УДК [004.02/.032/.421] + 621.391 +004.031.42+007.2 к.т.н. **Козубцова Л.М.** (ВІТІ)

DOI: https://doi.org/10.17721/2519-481X/2021/71-07

ПРОЦЕСНО-РИЗИКОВИЙ ПІДХІД У ПЛАНУВАННІ ЗАХОДІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Кібербезпека як стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання, нейтралізація кіберзагроз є актуальною задачею сучасного суспільства. Забезпечення кібербезпеки та управління нею в організації є безперервним циклічним процесом. Він ґрунтується на творчому підході, рекомендованому в NIST Special Publication 800-53 та в долученні процесного підходу, подано в стандарті ISO 9001:2000. Мета дослідження полягає в тому, щоб на основі аналізу світових рішень та підходів до планування заходів кібербезпеки організацій обґрунтувати підхід до планування заходів кібернетичної безпеки об'єктів критичної інформаційної інфраструктури.

У статті проаналізовано ключовий досвід з рішення та підхід до планування заходів кібербезпеки організацій. Встановлено, що забезпечення кібербезпеки та управління нею в організації є безперервним циклічним процесом. Тому надано перевагу застосуванню процесного підходу за схемою PDCA (Plan, Do, Chek, Akt). На підставі аналізу запропоновано обрати базовий підхід до планування заходів кібер безпеки організацій. Таким чином, одержано наукову новизну, яка полягає в тому, що вперше запропоновано до удосконаленої онтології кібербезпеки блок «заходи захисту» доповнити моделлю процесів за схемою PDCA. Практичне значення полягає в доповненні удосконаленої онтології кібербезпеки, а саме блок «заходи захисту моделлю процесів за схемою PDCA, що дає змогу отримати методику планування заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури.

Перспективи подальших досліджень у даному напрямку доцільно зорієнтувати на обґрунтування постановки завдання щодо доцільності розробки:

1) методики планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури;

2) методики оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури.

Ключові слова: підхід, планування, заходи, кібербезпека, об'єкт критичної інформаційної інфраструктури.

Вступ. Кібербезпека – стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави [1].

Постановка завдання і зв'язок її з важливими науковими завданнями. На підставі положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку сектору безпеки і оборони України визначено оперативну ціль «1.5. Удосконалення системи кібербезпеки та захисту інформації» [2, с. 33], Закону України "Про основні засади забезпечення кібербезпеки України" [3]; Стратегії кібербезпеки України [4]; Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [5]; постає адміністративно-розпорядче завдання щодо необхідності розробки методики планування заходів кібербезпеки організацій.

Виділення невирішених раніше частин загальної проблеми, якій присвячується стаття. Однак з наукової точки зору необхідно провести аналіз світових рішень та підходів до планування заходів кібербезпеки організацій на додержання вимог щодо кіберзахисту об'єктів критичної інфраструктури визначених в Постанові КМУ [6], на що буде зорієнтоване дійсне дослідження.

Аналіз останніх досліджень і публікацій. Дана робота є продовженням дослідження з попереднього опису “Майбутнє безпекове середовище 2030” [7], розширюючи наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій [5]. При опрацюванні матеріалів цікавим виявився досвід та результати роботи [8], в якій автори досліджували питання можливості управління інформаційною безпекою інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act». Питання розробки динамічного планування та прийняття рішень на основі ймовірнісно-статистичних методів розглянуто в дисертації [9].

Формулювання мети дослідження. На основі аналізу світових рішень та підходів до планування заходів кібербезпеки організацій запропонувати підхід до планування заходів кібербезпеки об’єктів критичної інформаційної інфраструктури (ОКІІ).

Виклад основного матеріалу дослідження. У світовій теорії та практиці набув практичного впровадження процесний підхід [10]. Він притаманний сучасному уявленню про функціонування організації та інформаційних систем (рис. 1 – 2). Процесний підхід детально подано в стандарті ISO 9001:2000 й міцно увійшов у повсякденну діяльність багатьох світових компаній, для опису бізнес-процесів. Процес – сукупність організаційних елементів, відношень, ресурсів, що розглядаються у динаміці.

Рисунок 1 – Уявлення процесу

Зручність у застосуванні цього підходу полягає також у тому, що стає можливим контролювати проходження кожного процесу (рис. 2), чим забезпечується й контрольованість функціонування системи. Тому процесний підхід є основою забезпечення управління (менеджменту) кібербезпеки.

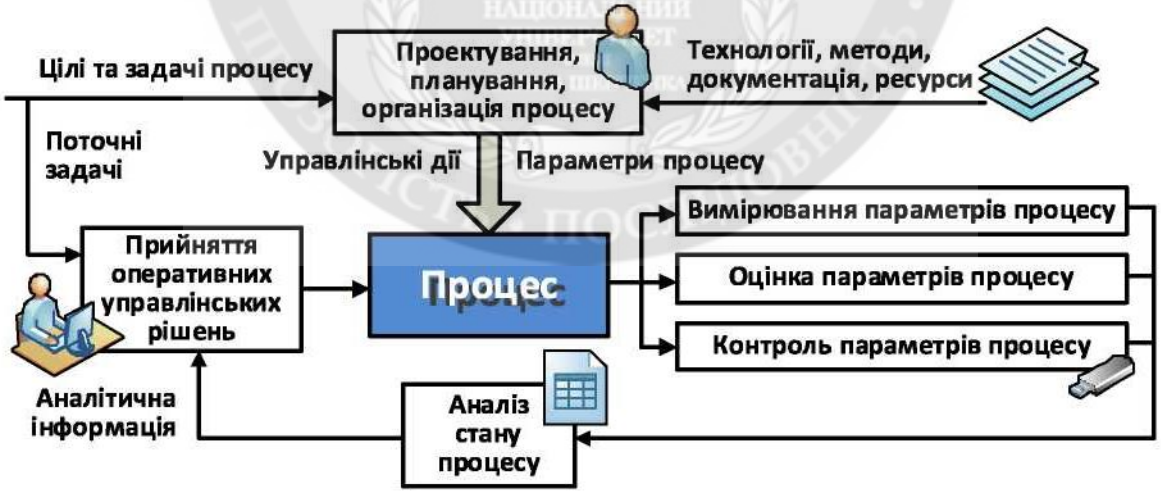

Рисунок 2 – Схема контролю процесу у системі

На рис. 3 наведено структуру процесів забезпечення кібербезпеки за схемою PDCA (Plan, Do, Chek, Akt), тобто означають (Планування заходів, Впровадження заходів, Перевірка ефективності, Покращення заходів). [8].

Забезпечення кібербезпеки та управління нею в організації є безперервним циклічним процесом. Він ґрунтується на творчому підході згідно рекомендацій NIST Special Publication 800-53 [11]. Тому безперечною перевагою є застосування процесного підходу з її простотою.

Недоліками є труднощі впровадження цього підходу, пов'язані із складністю з визначенням чіткої інтеграції процесів в єдину систему із за значної їх кількості, проблематичністю дотримання інтересів всіх учасників ланцюга процесів, різними тлумаченнями й розумінням стандарту у різних консультантів (експертів).

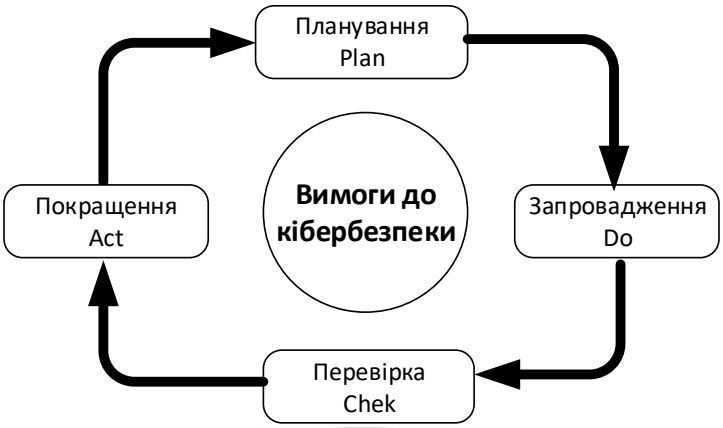

Рисунок 3 – Структура процесів забезпечення кібербезпеки за схемою PDCA

Практика свідчить, що процесний підхід «запрацює» тільки в умовах створення системи збалансованих показників в галузі безпеки. Але це дуже не просто, особливо з огляду на те, що система управління (менеджменту) інформаційної безпеки поки що знаходиться більше в області теорії й концепції, а не успішної практики.

Разом із тим керівництво організації переслідує мету, що кібербезпека повинна досягатися економічно виправданими заходами, коли можливий збиток є занадто великим, необхідно прийняти відповідні заходи захисту, але вони мають бути економічно виправданими. Очевидно, що оцінюючи розмір збитку, необхідно мати на увазі не тільки безпосередні витрати на заміну обладнання або відновлення інформації, але й інші параметри, при якому досягається прийнятний рівень кіберзахищеності (рис. 4) [10].

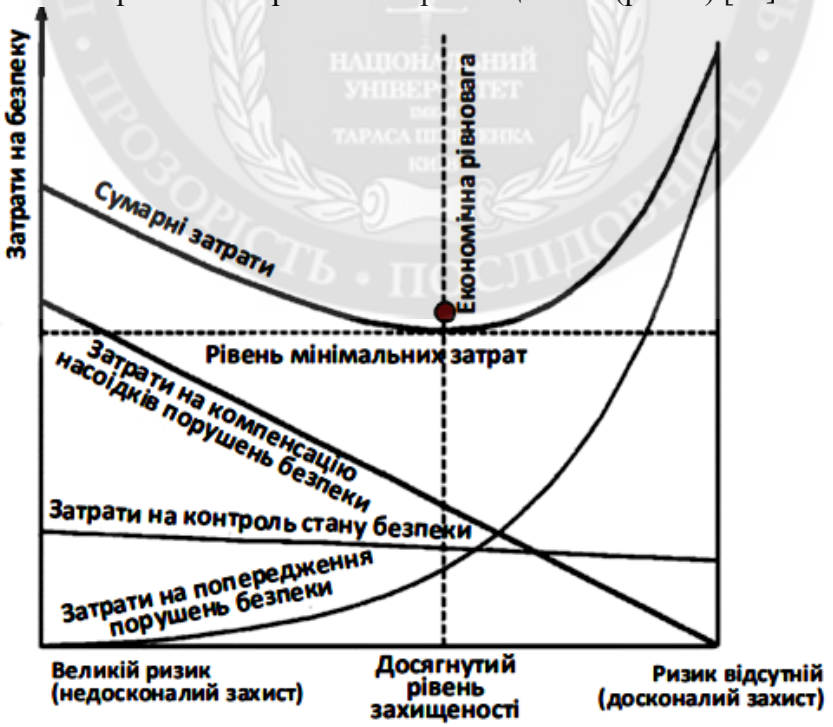

Рисунок 4 – Співвідношення затрат на забезпечення кібербезпеки та досягнутим рівнем захищеності

Рівень ризику є функцією ймовірності реалізації певної кіберзагрози, яка націлена на використання притаманних їй уразливих місць, а також розміри можливого збитку, критичного для цінних активів організації. Виходячи з цього, суть пропонованих заходів щодо управління ризиками полягає в тому, щоб оцінити їхній розмір, розробити ефективні й економічні заходи кібербезпеки та зниження ризиків, а потім переконатися, що ризики укладені в прийнятні норми і залишаються такими.

В роботі [12, с. 321] проведено додатково обґрунтування реалізації принципу розумної достатності функціонування комплексної системи захисту інформації (КСЗІ) на підприємстві. Типова залежність величини збитку підприємства (3) від вартості побудови КСЗІ (B) наведена на рис. 5. Авторами доказано, що із зростанням вартості побудови КСЗІ на підприємстві спостерігається значне зменшення ймовірності нанесеного збитку підприємства $P_{3б}$ (зменшення вразливості інформаційного ресурсу (ІР)). З рисунку також видно, що застосування навіть недорогих заходів і засобів на забезпечення інформаційної безпеки підприємства ($V_{ек}$) різко знижує сумарний збиток підприємства (B_{Σ}). Тому інвестиції в побудову КСЗІ дуже ефективні навіть в порівняно невеликих розмірах, а крива збитку (B_{Σ}) в деякій точці має найменше значення, яке можна вважати оптимальним.

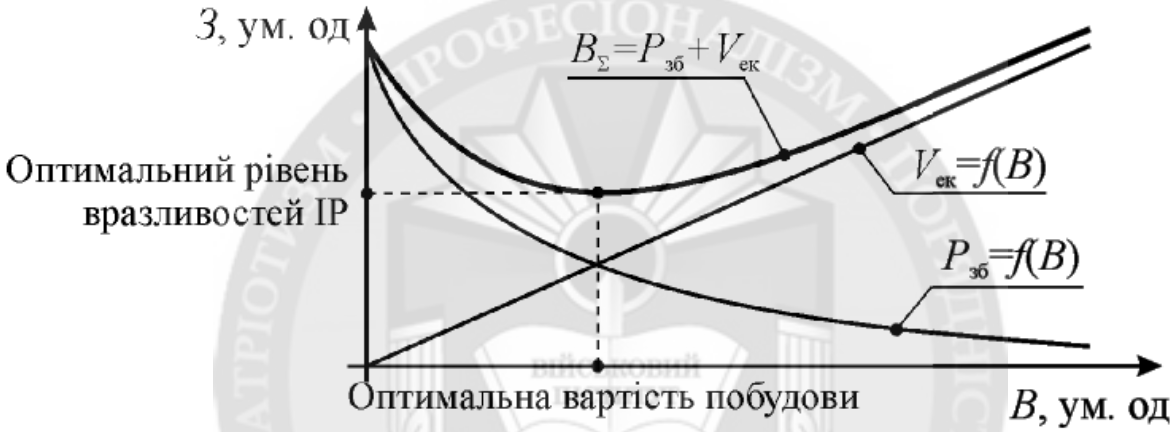

Рисунок 5 – Залежність збитку підприємства від вартості побудови КСЗІ

Зростання інвестицій в побудову КСЗІ вище за оптимальне значення веде до збільшення сумарних витрат підприємства. В цьому випадку підвищення надійності роботи КСЗІ і відповідне зниження ймовірності появи збитку підприємства нівелюються надмірно високою вартістю забезпечення інформаційної безпеки підприємства.

Тому якнайкращою стратегією, мабуть, є використання КСЗІ, що забезпечує мінімум сумарних витрат на її впровадження та експлуатацію. Ефективність цього рішення може бути підтверджена експериментальними дослідженнями. Виходячи з цього, виникає логічне запитання: Чи успішно досягнуто рівень захищеності організації в залежності від обраних заходів кібербезпеки? Тому на нашу думку є доречним обрати альтернативний шлях пошук рішення науково-технічної проблеми забезпечення кібербезпеки ОКІІ в умовах впливу кіберпростору. Слід констатувати, що час в наукових дослідженнях не достатньо приділено уваги поняттям «актив» і «збитків організації» від втрати «активів». Саме через відсутність в зверненні понять «активи» організації, його втрати активу, що не дозволяло знаходити причинно-наслідкові зв'язки необхідної для моделювання найгіршого варіанту забезпечення кібербезпеки ОКІІ.

На підставі результатів та висновків з аналізу відомих світових рішень щодо планування заходів, спрямованих на забезпечення кібербезпеки організацій та обраного шляху підвищення кібербезпеки ОКІІ в дійсній статті пропонуємо обрати за структуру методики планування заходів кібербезпеки ОКІІ модель PDCA та долучити удосконалену онтологію [13]. Результат для наочності зобразимо на рис. 6. Процес планування, впровадження, перевірки здійснюється для кожного засобу (Z_i), та компоненти (K_j) ОКІІ, які вразливі до деструктивних інформаційних впливів. За результатами оцінювання ефективності виконання

заходів, спрямованих на забезпечення кібербезпеки ОКІІ приймається рішення щодо подальших дій на необхідність посилення (покращення) заходів чи лишити їх без змін.

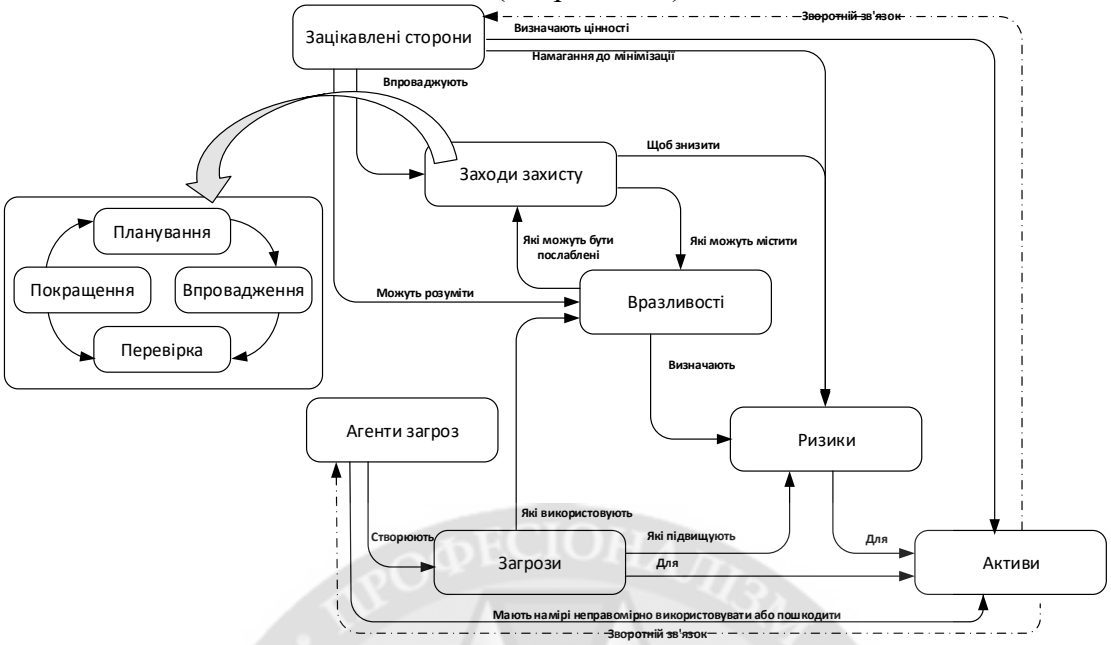

Рисунок 6 – Місце моделі PDCA в удосконаленій онтології кібербезпеки

Обговорювання результатів. Запропоноване рішення на рис. 6 дає законні підстави до застосування процесного підходу в плануванні заходів забезпечення кібербезпеки ОКІІ, що забезпечуватиме виконання вимог додержання максимальної ефективності прогнозованих ризиків. Співвідношення ризиків та наслідків наочно демонструється на рис. 7. Для забезпечення її функціонування необхідно розробити методику оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ, що і пропонується у підпункті перспективи подальших досліджень.

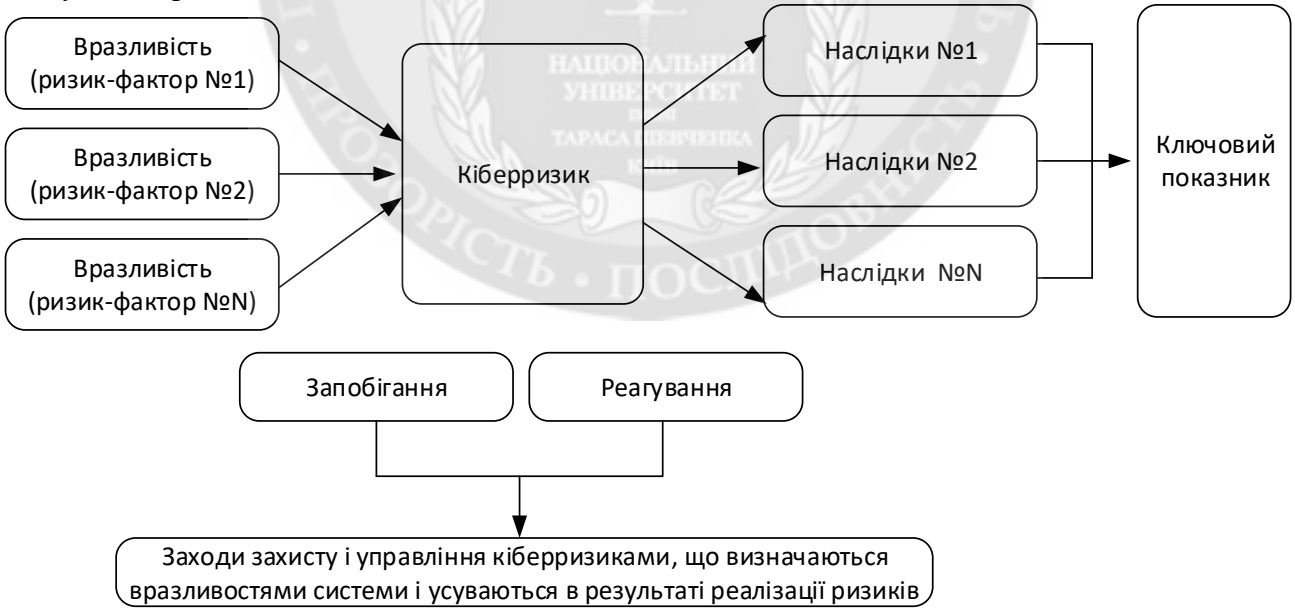

Рисунок 7 – Діаграма аналізу кіберризику

Результати обчислень за цією методикою буде вихідна інформація, яка по лінії зворотного зв’язку надходитиме до блоку «покращення» для прийняття рішення адміністратором щодо подальших дій, а саме відповідно до моделі PDCA на зміну заходів забезпечення кібербезпеки організацій.

Таким чином, до майбутньої методики планування заходів забезпечення кібербезпеки організацій необхідно також доповнити логічним етапом методики оцінки кіберзахищеності організації, опис якої подано в роботах [14; 15]. Ми прогнозуємо, що значення кіберзахищеності ОКІІ необхідні для розрахунку та оцінюванні ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ.

Висновки з даного дослідження. Таким чином, можна сформулювати наступні висновки:

1. Питання планування заходів забезпечення кібербезпеки є вкрай критично необхідним для всіх ОКІІ. По-перше, діяльність організації все більше пов'язана із ОКІІ, а саме збиранням, оброблення та зберіганням безпрецедентної кількості даних на комп'ютерах та інших пристроях. По-друге, не забезпечення своєчасного планування заходів, спрямованих на забезпечення кібернетичної безпеки ОКІІ організації, зростає ймовірність настання для організації катастрофічних наслідків прогнозованих в "Майбутньому безпековому середовище 2030. Аналіз стратегічного передбачення".

2. Аналіз світових рішень щодо планування заходів забезпечення кібербезпеки організацій підтверджує перспективність застосування моделі процесів за схемою PDCA для планування заходів забезпечення кібербезпеки ОКІІ.

3. Пропонується структуру майбутньої методики планування заходів забезпечення кібербезпеки ОКІІ побудувати таким чином, щоб враховувала логіку моделі процесів PDCA.

Наукова новизна. Вперше запропоновано до удосконаленої онтології кібербезпеки в блок «заходи захисту» додати модель процесів за схемою PDCA.

Практичне значення в доповнені удосконаленої онтології кібербезпеки, а саме в блок «заходи захисту», моделлю процесів за схемою PDCA, що дає змогу отримати методику планування заходів забезпечення кібербезпеки ОКІІ.

Перспективи подальших досліджень доцільно зорієнтувати на обґрунтуванні постановки завдання щодо доцільності розробки:

1) методики планування заходів кібербезпеки ОКІІ;

2) методики оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ.

ЛІТЕРАТУРА:

1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. К.: ДУТ, 2015. 288 с.

2. Петренко А.Г. План дій щодо впровадження оборонної реформи у 2016–2020 роках (дорожня карта оборонної реформи). Затверджено Міністром оборони України від 15.08.2016 р. К.: ДВПСП та МС МО України, 2016. 210 с.

3. Закон України "Про основні засади забезпечення кібербезпеки України". Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 28.05.21).

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", затверджена Указом Президента України від 15.03.16 №96/2016. Верховна Рада України. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення 28.05.21).

5. Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13.02.17 № 254/2017. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17 (дата звернення 28.05.21).

6. Про затвердження "Загальних вимог до кіберзахисту об'єктів критичної інфраструктури". Постанова КМУ від 19.06.19 №518. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п (дата звернення 28.05.21).

7. Козубцов І.М., Козубцова Л.М. Прогноз можливих наслідків настання "колапсу інформаційних систем спеціального призначення". *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50 – 53.

8. Воропаєва В.Я., Щербов І.Л., Хаустова Е.Д. Управління інформаційною безпекою

інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act». *Наукові праці Донецького національного технічного університету.* Серія: Обчислювальна техніка та автоматизація. Випуск 25. 2013. С. 104 – 110.

9. Гожий О.П. Інформаційні технології динамічного планування та прийняття рішень на основі ймовірнісно-статистичних методів: дисертація на здобуття наукового ступеня доктора технічних наук 05.13.06 – Інформаційні технології. Миколаїв: Чорноморський державний університет імені Петра Могили, 2016. 375 с.

10. Ковтунець В.В., Нестеренко О.В., Савенков О.І. Безпека систем підтримки прийняття рішень: навч. посібник. К.: Національна академія управління, 2016. 190 с.

11. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

12. Грицюк Ю.І. Особливості реалізації принципу розумної достатності функціонування комплексної системи захисту інформації на підприємстві. *Науковий вісник НЛТУ України*. 2015. Вип. 25.4. С. 313 – 324.

13. Хлапонін Ю.І., Козубцов І.М., Козубцова Л.М. Ідея впровадження зворотного зв'язку як вдосконалення функціональної залежності реалізації кібернетичної безпеки. Міжнародна науково-практична конференція "*Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку*". Збірник тез доповідей (Харків, 15 березня 2021 р.). Х.:. НАНГ України, 2021. С. 86 – 87.

14. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П Методика оцінки кібернетичної захищеності системи зв'язку організації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. №1(31). С. 43 – 46.

15. Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. *Збірник наукових праць ВІТІ*. К.: ВІТІ, 2018. № 2. С. 67 – 76.

REFERENCES*:*

1. Buriachok V.L., Tolubko V.B., Khoroshko V.O. and Toliupa S.V. (2015) "Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk" [Information and cybersecurity: socio-technical aspect: textbook]. K .: DUT, 288 p.

2. Petrenko A.H. (2016) "Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016–2020 rokakh (dorozhnia karta oboronnoi reformy). Zatverdzheno Ministrom oborony Ukrainy vid 15.08.2016 r." [Action Plan for the Implementation of Defense Reform in 2016–2020 (Defense Reform Roadmap). Approved by the Minister of Defense of Ukraine on 15.08.2016.]. K.: DVPSP and MS MoD of Ukraine, 210 p.

3.Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" [Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"]. Verkhovna Rada of Ukraine URL: zakon.rada.gov.ua/laws/show/2163-19 (accessed 28.05.21).

4. "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy", zatverdzhena Ukazom Prezydenta Ukrainy vid 15.03.16 #96/2016" [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine", approved by the Decree of the President of Ukraine of March 15, 2016 №96/2016]. Verkhovna Rada of Ukraine URL: zakon5.rada.gov.ua/laws/show/96/2016 (accessed 28.05.21).

5. "Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 10.07.17 "Pro stan vykonannia rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku" "Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii", vvedenoho v diiu Ukazom Prezydenta Ukrainy vid 13.02.17 #254/2017" [Decision of the National Security and Defense Council of Ukraine dated 10.07.17 "On the status of implementation of the decision of the National Security and Defense Council of Ukraine dated December 29, 2016" "On threats to cybersecurity and urgent measures to neutralize them", enacted by Presidential Decree of 13.02. 17 № 254/2017]. Verkhovna Rada of Ukraine URL: zakon.rada.gov.ua/laws/show/n0006525-17 (accessed 28.05.21).

6. "Pro zatverdzhennia "Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury". Postanova KMU vid 19.06.19 #518" [On approval of the "General requirements for cyber protection of critical infrastructure". Resolution of the Cabinet of Ministers of 19.06.19 18518]. Verkhovna Rada of Ukraine URL: zakon.rada.gov.ua/laws/show/518-2019-п (accessed 28.05.21).

7. Kozubtsov I.M. and Kozubtsova L.M. (2021) "Prohnoz mozhlyvykh naslidkiv nastannia "kolapsu informatsiinykh system spetsialnoho pryznachennia" [Forecast of possible consequences of the onset of

"collapse of special purpose information systems"]. *Actual problems of information security management of the state*: collection. thesis science. ext. scientific-practical conf. (Kyiv, March 26, 2021). Kyiv. NA SBU, 2021. Pp. 50 – 53.

8. Voropaieva V.Ya., Shcherbov I.L. and Khaustova E.D. (2013) "Upravlinnia informatsiinoiu bezpekoiu informatsiino-telekomunikatsiinykh system na osnovi modeli «plan-do-check-act»" [Information security management of information and telecommunication systems based on the "plan-do-check-act" model]. *Scientific works of Donetsk National Technical University*. Series: Computing and automation. Issue 25, Pp. 104 – 110.

9. Hozhyi O.P. (2016) "Informatsiini tekhnolohii dynamichnoho planuvannia ta pryiniattia rishen na osnovi ymovirnisno-statystychnykh metodiv" [Information technologies of dynamic planning and decision-making on the basis of probabilistic-statistical methods]. The dissertation on competition of a scientific degree of the doctor of technical sciences 05.13.06 - Information technologies. Mykolaiv. Petro Mohyla Black Sea State University, 375 p.

10. Kovtunets V.V., Nesterenko O.V. and Savenkov O.I. (2016) "Bezpeka system pidtrymky pryiniattia rishen" [Security of decision support systems] textbook. Manual. Kyiv. National Academy of Management, 190 p.

11. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

12. Hrytsiuk Yu.I. (2015) "Osoblyvosti realizatsii pryntsypu rozumnoi dostatnosti funktsionuvannia kompleksnoi systemy zakhystu informatsii na pidpryiemstvi" [Peculiarities of realization of the principle of reasonable sufficiency of functioning of complex system of information protection at the enterprise]. *Scientific herald of NLTU of Ukraine*. Vip. 25.4. Pp. 313 – 324.

13. Khlaponin Yu.I., Kozubtsov I.M. and Kozubtsova L.M. (2021) "Ideia vprovadzhennia zvorotnoho zviazku yak vdoskonalennia funktsionalnoi zalezhnosti realizatsii kibernetychnoi bezpeky" [The idea of introducing feedback as an improvement of the functional dependence of the implementation of cyber security] International scientific-practical conference "*The use of information technology in the training and operation of law enforcement agencies*." Collection of abstracts (Kharkiv, March 15, 2021). Kharkiv. NANG of Ukraine, Pp. 86 – 87.

14. Kozubtsov I.M., Kozubtsova L.M., Kutsaiev V.V. and Tereshchenko T.P. (2018) "Metodyka otsinky kibernetychnoi zakhyshchenosti systemy zviazku orhanizatsii" [Methods for assessing the cyber security of the communication system of the organization]. *Modern information technologies in the field of security and defense*. №1 (31). Pp. 43 – 46.

15. Kutsaiev V.V., Radchenko M.M., Kozubtsova L.M. and Tereshchenko T.P. "Metodyka otsinky kibernetychnoi zakhyshchenosti informatsiino-telekomunikatsiinoho vuzla zviazku" [Methods for assessing the cyber security of information and telecommunications nodes]. *Collection of scientific papers VITI*. Kyiv. VITI, 2018. № 2. Pp. 67 – 76.

Ph.D. Kozubtsova L.M.

RISK PROCESS APPROACH IN PLANNING CYBER SECURITY MEASURES OF CRITICAL INFRASTRUCTURE FACILITIES

Cybersecurity as a state of security of critical objects of the national information infrastructure and its individual components, which ensures their sustainable functioning and development, timely detection, prevention, neutralization of cyber threats is an urgent task of modern society. Ensuring cybersecurity and its management in an organization is a continuous cyclical process. It is based on the creative approach recommended in NIST Special Publication 800-53 and in the introduction of the process approach, presented in the ISO 9001: 2000 standard. The purpose of the study is to justify an approach to planning cybersecurity activities of critical information infrastructure objects based on the analysis of global solutions and approaches to planning cybersecurity activities of organizations.

The article analyzes the key experience in solving and the approach to planning cybersecurity activities of organizations. It is established that the provision of cybersecurity and its management in the organization is a continuous cyclical process. Therefore, preference is given to the use of a process approach according to the PDCA scheme (Plan, Do, Chek, Akt). Based on the analysis, it is proposed to choose a basic approach to planning cybersecurity activities of organizations.

Thus, the scientific novelty is obtained, which consists in the fact that for the first time it is proposed to supplement the "protection measures" block to the improved ontology of cybersecurity with a model of processes according to the PDCA scheme. The practical significance is to supplement the improved

cybersecurity ontology, namely the "protection measures" block with a model of processes according to the PDCA scheme, which allows us to obtain a methodology for planning measures to ensure cybersecurity of critical information infrastructure objects.

It is advisable to focus the prospects for further research in this direction on the justification of the formulation of the problem of the expediency of development:

1) methods of planning cybersecurity measures for critical information infrastructure facilities;

2) methods for evaluating the effectiveness of measures aimed at ensuring the cybersecurity of critical information infrastructure facilities.

Key words: approach, planning, activities, cyber security, critical information infrastructure object.