КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.829
УДК 004.056.5

Юдіна Діана Олексіївна
аспірант факультету комп'ютерних наук та технологій
Державний університет "Київський авіаційний інститут", Київ, Україна
ORCID ID: 0000-0002-1277-8771
diana.yudina22@gmail.com

МОДЕЛЬ РОЗРАХУНКУ РІВНЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Зростання кількості кібератак на об'єкти критичної інфраструктури в Україні є сталою тенденцією, що обумовлює необхідність системного вдосконалення підходів до забезпечення кібербезпеки. Особливої актуальності набуває питання підвищення рівня захищеності інформаційно-комунікаційних систем та інформаційних ресурсів об'єктів критичної інформаційної інфраструктури. Незважаючи на наявність у законодавстві України визначених механізмів оцінки стану кіберзахисту таких об'єктів, їх практичне впровадження залишається складним та ресурсозатратним. У багатьох випадках власники об'єктів критичної інфраструктури та оператори критичної інфраструктури не мають достатніх можливостей для ефективної реалізації встановлених вимог, що зумовлює потребу у розробці більш доступних та адаптивних моделей оцінювання. На сучасному етапі в Україні процес ідентифікації та захисту об'єктів критичної інфраструктури перебуває на початковому рівні, що створює ризики для національної безпеки та функціонування важливих суспільних систем. У статті запропоновано модель розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури, яка передбачає можливість розширення системи характеристик шляхом застосування теоретико-множинного підходу. Здійснено формалізацію підмножин критеріїв (класів заходів кіберзахисту) та відповідної системи параметрів, що дозволяє проводити кількісну оцінку рівня захищеності об'єкта. Запропонована модель має потенціал для практичного використання як інструмент моніторингу та підвищення ефективності заходів кіберзахисту. У подальших дослідженнях планується використати запропоновану модель для розробки методу підвищення рівня кіберзахисту.

Ключові слова: кіберзахист; критична інфраструктура; об'єкти критичної інфраструктури; заходи кіберзахисту; оцінювання стану кіберзахисту критичної інфраструктури.

ВСТУП

Одним з основних чинників, що створює небезпеку об'єктам критичної інфраструктури (ОКІ) є кіберзагрози та кібератаки. Російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, що ґрунтується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів критичної інформаційної інфраструктури. За друге півріччя 2024 року Державним центром кіберзахисту Держспецзв'язку було зафіксовано та зареєстровано на 48 % більше кіберінцидентів ніж за перше півріччя 2024 року [1]. Від початку 2023 року Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, фіксувала зростання кількості атак з метою шпигунства з акцентом на утриманні постійного доступу до організації [2]. Зокрема, такі кібератаки спрямовані на ОКІ, як державного, так і приватного секторів. Таким чином, спостерігається тенденція до

© Д.О. Юдіна, 2025

зростання кількості кіберінцидентів на ОКІ, що зумовлює необхідність покращення стану кібербезпеки, підвищення захищеності інформаційних ресурсів та інформаційно-комунікаційних систем ОКІ, в особливості об'єктів критичної інформаційної інфраструктури [3], [4]. Одним з шляхів покращення стану кібербезпеки є розробка моделі розрахунку рівня кіберзахисту ОКІ. Така модель забезпечить об'єктивну оцінку дієвості впроваджених заходів кібербезпеки.

Постановка проблеми. Робота щодо ідентифікації ОКІ в Україні розпочалась у 2020 році, проте поштовхом до прискорення цієї діяльності стало повномасштабне вторгнення рф на територію України. ОКІ, особливо паливно-енергетичного сектору, стали першочерговими мішенями хакерів, що створює потребу в постійному оцінюванні та підтримці високого рівня кіберзахисту. Порушення роботи ОКІ може призвести до великих фінансових та іміджевих втрат, порушення соціального порядку, втрати довіри громадськості тощо. Оскільки критична інфраструктура включає енергетичні системи, транспорт, банківську сферу, системи охорони здоров'я та інші життєво важливі сектори, то збій або втрата їх функціональності може мати серйозні наслідки для економіки та безпеки держави. У зв'язку з тим, що напрямок захисту критичної інфраструктури є новим для України, а також враховуючи, що законодавство у сфері кібербезпеки постійно змінюється, вимагаючи від організацій впроваджувати нові норми та стандарти, то оцінювання стану кіберзахисту допоможе операторам критичної інфраструктури визначити власний поточний стан кіберзахисту та сформувати напрямки щодо покращення кіберзахисту своїх об'єктів критичної інформаційної інфраструктури.

Актуальність питання оцінювання стану кіберзахисту ОКІ держави обумовлена низкою важливих чинників, таких як зростання кіберзагроз, важливість для національної безпеки, соціально-економічний вплив, регулювання законодавства та відповідність новим нормам і стандартам у сфері кібербезпеки, технологічний фактор (наприклад, ідентифікація потенційних уразливостей в нових технологічних рішеннях) тощо. Пропоновані державою механізми підвищення рівня кіберзахисту є ресурсомісткими як у фінансовому, так і у часовому вимірах. Щоденне збільшення кількості кібератак на критичну інфраструктуру України не дозволяє операторам критичної інфраструктури виконувати у повному обсязі затверджені вимоги до кіберзахисту. Таким чином, необхідно визначити першочергові ключові заходи кіберзахисту, що допоможуть захистити об'єкти критичної інформаційної інфраструктури з можливістю подальшого розширення заходів до визначених законодавством. Враховуючи ці чинники можемо констатувати, що важливість оцінювання стану кіберзахисту ОКІ є важливим елементом стратегії національної безпеки та економічної стабільності будь-якої держави.

Зазначені твердження свідчать про наявність важливого наукового завдання щодо аналізу існуючих досліджень у галузі кіберзахисту об'єктів критичної інформаційної інфраструктури та розробки моделі розрахунку рівня кіберзахисту ОКІ.

Аналіз останніх досліджень і публікацій. Для покращення стану кібербезпеки та підвищення рівня захищеності об'єктів критичної інформаційної інфраструктури необхідно визначити найбільш дієвий механізм підвищення рівня кіберзахисту ОКІ. З цією метою були розглянуті основні нормативні та рекомендаційні міжнародні і вітчизняні документи в галузі кіберзахисту, а також проведено їх порівняльний аналіз.

Перш за все звернемо увагу на законодавчу та нормативно-правову базу у сфері кібербезпеки та кіберзахисту України. Зокрема, було проаналізовано нормативно-правові акти українського законодавства щодо кібербезпеки та кіберзахисту [5] – [9].

Відповідно до Закону України [7], кіберзахист — це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного

захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Для досягнення певного стану кібербезпеки мають бути виконані дії з кіберзахисту (впроваджені заходи кіберзахисту).

Для кіберзахисту ОКІ законодавством України визначено певні конкретні механізми, а саме Загальні вимоги до кіберзахисту ОКІ, викладені в постанові Кабінету Міністрів України [8] та Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної структури (далі — Методичні рекомендації), затверджених наказом Адміністрації Держспецзв'язку [9].

Отже, державою запропоновано механізми підвищення рівня кіберзахисту ОКІ. Провівши детальний аналіз кожного з перелічених документів виявлено наступне.

В постанові Кабінету Міністрів України [8] окреслено основні вимоги, що мають бути виконані власником та/або керівником ОКІ, проте не надано практичних рекомендацій щодо виконання таких вимог, а також акцентовано увагу на необхідності створення комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю. Постанова Кабінету Міністрів України [8] передбачає виконання 53 вимог до кіберзахисту, які є загальними та включають по декілька завдань із кіберзахисту.

Водночас наказом Адміністрації Держспецзв'язку [9] надано вичерпні рекомендації щодо виконання вимог до кіберзахисту ОКІ, шляхом реалізації 108 заходів кіберзахисту. Методичні рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity, CSF) [10], виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology). Вони базуються на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. В наказі Адміністрації Держспецзв'язку [9] та CSF [10] визначено 108 заходів кіберзахисту, що згруповані у п'ять класів заходів кіберзахисту — Ідентифікація ризиків кібербезпеки, Кіберзахист, Виявлення кіберінцидентів, Реагування на кіберінциденти та Відновлення стану кібербезпеки [11], [12].

[9] та [10] також визначають етапи впровадження заходів кіберзахисту: розробка поточного профілю кіберзахисту, проведення оцінки ризиків, створення цільового профілю кіберзахисту, визначення, аналіз та пріоритезація недоліків (шляхом порівняння цільового та поточного профілів кіберзахисту) та реалізація плану удосконалення заходів кіберзахисту.

Разом з тим, на початку 2024 року CSF [10] було оновлено, додано додатковий, шостий клас заходів кіберзахисту (Управління) та визначено 106 заходів кіберзахисту [13].

Водночас, враховуючи що в Україні наразі робота з ідентифікації та захисту ОКІ перебуває на початковому рівні, власникам ОКІ та операторам критичної інфраструктури для впровадження запропонованих 108 заходів кіберзахисту (що не є вичерпними, а також потребують доповнення секторальними заходами кіберзахисту), розроблення поточного та цільового профілів кіберзахисту, розроблення плану з подолання недоліків необхідно задіяти значні ресурси, зокрема часові. Для прискорення цієї роботи, за умови, що агресія російської федерації в кіберпросторі збільшується, необхідно визначити першочергові чіткі та зрозумілі вимоги для підвищення рівня кіберзахисту ОКІ. Такі вимоги також мають враховувати нормативно встановлені

вимоги до кіберзахисту ОКІ, що визначені постановою Кабінету Міністрів України [8] та наказом Адміністрації Держспецзв'язку [9].

Враховуючи ці показники автором було обрано Міжгалузеві цілі ефективності кібербезпеки (Cross-Sector Cybersecurity Performance Goals, Version: 1.0.1, March 2023 Update, CPGs) [14], розроблені Агенцією з кібербезпеки і захисту інфраструктури Сполучених Штатів Америки (Cybersecurity and Infrastructure Security Agency, CISA).

Міжгалузеві цілі [14] є загальним набором засобів захисту, що є застосовними для всіх суб'єктів критичної інфраструктури, незалежно від приналежності до сектору критичної інфраструктури, форми власності (державна, приватна), розміру чи охоплення (великий, середній або малий бізнес). Міжгалузеві цілі [14] розроблені в результаті консультацій з представниками критичної інфраструктури США, уряду та експертами та організовані відповідно до Настанови [10].

Найбільш зручним в застосуванні Міжгалузевих цілей [14] є запропоновані CISA чек-лист та матриця з додатковою інформацію та референційними посиланнями.

Міжгалузеві цілі [14] мають 38 цілей, що згруповані у 5 великих цілей (аналогічно до [8, 10]), а також рекомендовані дії для виконання тієї чи іншої цілі.

Таким чином, Міжгалузеві цілі [14] є релевантною аналогією постанови Кабінету Міністрів України [8] та CSF [10], проте також мають перевагу над цими нормативними документами за кількістю заходів, які повинні бути впроваджені на ОКІ для першочергового кіберзахисту, зрозумілістю та простотою у використанні, а також за наявним чітким визначеним переліком рекомендованих дій для кожного заходу.

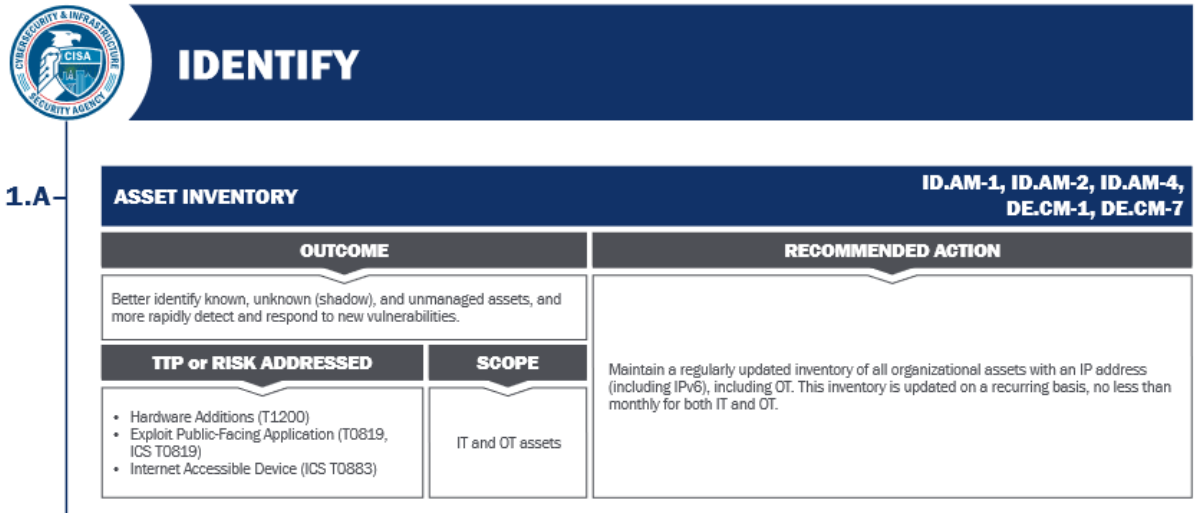

Рис. 1. Приклад моделі CPGs

Модель CPGs, приклад якої зображено на рис. 1, складається з певних компонентів: результат (outcome) – кінцевий результат, що має бути досягнуто після виконанні цілі; ТТР або ризик, на який спрямована ціль (TTP or risk addressed) — набір тактик, технік та процедур (tactics, techniques and procedures) або набір організаційних ризиків, які стануть менш імовірними у разі реалізації цілі; практики захисту (Security practice) — заходи з пом'якшення, що мають бути впроваджені ОКІ для зменшення впливу ТТР або ризиків; сфера застосування (Scope) — набір активів, до яких застосовна ціль; рекомендовані дії (Recommended action) — приклади підходів, які допоможуть ОКІ досягти цілі.

Механізм оцінювання стану кіберзахисту критичної інфраструктури, що представлений у чек-листі CPGs полягає у наступних кроках:

- проведення первинного самооцінювання. Цей крок необхідний для оцінювання кожної з 38 цілей станом на поточний момент для перегляду існуючих правил та політик кіберзахисту на ОКІ;
- ідентифікація прогалин та визначення пріоритетів. Цей крок має на меті допомогти ОКІ визначити пріоритетні напрямки для інвестування у кіберзахист на основі факторів вартості, складності та впливу на ОКІ;
- інвестування та виконання. На даному кроці ОКІ пропонується розпочати роботу над усуненням пріоритезованих прогалин;
- регулярний перегляд. ОКІ рекомендується переглядати та відстежувати прогрес у досягненні цілей з кіберзахисту кожні 12 місяців.

Проведення первинного самооцінювання та регулярний перегляд відбувається шляхом відношення цілі до однієї з чотирьох оцінок: «Впроваджено», «В процесі», «Розглядається» та «Не розпочато». Також кожну ціль можна додати власними нотатками, до яких рекомендується додавати назви та номери документів, якими на ОКІ затверджено ті чи інші політики.

У табл. 1 систематизовано результати проведеного аналізу популярних існуючих вимог та рекомендацій щодо підвищення рівня кіберзахисту критичної інфраструктури за такими критеріями:

Дескриптивність (ДС) — описовий характер без встановлення конкретних вимог або норм.

Гнучкість (ГН) — здатність адаптувати або змінювати правила, вимоги чи рекомендації відповідно до конкретних умов, ситуацій або потреб.

Можливість інтеграції з іншими стандартами та настановами (ІН).

Простота реалізації у співвідношенні затребуваного часу та кількості ресурсів для виконання конкретних вимог (ПР).

Юрисдикційна релевантність (ЮР) — ступінь відповідності документа чинному законодавству України, національній термінології, структурі органів управління та контексту критичної інформаційної інфраструктури.

Кількість заходів кіберзахисту, необхідних для впровадження (КЗ) (де 1 — найбільша кількість заходів, а 4 — найменша кількість заходів).

Таблиця 1

Порівняльний аналіз вимог та рекомендацій щодо підвищення рівня кіберзахисту ОКІ

№ з/п	Вимоги / рекомендації з підвищення рівня кіберзахисту	ДС	ГН	ІН	ПР	ЮР	КЗ
1	Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»	-	-	-	-	+	3
2	Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року № 601	+	+	+	-	+	1
3	CISA Cybersecurity Performance Goals	+	+	+	+	-	4
4	Настанова для підвищення кібербезпеки критичної інфраструктури	+	+	+	-	+	2

Таким чином, з табл. 1 видно, що найбільш придатними за усіма критеріями є Міжгалузеві цілі [14], оскільки вони є прийнятним, інтуїтивно зрозумілим та простим інструментом для проведення первинного оцінювання стану кіберзахисту на ОКІ. Проте, враховуючи, що Міжгалузеві цілі [14] розроблені представниками критичної інфраструктури, уряду та експертами США та його терміни, принципи й підходи не враховують специфіку українського контексту, вони не можуть бути цілком і повністю застосовні на ОКІ України. У разі застосування на ОКІ України перелік цілей необхідно доповнити додатковими цілями з кіберзахисту, що будуть включати національну та секторальну складові, а також внести корективи безпосередньо у механізм оцінювання стану кіберзахисту.

Метою статті є розроблення моделі розрахунку рівня кіберзахисту ОКІ із можливістю розширення системи характеристик на основі Міжгалузевих цілей [14].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Модель розрахунку рівня кіберзахисту ОКІ реалізується в наступних етапах:

Етап 1. Визначення множини системи критеріїв, яка охоплює групи заходів із кіберзахисту *(SC).*

Етап 2. Визначення підмножини параметрів кожної групи заходів із кіберзахисту *(SCi).*

Етап 3. Формування деталізованих заходів із кіберзахисту у вигляді показників параметрів.

Етап 4. Введення кількісних характеристик для формалізації результату.

Етап 5. Визначення рівня кіберзахисту ОКІ у вигляді кількісного показника.

Запропонована модель розрахунку рівня кіберзахисту ОКІ дозволяє розрахувати рівень кіберзахисту ОКІ у вигляді кількісного показника, більш детально та об’єктивно, в порівнянні з [14], сформувати параметри та їх показники, врахувавши секторальні/галузеві особливості ОКІ.

Етап 1. Визначення множини системи критеріїв, яка охоплює групи заходів із кіберзахисту *(SC).*

Для формалізації процесу побудови моделі розрахунку рівня кіберзахисту ОКІ застосуємо теоретико-множинний підхід. Для цього введемо множину системи критеріїв, яка охоплює групи заходів із кіберзахисту, і відобразимо її як:

$$SC = \{\cup_{i=1}^{n} SC_i\} = \{SC_1, SC_2, \dots, SC_n\}, \quad (1)$$

де $SC_i \subseteq SC(i = \overline{1,n})$ — ідентифікатор відповідного критерію (класу заходів кіберзахисту).

Наприклад, при $n = 5$ вираз (1) запишемо як:

$$SC = \{\cup_{i=1}^{n} SC_i\} = \{SC_1, SC_2, SC_3, SC_4, SC_5\} = \{ID, PR, DE, RS, RC\},$$

де $SC_1 = ID$ = *«Ідентифікація ризиків кібербезпеки»*, $SC_2 = PR$ = *«Кіберзахист»*, $SC_3 = DE$ = *«Виявлення кіберінцидентів»*, $SC_4 = RS$ = *«Реагування на кіберінцидентим»*, $SC_5 = RC$ = *«Відновлення стану кібербезпеки»*.

Етап 2. Визначення підмножини параметрів кожної групи заходів із кіберзахисту *(SCi).*

Кожний з зазначених класів заходів кіберзахисту характеризується підмножиною параметрів:

$$SC_i = \left\{\cup_{j=1}^{k_i} SC_{ij}\right\} = \{SC_{i1}, SC_{i2}, \dots, SC_{ik_i}\}, \quad (2)$$

де $SC_i \subseteq SC_{ij}\left(j = \overline{1,k_j}\right)$ — підмножина параметрів *i*-го класу заходів кіберзахисту.

З урахуванням (2) вираз (1) запишемо як:

$$SC = \left\{\cup_{i=1}^{n}\left\{\cup_{j=1}^{k_i} SC_{ij}\right\}\right\} = \left\{\{SC_{11}, SC_{12} \dots SC_{1k_1}\}, \{SC_{21}, SC_{22} \dots SC_{2k_2}\} \dots \{SC_{i1}, SC_{i2} \dots SC_{ik_n}\}\right\}, \quad (3)$$

Етап 3. Формування деталізованих заходів із кіберзахисту у вигляді показників параметрів.

Наприклад, з урахуванням табл. 2 при $n = 5$, $k_1 = 8$, $k_2 = 24$, $k_3 = 1$, $k_4 = 3$, $k_5 = 1$ вираз (3) запишемо як:

$$SC = \left\{\bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{k_i} SC_{ij}\right\}\right\}$$

$$= \{\{SC_{11}, SC_{12} \dots SC_{18}\}, \{SC_{21}, SC_{22} \dots SC_{224}\}, \{SC_{31}\}\{SC_{41}, SC_{42}, SC_{43}\}\{SC_{51}\}\}$$

$$= \left\{\begin{array}{c} \{ID_1, ID_2, ID_3, ID_4, ID_5, ID_6, ID_7, ID_8\}, \\ \{PR_1, PR_2, PR_3, PR_4, PR_5, PR_6, PR_7, PR_8, PR_9, PR_{10}, PR_{11}, PR_{12}, \\ PR_{13}, PR_{14}, PR_{15}, PR_{16}, PR_{17}, PR_{18}, PR_{19}, PR_{20}, PR_{21}, PR_{22}, PR_{23}, PR_{24}\}, \\ \{DE_1\}, \\ \{RS_1, RS_2, RS_3\}, \\ \{RC_1\} \end{array}\right\}$$

де, наприклад, *SC_{27}=PR_7=ZVS= «Чи забезпечено виявлення невдалих спроб входу в систему»; SC_{42}= RS_2=ZVR =«Чи забезпечено використання результатів досліджень щодо вразливостей»*.

Таблиця 2

Система базових чинників розрахунку рівня кіберзахисту

№ з/п	Групи чинників (критеріїв) *SC*	Параметри	Показники параметрів	Кількісна характеристика показників параметрів
1	SC_1 = *ID* = *«Ідентифікація ризиків кібербезпеки»*	*ID_1 = PIA*	Чи проведена інвентаризація активів?	Так – 1 Ні – 0
		ID_2 = PPO	Чи призначена керівна посадова особа, відповідальна за кібербезпеку на всьому ОКІ?	Так – 1 Ні – 0
		ID_3 = ZNV	Чи забезпечена належна взаємодія підрозділів ІТ та кіберзахисту?	Так – 1 Ні – 0
		ID_4 = OVV	Чи опрацьовано вплив відомих вразливостей?	Так – 1 Ні – 0
		ID_5 = ZSO	Чи залучена стороння організація для проведення незалежного аудиту інформаційної безпеки?	Так – 1 Ні – 0
		ID_6 = ZRSI	Чи забезпечено реагування на інформування постачальниками про визначені ними інциденти?	Так – 1 Ні – 0
		ID_7 = ZRSV	Чи забезпечено реагування на інформування постачальниками про виявлені ними вразливості?	Так – 1 Ні – 0
		ID_8 = ZVK	Чи затверджені вимоги щодо кібербезпеки до постачальників ІКТ або послуг?	Так – 1 Ні – 0
2	SC_2 = *PR* = *«Кіберзахист»*	*PR_1 = PZP*	Чи проведена зміна паролів, встановлених за замовчуванням?	Так – 1 Ні – 0

		PR_2 = *ZVN*	Чи забезпечено використання надійних паролів?	Так – 1 Ні – 0
		PR_3 = *ZUD*	Чи забезпечено унікальність облікових даних?	Так – 1 Ні – 0
		PR_4 = *ZPV*	Чи затверджена процедура вчасного видалення облікових даних звільнених працівників?	Так – 1 Ні – 0
		PR_5 = *UOP*	Чи унеможливлено отримання зловмисником прав доступу до привілейованих облікових даних адміністраторів або користувачів?	Так – 1 Ні – 0
		PR_6 = *PSM*	Чи проведена сегментація мережі?	Так – 1 Ні – 0
		PR_7 = *ZVS*	Чи забезпечено виявлення невдалих спроб входу в систему?	Так – 1 Ні – 0
		PR_8 = *VSP*	Чи впроваджена стійка до фішингу багатофакторна автентифікація?	Так – 1 Ні – 0
		PR_9 = *ZBN*	Чи запроваджено базове навчання з кібербезпеки для всіх співробітників?	Так – 1 Ні – 0
		PR_{10} = *ZDN*	Чи запроваджено додаткове навчання з кібербезпеки для персоналу підрозділу кіберзахисту?	Так – 1 Ні – 0
		PR_{11} = *ZSOI*	Чи забезпечено шифрування при обміні інформацією про активи між підрозділами ІТ та кіберзахисту?	Так – 1 Ні – 0
		PR_{12} = *ZZI*	Чи забезпечено захист інформації з обмеженим доступом?	Так – 1 Ні – 0
		PR_{13} = *ZZE*	Чи забезпечена захищеність електронної пошти від спуфінгу, фішингу та перехоплення повідомлень?	Так – 1 Ні – 0
		PR_{14}=*VVZ*	Чи вимкнені встановлені за замовчуванням макроси та інший програмний код?	Так – 1 Ні – 0
		PR_{15}=*ZDC*	Чи забезпечено документування конфігураційних файлів ІКТ, що обробляють активи?	Так – 1 Ні – 0
		PR_{16}=*ZDS*	Чи забезпечено документування схеми розміщення та з'єднання обладнання мереж?	Так – 1 Ні – 0
		PR_{17}=*ZPI*	Чи затверджені процедури інсталяції ІКТ?	Так – 1 Ні – 0
		PR_{18}=*ZRS*	Чи забезпечено регулярне створення резервних копій конфігураційних файлів?	Так – 1 Ні – 0
		PR_{19}=*ZTV*	Чи затверджено, регулярно тестуються та вносяться зміни до планів реагування на кіберінциденти?	Так – 1 Ні – 0
		PR_{20}=*ZZZ*	Чи забезпечено збір журналів подій?	Так – 1 Ні – 0
		PR_{21}=*ZBZ*	Чи забезпечено безпечне зберігання журналів подій?	Так – 1 Ні – 0

		PR_{22}=*ZZP*	Чи забезпечено заборону підключення неавторизованих пристроїв?	Так – 1 Ні – 0
		PR_{23}=*ZVOI*	Чи забезпечено виявлення та обмеження використання Інтернет-послуг?	Так – 1 Ні – 0
		PR_{24}=*ZOP*	Чи забезпечено обмеження підключення ОКІІ до мережі Інтернет?	Так – 1 Ні – 0
3	SC_3 = *DE* = *«Виявлення кіберінцидентів»*	DE_1=*VPP*	Чи визначено порядок проведення моніторингу загроз та застосування відповідних тактик, технік і процедур?	Так – 1 Ні – 0
4	SC_4 = *RS* = *«Реагування на кіберінциденти»*	RS_1=*ZIK*	Чи забезпечено інформування про кіберінциденти?	Так – 1 Ні – 0
		RS_2=*ZVR*	Чи забезпечено використання результатів досліджень щодо вразливостей?	Так – 1 Ні – 0
		RS_3=*ZRF*	Чи забезпечено розміщення файлів security.txt та опрацювання отриманої завдяки їм інформації?	Так – 1 Ні – 0
5	SC_5 = *RC* = *«Відновлення стану кібербезпеки»*	RC_1=*ZPVI*	Чи затверджені плани відновлення після інцидентів?	Так – 1 Ні – 0

Етап 4. Введення кількісних характеристик для формалізації результату.

Таким чином, виконавши дії, вказані у виразі (3) рівень кіберзахисту ОКІ буде розраховано. Проте, результат підвищення рівня кіберзахисту ОКІ має бути формалізованим. Для цього пропонується розрахувати рівень кіберзахисту ОКІ, шляхом введення кількісних характеристик: Так — «1», Ні — «0».

Етап 5. Визначення рівня кіберзахисту ОКІ у вигляді кількісного показника.

Для визначення рівня кіберзахисту ОКІ визначимо середнє арифметичне за кожним із класів заходів кіберзахисту. Для цього визначимо середнє арифметичне критеріїв (класів заходів кіберзахисту):

$$SA_{SC} = \frac{\sum_{i=1}^{n} \mathrm{SA_{SC_i}}}{n}, \quad (4)$$

Визначення середнього арифметичного в кожному класі заходів кіберзахисту:

$$\mathrm{SA_{SC_i}} = \frac{\sum_{j=1}^{k} \mathrm{SC_{ij}}}{k}, \quad (5)$$

З урахуванням (5) вираз (4) запишемо як:

$$SA_{SC} = \frac{\sum_{i=1}^{n} \mathrm{SA_{SC_i}}}{n} = \frac{\sum_{i=1}^{n} \frac{\sum_{j=1}^{k} \mathrm{SC_{ij}}}{k}}{n}, \quad (6)$$

При $n = 5$ та з урахуванням системи чинників вираз (6) запишемо як:

$$SA_{SC} = \frac{\sum_{i=1}^{5} \frac{\sum_{j=1}^{k} \mathrm{SC_{ij}}}{k}}{5} = \frac{SA_{SC_1}+SA_{SC_2}+SA_{SC_3}+SA_{SC_4}+SA_{SC_5}}{5}, \quad (7)$$

Наприклад, з урахуванням табл. 2, при $n=5$, $k_1=8$, $k_2=24$, $k_3=1$, $k_4=3$, $k_5=1$ вираз (7) запишемо як:

$$SA_{SC} = \frac{\frac{ID_1+ID_2+\cdots+ID_8}{8}+\frac{PR_1+PR_2+\cdots+PR_{24}}{24}+\frac{DE_1}{1}+\frac{RS_1+RS_2+\mathrm{RS_3}}{3}+\frac{RC_1}{1}}{5}$$

Загальну структуру розробленої узагальненої моделі (з урахуванням наведених прикладів) представлено на рис. 2.

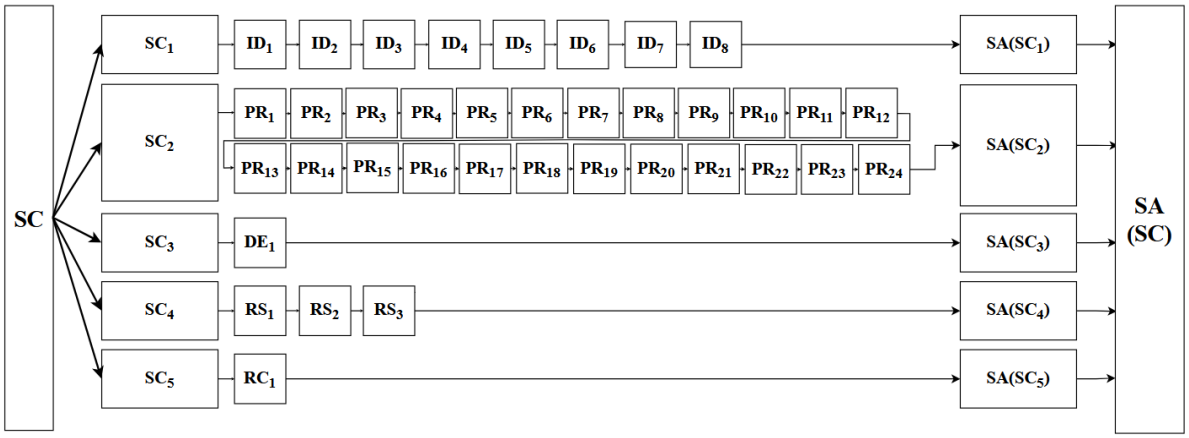

Рис. 2. Модель розрахунку рівня кіберзахисту ОКІ

Модель охоплює множинну систему характеристик (класів заходів кіберзахисту), які в свою чергу охоплюють групи критеріїв (безпосередньо заходів кіберзахисту). За умови реалізації всіх заходів кіберзахисту, що визначені як першочергові, рівень кіберзахисту ОКІ буде підвищено, що дозволить на основі вже існуючих (впроваджених) заходів кіберзахисту запроваджувати інші заходи кіберзахисту вищої складності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті було проаналізовано поточний стан законодавства у сфері кіберзахисту ОКІ, що дало можливість визначити певні недоліки в процесі підвищення рівня кіберзахисту ОКІ, відповідно до поточного стану розвитку ОКІ. Встановлено, що існуючі встановлені вимоги щодо кіберзахисту для ОКІ України є складними для впровадження, зокрема з урахуванням часових обмежень, що спричинені агресією російської федерації в кіберпросторі. Запропоновано альтернативний оптимальний підхід, що визначає першочергові чіткі та зрозумілі вимоги для підвищення рівня кіберзахисту ОКІ (Міжгалузеві цілі ефективності кібербезпеки), який потребує доопрацювання, зокрема щодо розширення переліку цілей з урахуванням національної та секторальної складових. На основі визначеного підходу запропоновано модель розрахунку рівня кіберзахисту ОКІ, що містить множинну систему характеристик (класів заходів кіберзахисту), яка охоплює групи критеріїв (заходів кіберзахисту) для підвищення рівня кіберзахисту ОКІ. Продовженням дослідження стане проведення експерименту та верифікація запропонованої моделі розрахунку рівня кіберзахисту ОКІ. Крім того, в подальшому, планується використання даної моделі для розробки методу підвищення рівня кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine. (2024). *Russian cyber operations. H2 '2024*. https://cip.gov.ua/services/cm/api/attachment/download?id=68769
2. State Service of Special Communications and Information Protection of Ukraine. (2024). *Cyberattacks on Ukraine: Russia is trying to gain any information for an advantage in conventional warfare*. https://cip.gov.ua/ua/news/kiberataki-na-ukrayinu-za-dopomogoyu-khakeriv-rosiya-namagayetsya-otrimati-bud-yaku-informaciyu-yaka-mozhe-dati-yii-perevagu-v-konvenciinii-viini

3. Gnatyuk, S., Sydorenko, V., & Polozhentsev, A. (2023). Method for cybersecurity level evaluation in the civil aviation critical infrastructure. *Proceedings of the International Workshop on Advances in Civil Aviation Systems Development (ACASD 2023)*, 736, 203–214). https://doi.org/10.1007/978-3-031-38082-2_16
4. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sotnichenko, Y. (2020). Experimental cybersecurity level determination in the civil aviation critical infrastructure. *In 2020 International Conference on Problems of Infocommunications Science and Technology (PIC S&T),* 757–764. IEEE. https://doi.org/10.1109/PICST51311.2020.9467987
5. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2025) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. On the Protection of Information in Information and Telecommunication Systems, Law of Ukraine No. 80/94-VR (1994) (Ukraine).
7. On the Basic Principles of Cybersecurity in Ukraine, Law of Ukraine No. 2163-VIII. (2017) (Ukraine)
8. On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities, Resolution No. 518 (2019) (Ukraine).
9. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2021). *Methodological recommendations on improving the level of cybersecurity of critical information infrastructure* (Order No. 601 dated October 6, 2021). https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
10. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework*. https://www.nist.gov/cyberframework
11. Yudina, D. O. (2023). Cybersecurity measures for critical information infrastructure facilities against cyber threats and cyber attacks. *In Challenges and Threats to Critical Infrastructure*, 89–93. Detroit, MI: NGO Institute for Cyberspace Research.
12. Yudina, D. O., Shulha, V. P., Khorchenko, O. H., Ivanchenko, Y. V., Bakalynskyi, O. O., Myalkovskyi, D. V., & Zubkov, D. A. (2023). Method for assessing the cybersecurity state of a critical infrastructure facility under review. *Problems of Creation, Testing, Application, and Operation of Complex Information Systems: Collection of Scientific Papers of ZhVI, 25(II)*, 40–57.
13. Zhylin, A., Beliavsky, V., & Bakalynsky, O. (2024). NIST CSF 2.0: New cybersecurity framework from the National Institute of Standards and Technology of the United States. *Ukrainian Scientific Journal of Information Security, 30(1),* 73–76.
14. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals*. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Yudina Diana
PhD student of the Faculty of Computer Science and Technology
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-1277-8771
diana.yudina22@gmail.com

MODEL FOR CALCULATING THE LEVEL OF CYBER SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The growing number of cyberattacks on critical infrastructure facilities in Ukraine is a steady trend that necessitates systematic improvement of approaches to cybersecurity. The issue of improving the security of information and communication systems and information resources of critical information infrastructure facilities is of particular relevance. Despite the existence of certain mechanisms in Ukrainian legislation for assessing the state of cybersecurity of such facilities, their practical implementation remains difficult and resource-intensive. In many cases, critical infrastructure owners and operators do not have sufficient capacity to effectively implement the established requirements, which necessitates the development of more accessible and adaptive assessment models. At the current stage in Ukraine, the process of identification and protection of critical infrastructure is at an initial level, which creates risks for national security and the functioning of important social systems. The article proposes a model for calculating the level of cybersecurity of critical information infrastructure facilities, which provides for the possibility of expanding the system of characteristics by applying a set-theoretic approach. The formalization of subsets of criteria (classes of cybersecurity measures) and the corresponding system of parameters is carried out, which allows for a quantitative assessment of the level of security of the object. The proposed model has the potential for practical use as a tool for monitoring and improving the effectiveness of cybersecurity measures. In further research, it is planned to use the proposed model to develop a method for improving the level of cybersecurity.

Keywords: cybersecurity; critical infrastructure; critical infrastructure facilities; cybersecurity measures; assessment of the state of cybersecurity of critical infrastructure.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine. (2024). *Russian cyber operations. H2 '2024*. https://cip.gov.ua/services/cm/api/attachment/download?id=68769
2. State Service of Special Communications and Information Protection of Ukraine. (2024). *Cyberattacks on Ukraine: Russia is trying to gain any information for an advantage in conventional warfare*. https://cip.gov.ua/ua/news/kiberataki-na-ukrayinu-za-dopomogoyu-khakeriv-rosiya-namagayetsya-otrimati-bud-yaku-informaciyu-yaka-mozhe-dati-yii-perevagu-v-konvenciinii-viini
3. Gnatyuk, S., Sydorenko, V., & Polozhentsev, A. (2023). Method for cybersecurity level evaluation in the civil aviation critical infrastructure. *Proceedings of the International Workshop on Advances in Civil Aviation Systems Development (ACASD 2023)*, 736, 203–214). https://doi.org/10.1007/978-3-031-38082-2_16
4. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sotnichenko, Y. (2020). Experimental cybersecurity level determination in the civil aviation critical infrastructure. *In 2020 International Conference on Problems of Infocommunications Science and Technology (PIC S&T)*, 757–764. IEEE. https://doi.org/10.1109/PICST51311.2020.9467987
5. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2025) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. On the Protection of Information in Information and Telecommunication Systems, Law of Ukraine No. 80/94-VR (1994) (Ukraine).
7. On the Basic Principles of Cybersecurity in Ukraine, Law of Ukraine No. 2163-VIII. (2017) (Ukraine)
8. On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities, Resolution No. 518 (2019) (Ukraine).

9. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2021). *Methodological recommendations on improving the level of cybersecurity of critical information infrastructure* (Order No. 601 dated October 6, 2021). https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601
10. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework*. https://www.nist.gov/cyberframework
11. Yudina, D. O. (2023). Cybersecurity measures for critical information infrastructure facilities against cyber threats and cyber attacks. *In Challenges and Threats to Critical Infrastructure*, 89–93. Detroit, MI: NGO Institute for Cyberspace Research.
12. Yudina, D. O., Shulha, V. P., Khorchenko, O. H., Ivanchenko, Y. V., Bakalynskyi, O. O., Myalkovskyi, D. V., & Zubkov, D. A. (2023). Method for assessing the cybersecurity state of a critical infrastructure facility under review. *Problems of Creation, Testing, Application, and Operation of Complex Information Systems: Collection of Scientific Papers of ZhVI, 25(II)*, 40–57.
13. Zhylin, A., Beliavsky, V., & Bakalynsky, O. (2024). NIST CSF 2.0: New cybersecurity framework from the National Institute of Standards and Technology of the United States. *Ukrainian Scientific Journal of Information Security, 30(1)*, 73–76.
14. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals*. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.