ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.30.18610

СИСТЕМА ОЦІНЮВАННЯ ПІДВИЩЕННЯ СТАНУ КІБЕРЗАХИСТУ ОБ'ЄКТІВ ОГЛЯДУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Олександр Корченко[1], Євгенія Іванченко[2]

[1]Державний університет інформаційно-комунікаційних технологій
[2]Національний авіаційний університет

КОРЧЕНКО Олександр Григорович, д.т.н., проф.
Рік та місце народження: 1961 рік, м. Київ.
Освіта: Київський інститут інженерів цивільної авіації, 1983 рік.
Посада: перший проректор Державного університету інформаційно-комунікаційних технологій, завідувач кафедри Безпеки інформаційних систем і технологій Університету Комісії народної освіти (Краків, Польща), професор кафедри Безпеки інформаційних технологій Національного авіаційного університету, член-кореспондент НАН України, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки.
Наукові інтереси: кібербезпека та захист інформації.
Публікації: понад 390 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: agkorchenko@gmail.com.
Orcid ID: 0000-0003-3376-0631.

ІВАНЧЕНКО Євгенія Вікторівна, к.т.н., проф., лауреат Національної премії України ім. Б. Патона
Рік та місце народження: 1976 рік, м. Київ.
Освіта: Київський міжнародний університет цивільної авіації.
Посада: в.о. завідувача кафедри безпеки інформаційних технологій з 2023 року.
Наукові інтереси: кібербезпека та захист інформації.
Публікації: близько 130 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: evivancenko@gmail.com.
Orcid ID: 0000-0003-3017-5752.

***Анотація**. У сучасному цифровому світі, де величезна частина наших повсякденних дій відбувається в онлайн просторі, безпека кіберпростору стає невід'ємною складовою національної безпеки кожної держави. Особливо важливою виявляється захист критичної інфраструктури, яка забезпечує функціонування економіки, комунікацій та суспільства загалом. У зв'язку з цим, розробка та впровадження системи оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури стає надзвичайно актуальним завданням для держав та організацій. Запропонована структурна модель системи оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави, яка за рахунок бази даних заходів кіберзахисту, правил та еталонів, а також модулів формування поточних значень, фазифікації і формування ЛЗ, формування характеристик огляду та параметрів наближеності, дозволить реалізувати оцінювати підвищення рівня стану кіберзахисту об'єктів критичної інфраструктури в слабоформалізованому нечіткому довкіллі. У даному контексті, її впровадження стає критично важливим кроком для забезпечення безпеки критичної інфраструктури держави в умовах постійно зростаючих кіберзагроз. Вона сприяє підвищенню рівня готовності та стійкості до потенційних кібератак, що є невід'ємною складовою стратегії забезпечення національної безпеки.*

***Ключові слова**: інформаційна безпека, кібербезпека, захист інформації, кіберзахист, об'єкт огляду критичної інфраструктури, критична інфраструктура, кіберзагрози, оцінювання стану кіберзахисту, нечіткі множини.*

Постановка проблеми

В сучасному світі, де величезну частину життя перенесено в цифровий простір, кіберзахист стає надзвичайно важливим аспектом забезпечення національної безпеки. Перед урядами і організаціями стоїть завдання ефективного захисту критичної інфраструктури від кіберзагроз. Для досягнення цієї мети необхідно мати систему оцінювання, яка спрямована на контролювання стану кіберзахисту об'єктів огляду критичної інфраструктури держави. Така система оцінювання відіграє ключову роль у виявленні слабких місць в захисті, ідентифікації потенційних загроз та визначенні оптимальних стратегій реагування.

Вона базується на аналізі різноманітних параметрів, включаючи рівень захисту, уразливості, реакційність до загроз, ефективність заходів безпеки та інші.

Система буде орієнтована не лише на забезпечення оперативного реагування на потенційні кіберзагрози, а й створення стратегій превентивних заходів, що дозволить уникнути можливих атак та сприятиме підвищенню рівня готовності і реакції до можливих кібернападів, що є критичним у забезпеченні безпеки держави.

У даному контексті система оцінювання стає ключовим інструментом для ефективного управління кіберзахистом, допомагаючи урядам та відповідальним організаціям збільшити стійкість критичної інфраструктури до сучасних кіберзагроз.

Актуальність системи оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави в сучасний період надзвичайно висока. Зростання кількості та складності кіберзагроз, а також постійне вдосконалення технологій, що використовуються порушниками, роблять кібербезпеку однією з найбільш актуальних та важливих сфер для будь-якої держави.

Критична інфраструктура, така як енергетика, транспорт, медицина тощо є основними складовими національної безпеки та економічного розвитку. Уразливість цих систем до кібератак може мати серйозні наслідки для суспільства та економіки країни. Система оцінювання підвищення стану кіберзахисту допомагає ідентифікувати, аналізувати та усувати потенційні загрози для критичної інфраструктури. Вона забезпечить ефективну можливість реагування на кіберзагрози, а також вчасно розробляти та впроваджувати стратегії кіберзахисту. У контексті постійно зростаючої кількості кібератак та їхньої складності, а також швидкого розвитку цифрових технологій, система оцінювання кіберзахисту стає невід'ємною складовою ефективної національної стратегії безпеки. Вона допоможе державам залишатися впевненими у стійкості своєї критичної інфраструктури перед сучасними кіберзагрозами.

Аналіз останніх джерел та публікацій

Сучасні систем оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави відповідають наступним ключовим критеріям:

- методологія та підходи до оцінки: різні системи можуть використовувати різні методології та підходи до оцінки стану кіберзахисту. Деякі можуть базуватися на кількісних метриках, таких як рівень захисту чи вразливостей, тоді як інші можуть використовувати більш кількісні методи, такі як рівень відповідності до стандартів безпеки;
- обсяг оцінки: деякі системи можуть оцінювати лише певні аспекти безпеки, такі як мережевий захист або захист даних, тоді як інші можуть охоплювати ширший спектр компонентів, включаючи фізичну та кібербезпеку;
- гнучкість та адаптивність: деякі системи можуть бути більш гнучкими та адаптивними до змін технологій та кіберзагроз, в той час як інші характеризуватимуться низькоадаптивними та менш придатними до швидких змін;
- реагування на інциденти: деякі системи можуть мати більш розвинені процедури реагування на кіберінциденти та розробку стратегій відновлення, тоді як інші бути менш зорієнтованими на цей аспект;
- масштабованість: деякі системи можуть бути більш придатними для використання на рівні окремих організацій або підприємств, а інші орієнтовані для застосування на національному рівні або для оцінки кіберзахисту на рівні критичної інфраструктури держави.

Існує кілька систем оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави, кожна з яких має свої унікальні особливості, наприклад NIST, Cybersecurity Framework (CSF) - базується на основних принципах кіберзахисту: захист, виявлення, реагування та відновлення [1]. Зазначена CSF оцінює кіберзахист за допомогою рамки, що охоплює п'ять основних категорій та понад 100 підкатегорій. Ця система гнучка та може бути адаптована до різних організаційних потреб, також CSF надає рекомендації щодо реагування на кіберінциденти та відновлення після них. Система ISO/IEC 27001 надає загальний підхід до управління інформаційною безпекою, включаючи кіберзахист, охоплює широкий спектр аспектів кіберзахисту, включаючи організаційні процеси, фізичні та технічні заходи безпеки, дозволяє організаціям розробляти власні системи кіберзахисту, що відповідають їхнім потребам та надає вказівки щодо реагування на кіберінциденти та відновлення після них [2]. Система Cybersecurity Maturity Model Certification (CMMC) розроблена за ініціативою військового відомства США і визначає п'ять рівнів зрілості кіберзахисту, від базового до продвинутого, оцінює зрілість кіберзахисту відповідно до вимог, що визначені для кожного рівня, має обов'язкові вимоги для підприємств, що працюють з військовими даними та контрактами, надає рекомендації щодо реагування на кіберінциденти та відновлення після них [3]. Також ще відомі системи оцінювання рівня кіберзахисту [4-6], але вони не враховують специфіку критичних інфраструктур та не використовують відповідні сучасні техніки та інструменти.

Мета та постановка завдання

Зазначені системи відзначаються своєю унікальністю до вирішення задач оцінювання, але всі вони спрямовані на поліпшення кіберзахисту та забезпечення безпеки критичної інфраструктури держави і не орієнтовані на оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави. Зазначимо, що вибір конкретної системи залежить від потреб, характеристик та стратегій кіберзахисту конкретної організації чи держави. Тому метою роботи є побудова такої системи, яка забезпечить оцінювання рівня підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави. Це досягається за рахунок використання розроблених методів оцінювання стану кіберзахисту та рівня його підвищення, а також відповідних моделей даних та системи їх характеристик для оцінювання заходів кіберзахисту в Україні. Розробка дозволить ефективно і оперативно визначати поточний стан рівня кіберзахисту об'єктів критичної інфраструктури.

Виклад основного матеріалу дослідження

На базі методики оцінювання стану кіберзахисту критичної інформаційної інфраструктури Державної служби спецзв'язку та захисту інформації України [7], моделі системи характеристик даних для

оцінювання заходів кіберзахисту в Україні [8], моделі даних для оцінювання стану кіберзахисту в Україні [9], методу оцінювання стану кіберзахисту об'єкту огляду критичної інфраструктури держави [10] та методу оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави [11] побудуємо систему оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави, яка дозволить автоматизувати відповідний процес оцінювання.

Структурна модель системи оцінювання підвищення стану кіберзахисту СМСО (рис. 1) складається з:

- бази даних заходів кіберзахисту (БДЗКЗ);
- бази даних правил (БДП);
- бази даних еталонів (БДЕ);

а також модулі:

- модуля формування поточних значень (МФПЗ);
- модуля фазифікації і формування ЛЗ (МФФЛЗ);
- модуля формування характеристик об'єкту огляду (МФХОО);
- модуля формування параметрів наближеності (МФПН);
- модуля візуалізації (МВ).

База БДЗКЗ містить множину ЗКЗ $\tilde{\boldsymbol{E}} = \{\cup_{q=1}^{m} \tilde{E}_{\square}^{q}\} = \{\tilde{E}^1, \tilde{E}_{\square}^2, \dots \tilde{E}_{\square}^m\}$, де $\tilde{E}_{\square}^{q} \subseteq \tilde{\boldsymbol{E}}(q = \overline{1,m})$ НЧ, що характеризує q-ий об'єкт огляду, а m – їх кількість [8,9.], за допомогою яких здійснюється визначення стану кіберзахисту q-го об'єкту огляду критичної інфраструктури держави (див. етап 4 в [10]):

$$\tilde{E}^{\boldsymbol{q}} = (\sum_{i=1}^{n} \widetilde{SD}_i^q)/n = (\widetilde{SD}_1^q \oplus \widetilde{SD}_2^q \oplus \dots \oplus \widetilde{SD}_n^q)/n,$$

де $\widetilde{SD}_{\boldsymbol{i}}^{\boldsymbol{q}}(i = \overline{1,n})$ i-та характеристика q-го об'єкту огляду, n – кількість характеристик (категорій), а $\widetilde{\oplus}$ – нечітка сума [6];

$$\tilde{E}^{\boldsymbol{q}} = \frac{\sum_{i=1}^{\eta} \widetilde{ACM}_i^q}{\eta} = (\widetilde{ACM}_1^q \widetilde{\oplus} \widetilde{ACM}_2^q \widetilde{\oplus} \dots \widetilde{\oplus} \widetilde{ACM}_n^q)/\eta,$$

де $\widetilde{ACM}_{\boldsymbol{i}}^{\boldsymbol{q}}(i = \overline{1,\eta})$ i-й клас заходів кіберзахисту q-го об'єкту огляду, η – кількість категорій [10].

База БДП складається з узагальнених значень $\widetilde{SD}_{ij}^q$ та $\widetilde{ACM}_{ij}^q$, які входять до множини базових правил:

$$AR(\widetilde{SD}_{\square}^q; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T}'_{SCS}/ECI') \text{ та}$$
$$AR(\widetilde{ACM}_{\square}^q; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T}'_{SCS}/ECI'),$$

де $\widetilde{ACM}_{ij}^q$ та $\widetilde{SD}_{ij}^q$ – i-ті характеристики об'єкту огляду, $j = \overline{1,f}$, а $\underset{\sim}{T}_{SCSi}$ – рівні захисту.

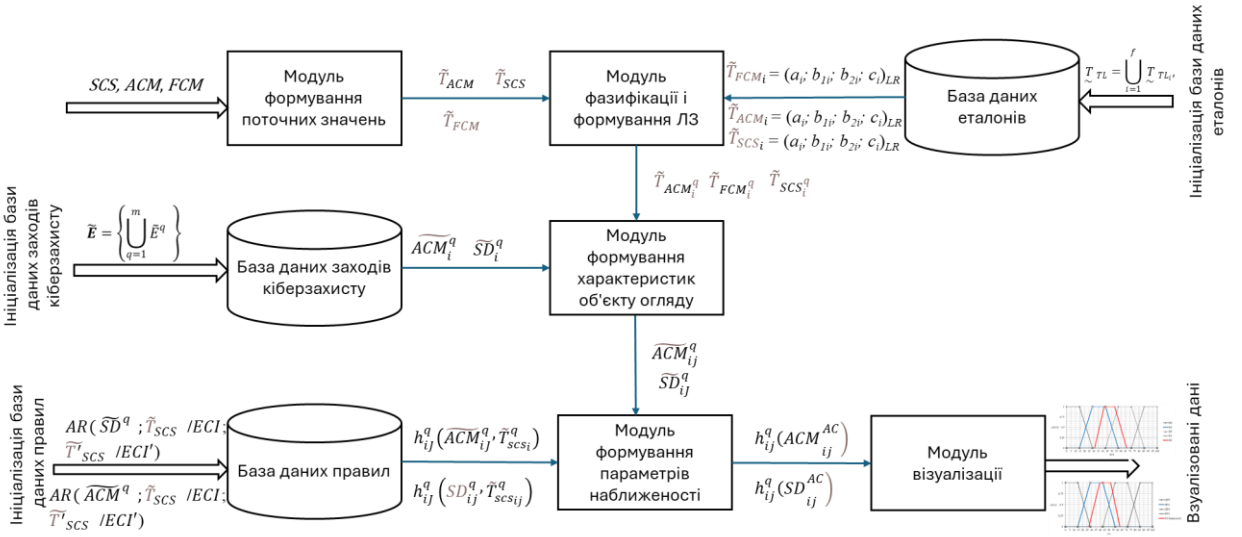

Рис. 1. Структурна модель СМСО

База БДЕ містить множину еталонів:

$$\underset{\sim}{T}_{SCS} = \bigcup_{i=1}^{4} \underset{\sim}{T}_{SCS_i}, = \{\underset{\sim}{T}_{SCS_1}, \underset{\sim}{T}_{SCS_2}, \underset{\sim}{T}_{SCS_3}, \underset{\sim}{T}_{SCS_4}\} =$$
{"ПОЧАТКОВИЙ РІВЕНЬ ЗАХИСТУ",
"ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ",
"ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ",
"РОЗВИНУТИЙ РІВЕНЬ ЗАХИСТУ"},

$$\underset{\sim}{T}_{FCM} = \bigcup_{i=1}^{4} \underset{\sim}{T}_{FCM_i} =$$
$$\{\underset{\sim}{T}_{FCM_1}, \underset{\sim}{T}_{FCM_2}, \underset{\sim}{T}_{FCM_3}, \underset{\sim}{T}_{FCM_4}\} =$$
{"НЕ ПОТРЕБУЄТЬСЯ",
"РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ", "У ПРОЦЕСІ", "РЕАЛІЗОВАНО"},

$$\underset{\sim}{T}_{ACM} = \cup_{i=1}^{4} \underset{\sim}{T}_{ACM_i} =$$
$$\{\underset{\sim}{T}_{ACM_1}, \underset{\sim}{T}_{ACM_2}, \underset{\sim}{T}_{ACM_3}, \underset{\sim}{T}_{ACM_4}\} =$$
{"НЕ ПОТРЕБУЄТЬСЯ", "РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ" "У ПРОЦЕСІ", "РЕАЛІЗОВАНО"},

призначених для формування загального результату оцінювання стану виконання заходів кіберзахисту q-тим об'єктом огляду критичної інфрастуктури [9, 10]. Модуль МФПЗ призначений для формування всіх можливих поточних значень нечітких параметрів:

$$\underset{\sim}{T}_{SCS_i} = \cup_{i=1}^{f} \underset{\sim}{T}_{SCS_i}, \underset{\sim}{T}_{FSM_i} = \cup_{i=1}^{f} \underset{\sim}{T}_{FSM_i}, \underset{\sim}{T}_{ACM_i} =$$
$$\cup_{i=1}^{f} \underset{\sim}{T}_{ACM_i}, (i = \overline{1,f}) - \text{терми НЧ}),$$

що визначається кортежами < ***SCS***, $\underset{\sim}{T}_{SCS}$, X_{SCS}>, < ***FCM***, $\underset{\sim}{T}_{FCM}$, X_{FCM}> та < ***ACM***, $\underset{\sim}{T}_{ACM}$, X_{ACM}> на підставі базової терм-множини ***TL*** за допомогою f термів [4, 10]:

$$\underset{\sim}{T}_{TL} = \bigcup_{i=1}^{f} \underset{\sim}{T}_{TL_i},$$

де для значень $i=\overline{1,f}$ формується свій інтервал, що лежить в межах $X_{TL}=[tl_1; tl_{f+1}]$ та складається з $[tl_1; tl_2[$, …, $[tl_i; tl_{i+1}[$,…, $[tl_n; tl_{f+1}]$.

Модуль МФФЛЗ за допомогою метода [10] реалізує фазифікацію інтервалів $[Xscs_1; Xscs_2[$, …, $[Xscs_i; Xscs_{i+1}[$,…, $[Xscs_f; Xscs_{f+1}]$, $[X_{FSM_1}; X_{FSM_2}[$, $[X_{FSM_i}; X_{FSM_{i+1}}[$,…, $[X_{FSM_f}; X_{FSM_{f+1}}]$ та $[X_{ACM1}; X_{ACM2}[$, …, $[X_{ACMi}; X_{ACMi+1}[$,…, $[X_{ACMf}; X_{ACMf+1}]$ та формування ЛЗ **SCS** – "СТАН КІБЕРЗАХИСТУ", **FCM** – «ВИКОНУВАНІСТЬ ЗАХОДІВ КІБЕРЗАХИСТУ» та **ACM** – "СТАН ЗАХОДІВ КІБЕРЗАХИСТУ".

Модуль МФХОО здійснює еквівалентне перетворення НЧ за допомогою зведення всіх еталонних $\underset{\sim}{T}_{TL}$ та поточних $\tilde{E}^q$ величин до номінального (одного для всіх) числа компонент на основі методу лінійної апроксимації по локальним максимумам.

Модуль МФПН орієнтований на визначення, відповідно до заданої лінгвістичної змінної, ідентифікуючого еталонного терма, за яким із допомогою фазифікованих виразів та отриманих поточних значень характеристик об'єктів огляду ($\underset{\sim}{T}_{SCS_i}$, $\widetilde{SD}_i^q$ та $\widetilde{ACM}_i^q$), можна визначити рівень наближеності поточних значень до еталонних величин h_{ij}^q $(\widetilde{SD}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$ та $h_{ij}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$.

Модуль МВ використовується для графічної інтерпретації результатів оцінювання стану кіберзахисту об'єктів огляду для $\widetilde{SD}_j^q$ ($j=\overline{1,n}$, $q=\overline{1,m}$,) $\widetilde{ACM}_j^q$ ($j=\overline{1,n}$, $q=\overline{1,m}$) та $\widetilde{SD}_{\square}^q$ відносно відносно лінгвістичних еталонів $\underset{\sim}{T}_{TL}$ у вигляді визначеної області, яка характеризує стан системи кіберзахисту, а також відображення умовного виразу у вигляді правила $AR(\widetilde{SD}_{\square}^q; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T'}_{SCS}/ECI')$ та $R(\widetilde{ACM}_{\square}^q; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T'}_{SCS}/ECI')$, відповідно до якого було здійснено оцінювання [10].

Умовно роботу СМСО можна представити двома процесами:

1) процес ініціалізації БД;

2) процес оцінювання стану кіберзахисту.

Процес ініціалізації БД пов'язаний з наповненням (модифікацією) БДЗКЗ, БДП та БДЕ. За необхідністю, на етапі функціонування СМСО, зазначені БД можуть піддаватися модифікації.

Процес оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури SD_i^q здійснюється на підставі структури системи заходів, із розбиттям їх за категоріями і класами заходів кіберзахисту [7-9].

Далі, з БДЕ, БДЗКЗ та МФФЛЗ відповідно НЧ ($\underset{\sim}{T}_{SCS_i}$, $\widetilde{SD}_i^q$ та $\widetilde{ACM}_i^q$) еталонних та поточних даних, надходять в МФХОО, де здійснюється їх номіналізація [6].

У результаті цього, з БДП та МФХОО на вхід МФПН надходять перетворені НЧ $\widetilde{SD}_{ij}^q$ та $\widetilde{ACM}_{ij}^q$ де визначається їх наближеність до еталонних значень. На їх основі отримуємо числові оцінки у вигляді експертних коефіцієнтів параметрів $h_{ij}^q(\widetilde{SD}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$ та $h_{ij}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$ які інтерпретують лінгвістичні параметри і в сукупності відображають поточний стан кіберзахисту об'єктів огляду та його підвищення. Далі на основі підмножини характеристик огляду $\widetilde{ACM}_i^q$ та $\widetilde{SD}_i^q$, а також всіх перетворених $\underset{\sim}{T}_{SCS_i^q}$, $\underset{\sim}{T}_{FCM_i^q}$ та $\underset{\sim}{T}_{ACM_i^q}$, що надійшли з МФФЛЗ та значень $h_{ij}^q(\widetilde{SD}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$ і $h_{ij}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_{ij}}^q)$, які надійшли з МФПН, в МВ здійснюється графічна інтерпретація параметрів, що характеризують стан кіберзахисту [10, 11].

Висновки. Таким чином, запропонована структурна модель, яка за рахунок бази даних заходів кіберзахисту, правил та еталонів, а також модулів формування поточних значень, фазифікації і формування ЛЗ, формування характеристик огляду та параметрів наближеності, дозволяє реалізовувати процес оцінювання підвищення рівня стану кіберзахисту об'єктів критичної інфраструктури в слабоформалізованому нечіткому довкіллі. В подальшому необхідно розробити алгоритмічне та програмне забезпечення, що реалізує запропоновану модель, яка дозволить автоматизувати процес оцінювання підвищення зазначеного стану.

Список літератури

[1]. NIST Cybersecurity Framework // URL https: // www.nist.gov/cybersecurity-measurement.

[2]. ISO/IEC 27001 //URL https://www.assistem.kiev.ua /doc/dstu_ISO-IEC_27001_2015.pdf/.

[3]. Cybersecurity Maturity Model Certification // URL: https://dodcio.defense.gov/CMMC/Model/.

[4]. Корченко О.Г. Системи захисту інформації: Монографія. К.: НАУ, 2004. 264 с.

[5]. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ.: ЦП «Компринт», 2017. 435 с.

[6]. Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія. Київ.: ЦП «Компринт». 2019. 361 с.

[7]. Про затвердження Положення про організаційно-технічну модель кіберзахисту, Постанова від 29 грудня 2021. № 1426. URL https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.

[8]. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426, https://cip.gov.ua / ua / news / naukovo-praktichnii-komentar-do-polozhennya-pro-organiza ciino -tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukra yi ni -vid- 29-grudnya-2021-r-1426.

[9]. Потій О.В., Шульга В.П., Іванченко Є.В., Корченко О.Г., Бакалинський О.О., Мялковський Д.В., Верба Д.В., Зубков Д.А., Юдіна Д.О. Модель системи характеристик даних для оцінювання стану кіберзахисту в Україні, Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України №4 (107), 2023. С. 313-329

[10]. Шульга В.П., Корченко О.Г. Іванченко Є.В., Бакалинський О.О., Мялковський Д.В., Зубков Д.А., Юдіна Д.О. МОДЕЛЬ СИСТЕМИ ХАРАКТЕРИСТИК ДАНИХ ДЛЯ ОЦІНЮВАННЯ ЗАХОДІВ КІБЕРЗАХИСТУ В УКРАЇНІ, Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України №4 (108), 2024. С. 180-196.

[11]. Шульга В.П., Корченко О.Г. Іванченко Є.В., Бакалинський О.О., Мялковський Д.В., Зубков Д.А., Юдіна Д.О. Метод оцінювання стану кіберзахисту

об'єкту огляду критичної інфраструктури держави // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. Житомир: ЖВІ, 2023. Вип. 25 (ІІ). С. 40 - 57.

[12]. Корченко О.Г., Іванченко Є.В., Бакалинський О.О., Мялковський Д.В. Зубков Д.А., Метод оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави // Наукоємні технології.: науковий журнал: НАУ, № 1 (61). 2024. С.3-20.

УДК 004.946.5.056(477)(045)

Korchenko O., Ivanchenko Y. Assessment system for enhancing cybersecurity posture of critical infrastructure inspection objects of the state

Abstract. *In the modern digital world, where a significant portion of our daily activities takes place online, cybersecurity becomes an integral component of national security for every state. Particularly crucial is the protection of critical infrastructure, which ensures the functioning of the economy, communications, and society as a whole. Consequently, the development and implementation of a system for assessing the improvement of cybersecurity posture for critical infrastructure inspection objects become an extremely pressing task for governments and organizations. The proposed structural model of the system for assessing the enhancement of cybersecurity posture for critical infrastructure inspection objects of a state, which utilizes a database of cybersecurity measures, rules and standards, as well as modules for generating current values, phase formation, and formation of LV, formation of inspection characteristics, and proximity parameters, will enable the evaluation of the improvement in the level of cybersecurity posture of critical infrastructure objects in a loosely formalized fuzzy environment. In this context, its implementation becomes a critically important step in ensuring the security of the state's critical infrastructure in the face of constantly increasing cyber threats. It contributes to enhancing readiness and resilience to potential cyber-attacks, which is an indispensable component of national security strategy.*

Keywords: *information security, cybersecurity, information protection, cyber defense, critical infrastructure inspection object, critical infrastructure, cyber threats, cybersecurity posture assessment, fuzzy sets.*

Корченко Олександр Григорович, доктор технічних наук, професор, перший проректор Державного університету інформаційно-комунікаційних технологій, завідувач кафедри Безпеки інформаційних систем і технологій Університету Комісії народної освіти (Краків, Польща), професор кафедри Безпеки інформаційних технологій Національного авіаційного університету, член-кореспондент НАН України, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки.

Oleksandr Korchenko, doctor of technical sciences, professor, first vice-rector of the State University of Information and Communication Technologies, head of the Department of Security of Information Systems and Technologies of the University of the National Education Commission (Krakow, Poland), professor of the Department of Security of Information Technologies of the National Aviation University, member -correspondent of the National Academy of Sciences of Ukraine, Honored Worker of Science and Technology of Ukraine, laureate of the State Prize of Ukraine in the field of science and technology.

Іванченко Євгенія Вікторівна, кандидат технічних наук, професор, лауреат Національної премії України ім. Б. Патона, в.о. завідувача кафедри безпеки інформаційних технологій Національного авіаційного університету.

Eugenia Ivanchenko, candidate of technical sciences, professor, laureate of the National Prize of Ukraine named after B. Paton, acting Head of the Information Technology Security Department of the National Aviation University.

Отримано *23 лютого 2024 року*, затверджено редколегією *1 квітня 2024 року*