybersecurity in critical infrastructure sectors, in the national cybersecurity system, the development of indicators and indices of the state of security (network, information security, cybersecurity).*

The paper substantiates and proposes a hierarchy of models for assessing the maturity of cyber security in the national cyber security ecosystem (in the national cyber security system, critical infrastructure, particularly the fuel and energy sector). The investigation's main goal is to intensify the implementation of existing assessment models using multi-level cyber security assessment models (cybersecurity maturity), accumulating statistical data on cyber incidents, cyber-attacks, and countermeasures for further use in predictive analysis and modeling.

The tasks of the research are the analysis, comparative analysis of existing models for evaluating the maturity of cyber security, formulation of evaluation models using indicators of cyber security and maturity of cyber security defined by existing normative documents, as well as in the construction of a hierarchy of models for evaluating cyber security in the national system of cyber security, critical infrastructure, fuel and energy sector, development of methodological bases for assessment using cyber security indices. A draft of the methodology for assessing the cyber security of electrical networks, suitable for use in critical infrastructure, has been developed.

Keywords: *information security, cyber security, maturity models, indicators of cybersecurity maturity.*

М.М. Худинцев, І.Л. Палажченко

Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України, м. Київ, Україна

МОДЕЛІ ЗРІЛОСТІ КІБЕРБЕЗПЕКИ ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Анотація. *Робота містить перелік існуючих моделей зрілості (зрілості кібербезпеки) та аналіз застосування цих моделей для оцінювання кібербезпеки, рівня, зрілості кібербезпеки, зрілості систем і процесів забезпечення кібербезпеки у секторах критичної інфраструктури, в національній системі кібербезпеки, розробки індикаторів та індексів стану безпеки (мережевої, інформаційної безпеки, кібербезпеки).*

У роботі обґрунтована та запропонована ієрархія моделей оцінювання зрілості кібербезпеки в національній екосистемі кібербезпеки (національній системі кібербезпеки, критичній інфраструктурі, зокрема, паливно-енергетичному секторі). Основною метою дослідження є активізація впровадження існуючих моделей оцінювання за допомогою різнорівневих моделей оцінювання кібербезпеки (зрілості кібербезпеки), накопичення статистичних даних щодо кіберінцидентів, кібератак, заходів протидії для подальшого використання цих даних у прогностичному аналізі та моделюванні.

Завдання дослідження полягають у аналізі, порівняльному аналізі існуючих моделей оцінювання зрілості кібербезпеки, формулюванні моделей оцінювання з використанням показників кібербезпеки та зрілості кібербезпеки, визначених існуючими нормативними документами, а також в побудові ієрархії моделей оцінювання кібербезпеки у національній системі кібербезпеки, критичній інфраструктурі, паливно-енергетичному секторі, розробці методологічних основ оцінювання за допомогою індексів кібербезпеки. Розроблено проєкт методики оцінювання кібербезпеки електричних мереж, придатний для використання у критичній інфраструктурі.

Ключові слова: *інформаційна безпека, кібербезпека, моделі зрілості, індикатори зрілості кібербезпеки.*

https://doi.org/10.32347/2411-4049.2024.4.122-134

Вступ

Сфера кібербезпеки (забезпечення кібербезпеки) України складалась протягом останніх 10-15 років, сфера функціонування та захисту критичної інфраструктури та її об’єктів – останніх 5-10 років. Після прийняття у 2016 році Стратегії кібербезпеки України [1], а в 2017 та 2021 роках, відповідно, законів України «Про основні засади забезпечення кібербезпеки України» [2] та «Про критичну інфраструктуру» [3] розпочався планомірний розвиток цих сфер з нормативних, організаційних та технічних питань. Протягом 2016-2022 років в Україні прийнято близько 50 нормативних документів різного рівня у сферах кібербезпеки та критичної інфраструктури. Склалася практика використання стандартів Європейського інституту телекомунікаційних стандартів (ETSI), Національного інституту стандартів і технології (NIST), Північноамериканської корпорації з електричної надійності (NERC), Асоціації аудиту і контролю інформаційних систем (ISACA). Профіль

застосування положень нормативної та розпорядчої документації визначається кожним суб’єктом забезпечення кібербезпеки відповідно до вимог національного законодавства (невариативна складова профілю) та кращих фахових практик (варіативна складова профілю).

У 2016-2022 роках в Україні також прийнято низку нормативних документів у сфері критичної інфраструктури, зокрема: укази Президента України, що вводили у дію рішення Ради національної безпеки і оборони України «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» (2016), «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури» (2017), постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» (2016), «Деякі питання об'єктів критичної інфраструктури» [4], «Деякі питання об'єктів критичної інформаційної інфраструктури» (2020) [5], методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (2021) [6], інші нормативні документи окремих державних органів з питань захисту галузевої інформаційної інфраструктури.

До основних нормативних документів у сферах інформаційної безпеки, кібербезпеки та кіберзахисту, окрім зазначених вище, належать: Закон України «Про ратифікацію Конвенції про кіберзлочинність (2005), укази Президента України, що вводили у дію рішення Ради національної безпеки і оборони України «Про Національний координаційний центр кібербезпеки» (2016), «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (2017), постанови Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» (2019) [7], «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» (2020), «Про затвердження Положення про організаційно-технічну модель кіберзахисту» (2021) [8], Стратегію кібербезпеки України в новій редакції (2021) [9].

Завданням С.3-19 Стратегії кібербезпеки України [9] передбачено розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб’єктів національної системи кібербезпеки на їх офіційних сайтах. Дані кіберстатистики (статистична інформація щодо кібератак, кіберінцидентів та заходів протидії) включають інформацію стосовно оцінювання кібербезпеки основних суб’єктів національної системи кібербезпеки, секторальних органів у сфері захисту критичної інфраструктури, міністерств та інших центральних органів виконавчої влади, інших державних органів, установ та організацій, інших юридичних осіб.

Відкрита російська військова агресія (2022-2023 рр.) призвела до поглиблення існуючих та появи нових викликів, загроз та інших чинників, які впливають на стан та розвиток сфери безпеки та кібербезпеки секторів критичної інфраструктури. Зокрема, зареєстровано значне збільшення кількості кібератак на державну, енергетичну та банківську інфраструктуру [10],

надзвичайної актуальності набрало питання збереження та відновлення паливно-енергетичного комплексу України [11-13]. Практично усі нормативні документи містять проблематику формування показників (індикаторів) кібербезпеки та її оцінювання, але питання оцінювання зрілості кібербезпеки практично не розглядається.

Проблема оцінювання кібербезпеки, зрілості кібербезпеки, зрілості систем і процесів у секторах критичної інфраструктури, в національній системі кібербезпеки, розробки індикаторів, індексів стану безпеки (мережевої, інформаційної безпеки, кібербезпеки, зрілості безпеки) є актуальною та далекою від остаточного вирішення [14-17].

Оцінювання зазначених показників має здійснюватися на підставі застосування індикаторів високого рівня та індексів (рейтингів) кібербезпеки [18], які свідчать про розвиток сил, заходів та засобів кібербезпеки.

Моделі оцінки і індексації кібербезпеки, проблема оцінки і індексації організаційних і технічних показників стану безпеки і кібербезпеки в критичній інфраструктурі розглядались також у роботах О. Суходолі, Ю. Харазішвілі, Д. Бобро, А. Сменковського, Г. Рябцева, С. Завгородньої, О. Павленко, А. Антоненко та інших [19-24]. В 2022-2023 роках прийнято низку нормативних документів із зазначених питань [6, 25-28].

У той же час проблема оцінювання зрілості кібербезпеки, як наступний етап розвитку складних інформаційних систем та інформаційного суспільства в цілому, не отримала в Україні необхідного рівня дослідження та нормативного забезпечення. Оцінювання зрілості кібербезпеки є важливим елементом загального аналізу кібербезпеки та актуальною задачею у інформаційній сфері з використанням інформаційно-комунікаційних технологій.

Показники, індикатори та ієрархія моделей для оцінювання зрілості кібербезпеки в критичній інфраструктурі

Оцінку зрілості кібербезпеки пропонується виконувати на підставі моделей, побудованих для наборів показників (індикаторів), визначених прийнятими в Україні нормативними документами, а саме:

- модель заходів кіберзахисту «1176» [29];
- модель заходів кіберзахисту «601» [6];
- модель заходів кіберзахисту «463» [26];
- модель заходів кіберзахисту «417» [27];
- модель заходів кіберзахисту «375» [28];
- модель оцінки зрілості кібербезпеки електричних мереж «908» [25],

а також узагальнююча модель індексування LCSI [18].

В рамках зазначених моделей проведення оцінювання здійснюється по N_D доменах (логічних областях оцінювання) і N_I показниках (параметрах, індикаторах) за N_L рівнями зрілості, в окремих випадках – ще по N_{sD} піддоменах (субдоменах) або *objectives*. Кількісні характеристики наборів параметрів деяких з розглянутих моделей наведені у Таблиці 1.

Рівень складності моделі, в цілому, підвищується в залежності від кількості показників N_I.

Показники моделей, як правило, групуються у домени і піддомени (логічні області, класи, категорії, підкатегорії або інші угруповання).

Таблиця 1. Набори параметрів моделей для оцінювання зрілості кібербезпеки

Модель	*Abbr.*	N_D	N_{sD}	N_I	N_L
Cybersecurity Capability Maturity Model, version 2.1	C2M2	10	43	356	4
Smart Grid Maturity Model, version 1.2	SGMM	8	40	178	6
Порядок проведення огляду стану кіберзахисту КІІ, ДІР, ІВЗВЗ	«1176»	6		29	2
Методичні рекомендації щодо підвищення рівня КЗ КІІ	«601»	5	23	108	4
Методичні рекомендації щодо забезпечення КЗ АСУ ТП	«463»	2	23	107	5
Вимоги з КБ ПЕС КІ	«417»	5	23	102	4
Порядок огляду стану КБ ПЕС КІ	«375»	13			2
Методика оцінки зрілості КБ електричних мереж	«908»	10	43	356	4
Локальний індекс кібербезпеки	LCSI	3	82	503	2

Головним показником моделі (моделі зрілості кібербезпеки, моделі заходів кіберзахисту) є рівень зрілості (кібербезпеки, заходу кіберзахисту). Рівні зрілості є обов'язковими показниками моделі та визначаються для усіх інших показників моделі. Етапність впровадження заходів кіберзахисту є необов'язковим показником моделі.

Індикатор моделі – значення показника (параметра), визначеного в рамках прийнятої моделі. Індикатори моделей мають чисельний вигляд або вигляд твердження (яке позначається текстом, умовним за змістом, наприклад, C1, MIL2, f.4 і т.п.).

Індекс моделі – інтегральний (усереднений за визначеною процедурою) індикатор моделі у випадку, коли усі індикатори моделі мають чисельний вигляд.

Якщо індикатор моделі не має чисельного вигляду, до нього може бути застосовано процедуру чисельної індикації. Під чисельною індикацією будемо розуміти визначення відповідності чисельного значення (балу або ваги) до індикатора, який має вигляд твердження. Алгоритм визначення відповідності визначається в рамках моделі.

У випадку, коли показники моделі оцінюються по двобальній системі, відповідні індикатори приймають значення:

- «1» – показник відповідає запропонованому твердженню;
- «0» – показник не відповідає запропонованому твердженню.

У інших випадках індикатори розраховуються за формулами, які визначаються в рамках відповідної моделі.

Оцінювання показників моделі здійснюється шляхом визначення (встановлення) відповідності:

- показнику моделі відповідає індикатор моделі у вигляді твердження;
- показнику моделі відповідає індикатор моделі у чисельному вигляді;
- показнику моделі відповідає індикатор моделі у вигляді твердження, до якого застосовано процедуру чисельної індикації.

У англомовній літературі показники і індикатори не розрізняються (використовується *indicators*).

Індекси кібербезпеки є узагальнюючими індикаторами («індикаторами індикаторів» або індикаторами 2-го рівня) та формуються (розраховуються) згідно з власною методологією.

За способом формування індекси кібербезпеки поділяються на синтетичні, аналітичні та автоматичні.

Синтетичні індекси кібербезпеки формуються в рамках моделей (фреймворків, усталених практик) оцінювання кібербезпеки (зрілості кібербезпеки), аналітичні – в рамках виключно аналітичних моделей (методологічних підходів) із застосуванням методу експертного оцінювання, автоматичні (в першу чергу, мережеві індекси кібербезпеки) – шляхом автоматичного збору та обробки інформації про інциденти, індикатори компрометації, загрози та ризики, як правило, технічного характеру.

Історично і методологічно моделі оцінювання кібербезпеки поділяються на моделі заходів кіберзахисту (МЗКЗ) та моделі зрілості кібербезпеки (МЗКБ). Ключовим критерієм моделі оцінювання кібербезпеки є вимірюваність показників МЗКЗ. Пропонується також додати до переліку цих моделей моделі індексів кібербезпеки (МІКБ): моделі синтетичних індексів кібербезпеки є розвитком моделей оцінювання кібербезпеки, моделі аналітичних та автоматичних індексів кібербезпеки на практиці застосовуються окремо (див. Рис. 1).

Основою методологічного підходу застосування індексів кібербезпеки має бути узгоджене оцінювання кібербезпеки (зрілості кібербезпеки) в рамках підходів, які використовують усі моделі синтетичних, аналітичних та автоматичних індексів кібербезпеки.

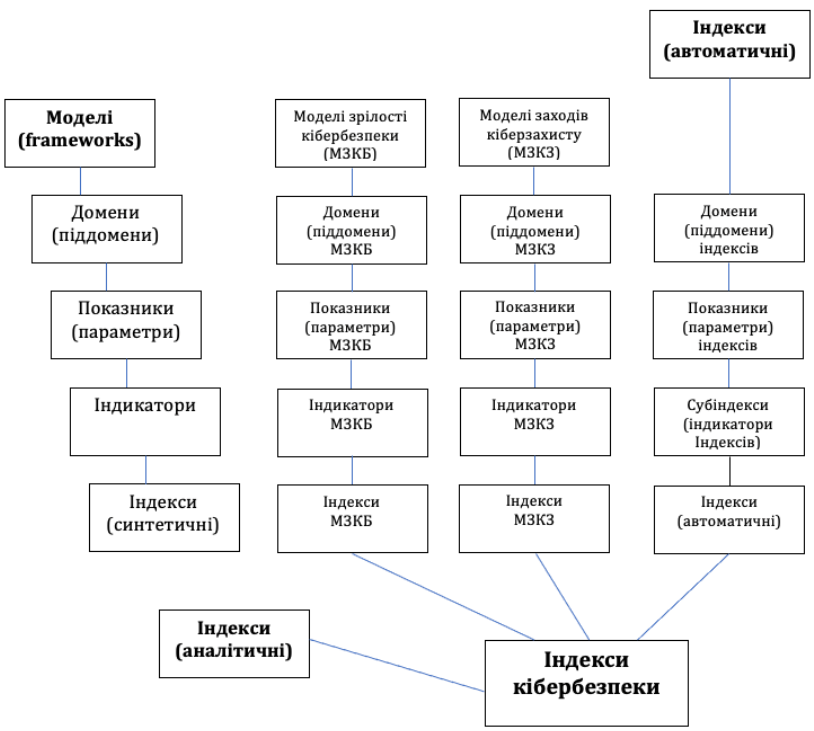

Рис. 1. Моделі оцінювання кібербезпеки (зрілості кібербезпеки)

Проведення оцінювання зрілості кібербезпеки

Проведення оцінювання зрілості кібербезпеки у критичній інфраструктурі, національній системі кібербезпеки, окремих суб'єктів забезпечення кібербезпеки має визначатися нормативно-правовим актом у встановленому порядку.

Методологічною основою для оцінювання є застосування відповідних запропонованих моделей. Процедура оцінювання має визначатися методикою оцінювання кібербезпеки або зрілості кібербезпеки.

Цільова група користувачів даних результатів оцінювання зрілості кібербезпеки в Україні має складатися з:

- Президента України (через робочий орган Ради національної безпеки і оборони – Національний координаційний центр кібербезпеки);
- державного органу, який призначений для формування та реалізації державної політики у сфері кіберзахисту;
- уповноваженого органу у сфері захисту критичної інфраструктури;
- секторальних органів у сфері захисту критичної інфраструктури.

Також до цільової групи можуть входити Верховна Рада України та Кабінет Міністрів України.

Форми оцінювання зрілості кібербезпеки:

- самооцінювання (суб'єктом оцінювання є власник або розпорядник об'єкта оцінювання);
- експертне оцінювання (суб'єктом оцінювання є особа, уповноважена на проведення оцінювання об'єкта оцінювання);
- індексування (суб'єкти оцінювання належать до цільової групи користувачів даних результатів оцінювання).

Оцінювання зрілості кібербезпеки здійснюється шляхом визначення (розрахунку, встановлення, формування) оцінки (індексу моделі) або профілю результатів оцінювання.

Профіль результатів оцінювання – це набір зафіксованих в результаті оцінювання індикаторів підходу або моделі. Профіль результатів оцінювання застосовується, якщо індикатори не мають чисельного вигляду.

Оцінка (індекс) – це усереднений за визначеною процедурою індикатор підходу або моделі у випадку, коли усі індикатори мають чисельний вигляд. Оцінка застосовується, якщо індикатори мають чисельний вигляд. Оцінка називається простою (зваженою) у випадку, коли ваги окремих індикаторів дорівнюють (відрізняються від) 0 або 1.

Визначення (розрахунок, формування) оцінки або профілю результатів оцінювання має відбуватися для кожного домену (піддомену) окремо і в цілому – для моделі.

Послідовність дій з оцінювання зрілості кібербезпеки:

1. Прийняття рішення про проведення оцінювання суб'єктом оцінювання.
2. Формування підстав та вихідних даних для проведення оцінювання.
3. Проведення оцінювання.
4. Формування звіту по результатах оцінювання.

Оцінювання має здійснюватися по мірі необхідності, але у будь-якому випадку – на регулярній основі не рідше 1 разу на рік.

Дані результатів оцінювання є адміністративними даними та даними кіберстатистики. Завдання з розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних вебсайтах визначено Стратегією кібербезпеки України (ціль С.3 абз.5).

Поводження з даними результатів оцінювання, захист цих даних має здійснюватися у відповідності до законодавства України.

Перегляд методики, показників та індикаторів оцінювання зрілості має здійснюватися за потребою, але не рідше ніж 1 раз на 2 роки.

Висновки

Запропоновані підходи та моделі оцінювання мають застосовуватися у залежності від рівня розвитку сил, засобів і заходів забезпечення кібербезпеки або кіберзахисту.

Проведено аналіз існуючих моделей оцінювання зрілості кібербезпеки, сформульовані моделі оцінювання з використанням показників кібербезпеки та зрілості кібербезпеки, визначених існуючими нормативними документами. Визначено ієрархію моделей оцінювання з урахуванням складу та кількості показників різних моделей оцінювання для національної системи кібербезпеки та секторів критичної інфраструктури. Запропоновано використання індексів кібербезпеки для індексування моделей оцінювання зрілості.

Відповідний аналіз та пропозиції застосовано для опису та впровадження процедури оцінювання зрілості кібербезпеки електричних мереж України. За основу було взято підходи, використані у моделі C2M2, з використанням також інших моделей оцінювання з показниками, визначеними існуючими нормативними документами. Розроблені методологічні основи та проєкт методики оцінки зрілості кібербезпеки електричних мереж.

Завдання з розробки методики оцінки зрілості кібербезпеки електричних мереж України визначено Концепцією впровадження “розумних мереж” в Україні до 2035 року та планом її реалізації. Дослідження та отримання науково-практичного результату здійснюються в рамках Другого проєкту передачі електроенергії, компонент 3 «Консультаційні послуги із запровадження системи оцінювання зрілості кібербезпеки в енергетичній системі України» (Позика № 8462-UA Світового банку).

СПИСОК ЛІТЕРАТУРИ

1. Стратегія кібербезпеки України (2016). Президент України. Указ від 15.03.2016 № 96/2016. Retrieved from https://www.president.gov.ua/documents/962016-19836.
2. Про основні засади забезпечення кібербезпеки України (2017). Верховна Рада України. Закон України від 05.10.2017 № 2163-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Про критичну інфраструктуру (2021). Верховна Рада України. Закон України від 16.11.2021 № 1882-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
4. Деякі питання об'єктів критичної інфраструктури (2020). Кабінет Міністрів України. Постанова від 09.10.2020 № 1109. Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

5. Деякі питання об'єктів критичної інформаційної інфраструктури (2020). Кабінет Міністрів України. Постанова від 09.10.2020 № 943. Retrieved from https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.
6. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (2021). Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Наказ від 06.11.2021 № 601. Retrieved from https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.
7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (2019). Кабінет Міністрів України. Постанова від 19.06.2019 № 518. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.
8. Про затвердження Положення про організаційно-технічну модель кіберзахисту (2021). Кабінет Міністрів України. Постанова від 29.12.2021 № 1426. Retrieved from https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.
9. Стратегія кібербезпеки України (2021). Президент України. Указ від 26.08.2021 № 447/20. Retrieved from https://www.president.gov.ua/documents/4472021-40013.
10. Кількість кібератак на енергетичну інфраструктуру з початку війни зросла на третину – Міненерго (2022). А. Жарікова. Листопад, 21, 2022. Київ. Retrieved from https://www.epravda.com.ua/news/2022/11/21/694084/.
11. Кібербезпека та стійкість об'єктів енергетики в суспільстві та державі в нормальних, критичних та аварійних умовах (2022). ІПМЕ. Енергетична криза & Кібербезпека, H2020 Електронний міжнародний захід, Баку, Азербайджан, 05-07.12.2022. Retrieved from https://electron-project.eu/blog/cybersecurity-and-sustainability-of-energy-sector-facilities-in-society-and-the-state-in-normal-critical-and-emergency-circumstances/#.
12. Д. Евенсен, Б. Совакул, Н. Далтон, К. Глебова (2022). Енергетична безпека, зміна клімату та майбутня відбудова України. Інститут глобального сталого розвитку Бостонського університету, Бостон, Массачусетс, США. 20 с. – Retrieved from https://www.bu.edu/igs/2022/10/20/energy-security-climate-change-and-the-future-of-ukraine-reconstruction/.
13. Кібербезпека в енергетичному секторі: які виклики стоять перед об'єктами критичної інфраструктури України? (2022). Ф. Сафаров, Є. Владіміров, С. Бракко, О. Харковина, Д. Дзядек. Energy Security Forum: Післявоєнне відновлення енергетичного сектору України, 21-25.11.2022, Київ. Retrieved from https://iclub.energy/energysecurityforum2022#!/tab/505198962-1.
14. Розробка концептуальних засад і науково-методичної бази оцінювання стану кібербезпеки та рівня захищеності інформаційних активів та ресурсів суб'єктів забезпечення кібербезпеки України (2021). Реєстраційна картка НДДКР 0121U112396, дата реєстрації: 29-07-2021, Громадська організація «Міжнародний університет кібербезпеки».
15. Розроблення переліку, методики оброблення для публікацій статистичних даних про кіберінциденти/кібератаки (2023). Реєстраційна картка НДДКР 0123U102272, дата реєстрації: 19-04-2023, Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.
16. М.М. Худинцев (2023). Концептуальні положення забезпечення кібербезпеки енергетичної галузі України, ISSN 0204–3572. Електрон. моделювання. Т. 45. № 1, С. 80-97. Retrieved from https://www.emodel.org.ua/images/em/45-1/45-1-6.pdf.
17. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-031-46880-3_17.

18. Худинцев М.М. (2021). Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог) / М.М. Худинцев, А.В. Жилін, А.В. Давидюк. – Київ: Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. ISBN 978-966-136-887-2. 240 с.
19. Суходоля О.М. (2020). Енергетична безпека України: методологія системного аналізу та стратегічного планування : аналіт. доп. / О.М. Суходоля, Ю.М. Харазішвілі, Д.Г. Бобро, А.Ю. Сменковський, Г.Л. Рябцев, С.П. Завгородня. Київ : НІСД. 178 с.
20. Суходоля О.М. (2021). Визначення рівня енергетичної безпеки України : аналіт. доп. / О.М. Суходоля, Ю.М. Харазішвілі, Д.Г. Бобро, А.Ю. Сменковський, Г.Л. Рябцев, С.П. Завгородня. Київ : НІСД. 71 с.
21. Суходоля О. (2022). Оцінка стійкості енергетичної інфраструктури України : аналіт. звіт / О. Павленко, А. Антоненко, Р. Ніцович, С. Євтушок, О. Суходоля. Київ : ГО «Діксі Груп». 72 с.
22. Гулак Г.М. (2021). Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики / Г.М. Гулак, І.С. Скітер, Є.Г. Гулак // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". Вип. 4(12). С. 172-186.
23. Кібербезпека енергетики, Науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : запрошення, програма та матеріали, 28 травня 2021 р. (2021). Київ : ІПМЕ ім. Г.Є. Пухова НАН України. 61 с.
24. Кібербезпека енергетики, Науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : запрошення, програма та матеріали, 27 травня 2022 р. (2022). Київ : ІПМЕ ім. Г.Є. Пухова НАН України. 128 с.
25. Концепції впровадження "розумних мереж" в Україні до 2035 року (2022). Кабінет Міністрів України. Розпорядження від 14 жовтня 2022 р. № 908-р. Retrieved from https://zakon.rada.gov.ua/laws/show/908-2022-%D1%80#Text.
26. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами (2023). Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Наказ від 29.05.2023 № 463. Retrieved from https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami.
27. Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури (2022). Міністерство енергетики України. – Наказ від 15.12.2022 № 417. Retrieved from https://zakon.rada.gov.ua/laws/show/z0249-23#Text.
28. Порядок огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури (2023). Міністерство енергетики України, КЕП (підписання) Галущенко Г.В. Наказ від 16.01.2023. Retrieved from https://mev.gov.ua/sites/default/files/2023-01/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7%20%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA%20%281%29.pdf.
29. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Кабінет Міністрів України, Постанова від 11.11.2020 № 1176.

Стаття надійшла до редакції 23.08.2024 і прийнята до друку після рецензування 20.11.2024

REFERENCES

1. Cybersecurity Strategy of Ukraine (2016). President of Ukraine. Decree of 15.03.2016 No. 96/2016. Retrieved from https://www.president.gov.ua/documents/962016-19836
2. On the Basic Principles of Ensuring Cybersecurity of Ukraine (2017). Verkhovna Rada of Ukraine. Law of Ukraine of 05.10.2017 No. 2163-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. On Critical Infrastructure (2021). Verkhovna Rada of Ukraine. Law of Ukraine of 16.11.2021 No. 1882-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text
4. Some issues of critical infrastructure facilities (2020). Cabinet of Ministers of Ukraine. Resolution of 09.10.2020 No. 1109. Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text
5. Some issues of critical information infrastructure facilities (2020). Cabinet of Ministers of Ukraine. Resolution of 09.10.2020 No. 943. Retrieved from https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
6. Methodological recommendations for increasing the level of cyber protection of critical information infrastructure (2021). Administration of the State Service for Special Communications and Information Protection of Ukraine. Order dated 06.11.2021 No. 601. Retrieved from https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
7. On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities (2019). Cabinet of Ministers of Ukraine. Resolution dated 19.06.2019 No. 518. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
8. On approval of the Regulation on the organizational and technical model of cyber defense (2021). Cabinet of Ministers of Ukraine. Resolution of 29.12.2021 No. 1426. Retrieved from https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
9. Cybersecurity Strategy of Ukraine (2021). President of Ukraine. Decree of 26.08.2021 No. 447/20. Retrieved from https://www.president.gov.ua/documents/4472021-40013
10. Zharikova, A. (November, 21, 2022). The number of cyberattacks on energy infrastructure has increased by a third since the beginning of the war – Ministry of Energy. Kyiv. Retrieved from https://www.epravda.com.ua/news/2022/11/21/694084/
11. Cybersecurity and Sustainability of Energy Sector Facilities in Society and the State in Normal, Critical and Emergency Circumstances (2022). IPME. Energy Crisis & Cybersecurity, H2020 Electronic International Event, Baku, Azerbaijan, 05-07.12.2022. Retrieved from https://electron-project.eu/blog/cybersecurity-and-sustainability-of-energy-sector-facilities-in-society-and-the-state-in-normal-critical-and-emergency-circumstances/#
12. Evensen, D., Sovakul, B., Dalton, N., Glebova, K. (2022). Energy Security, Climate Change and the Future Reconstruction of Ukraine. Institute for Global Sustainability, Boston University, Boston, Massachusetts, USA. 20 p. Retrieved from https://www.bu.edu/igs/2022/10/20/energy-security-climate-change-and-the-future-of-ukraine-reconstruction/
13. Safarov, F., Vladimirov, E., Brakko, S., Kharkovyna, O., Dzyadek, D. (2022). Cybersecurity in the Energy Sector: What Challenges Face Ukraine's Critical Infrastructure? Energy Security Forum: Postwar Reconstruction of Ukraine's Energy Sector, 21-25.11.2022, Kyiv. Retrieved from https://iclub.energy/energysecurityforum2022#!/tab/505198962-1
14. Development of conceptual principles and scientific and methodological basis for assessing the state of cybersecurity and the level of security of information assets and resources of cybersecurity entities of Ukraine (2021). Registration card R&D 0121U112396, registration date: 29-07-2021, Public organization "International University of Cybersecurity".
15. Development of a list, processing methods for publications of statistical data on cyber incidents/cyberattacks (2023). Registration card R&D 0123U102272, registration date: 19-04-2023, Institute of Modeling Problems in Energy named after G. E. Pukhov of the National Academy of Sciences of Ukraine.

16. Khudyntsev, M.M. (2023). Conceptual provisions for ensuring cybersecurity of the energy sector of Ukraine. *Electronic modeling*, 45, 1, 80-97. Retrieved from https://www.emodel.org.ua/images/em/45-1/45-1-6.pdf
17. Khudyntsev, M., Lebid, O., Bychenok, M., Zhylin, A., Davydiuk, A. (2023). Network Monitoring Index in the Information Security Management System of Critical Information Infrastructure Objects. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-031-46880-3_17
18. Khudintsev, M.M., Zhilin, A.V., Davydyuk, A.V. (2021). World Cybersecurity Indices: Overview and Formation Methods (Global Report / Catalog). Kyiv: International Cybersecurity University, Institute of Modeling Problems in Energy named after G.E. Pukhov NAS of Ukraine. ISBN 978-966-136-887-2. 240 p.
19. Sukhodolya, O.M., Kharazishvili, Y.M., Bobro, D.G., Smenkovsky, A.Yu., Ryabtsev, G.L., Zavgorodnya, S.P. (2020). Energy Security of Ukraine: Methodology of System Analysis and Strategic Planning: Analytical Supplement. Kyiv: NISD.
20. Sukhodolya, O.M. et al. (2021). Determining the level of energy security of Ukraine: analytical supplement. Kyiv: NISD.
21. Sukhodolya, O. et al. (2022). Assessment of the stability of the energy infrastructure of Ukraine: analytical report. Kyiv: NGO "Dixie Group".
22. Gulak, G.M., Skeeter, I.S., Gulak, E.G. (2021). Methodological principles for the creation and functioning of a cybersecurity center for information infrastructure of nuclear power facilities. *"Cybersecurity: education, science, technology"*, 4(12), 172-186.
23. Cybersecurity of energy. (2021). In Scientific and practical conference of the Institute of Modeling Problems in Energy named after G.E. Pukhov of the National Academy of Sciences of Ukraine: invitation, program and materials, May 28, 2021. Kyiv: IPME named after G.E. Pukhov of the National Academy of Sciences of Ukraine.
24. Cybersecurity of energy. (2022). In Scientific and practical conference of the Institute of Modeling Problems in Energy named after G.E. Pukhov of the NASU: invitation, program and materials, May 27, 2022. Kyiv: IPME named after G.E. Pukhov of the NASU.
25. Concepts of implementation of "smart grids" in Ukraine to 2035 (2022). Cabinet of Ministers of Ukraine. Order of October 14, 2022 No. 908-p. Retrieved from https://zakon.rada.gov.ua/laws/show/908-2022-%D1%80#Text
26. Methodological recommendations for ensuring cyber protection of automated technological process control systems (2023). Administration of the State Service for Special Communications and Information Protection of Ukraine. Order of 05/29/2023 No. 463. Retrieved from https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami
27. Requirements for cybersecurity of the fuel and energy sector of critical infrastructure (2022). Ministry of Energy of Ukraine. Order of 12/15/2022 No. 417. Retrieved from https://zakon.rada.gov.ua/laws/show/z0249-23#Text
28. Procedure for reviewing the state of cybersecurity of the fuel and energy sector of critical infrastructure (2023). Ministry of Energy of Ukraine. Order dated 16.01.2023. Retrieved from https://mev.gov.ua/sites/default/files/2023-01/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7%20%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA%20%281%29.pdf
29. Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for protection of which is established by law (2020). Cabinet of Ministers of Ukraine, Resolution dated 11.11.2020 No. 1176.

The article was received 23.08.2024 and was accepted after revision 20.11.2024

Худинцев Микола Миколайович
кандидат фізико-математичних наук, доцент, академік Академії зв'язку України, Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000-0002-9324-6901 ***e-mail:*** nh@te.net.ua

Палажченко Ігор Леонідович
аспірант, Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: 03186, Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0009-0000-0491-7068 ***e-mail:*** palazhchenko.ihor@gmail.com