DOI:**10.33099/2311-7249/2021-41-2-17-22**

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Леся Михайлівна Козубцова *(кандидат технічних наук)*[1]
Юрій Іванович Хлапонін *(доктор технічних наук, професор)*[2]
Ігор Миколайович Козубцов *(доктор педагогічних наук, старший науковий співробітник)*[1]

[1]***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2]***Київський національний університет будівництва і архітектури, Київ, Україна***

МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВИКОНАННЯ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЙ

В науковій статті обґрунтовано методику оцінювання ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури організацій. Дана робота є продовженням дослідження з попереднього опису "Майбутнє безпекове середовище 2030", розширюючи наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій. Необхідність статті обумовлена раціональним вибором та застосуванням заходів, спрямованих на забезпечення кібернетичної безпеки об'єктів інформаційної інфраструктури організацій. Встановлено, що на практиці оцінити ефективність виконання заходів, спрямованих на забезпечення кібернетичної безпеки можна через наступні показники (ймовірності): ризик кібернетичної безпеки, кіберзахищеність, функціональна працездатність системи об'єкта критичної інформаційної інфраструктури, кіберстійкість. Для застосування принципу наступності в статті під удосконалену онтологію кібербезпеки обрано показник (ймовірність) ризику кібернетичної безпеки. Методика оцінки ризику кібербезпеки об'єктів критичної інформаційної інфраструктури організацій базується на визначенні ймовірності реалізації кібератак, а також рівнів їх збитку. Методика включає наступні етапи: етап розробки системи показників оцінювання ефективності виконання заходів; етап планування процедур збирання вихідних даних для оцінювання ефективності виконання заходів; етап обчислення значення показника ефективності виконання заходів; етап інтерпретації значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій. Вихідні значення для розрахунку кіберзахищеності отримують за результатами аудиту об'єктів критичної інформаційної інфраструктури організацій. При розрахунку значень ймовірності кібератак, а також рівня можливого збитку слід скористатися статистичними методами, експертними оцінками або елементами теорії прийняття рішень. Наукова новизна одержаного результату полягає в тому, що вперше запропоновано методику оцінювання ефективності заходів кібербезпеки за показником (ймовірності) ризику кібербезпеки, яка доповнюватиме методику планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організацій.

Ключові слова: *методика, оцінювання, ефективність, заходи, кібербезпека, об'єкт критичної інформаційної інфраструктури, організація.*

Вступ

Постановка проблеми. Кібернетична безпека (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. 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» [1, с. 33], Закону України "Про основні засади забезпечення кібербезпеки України" [2]; Стратегії кібербезпеки України [3]; 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" [4] встановлено, що на даний час на існуючих об'єктах критичної інфраструктури організацій відсутня методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій за запропонованою методикою планування [5]. Однак залишається актуальним питанням з'ясувати за якими критеріями та показниками оцінити ефективність заходів і якого досягається рівня кібербезпеки ОКІІ організації виходячи із онтології поданої на рис. 1 [6]. Тому, на підставі [1-4] виникає об'єктивне наукове завдання щодо необхідності обґрунтування методики оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій.

Аналіз останніх досліджень і публікацій. Дана робота є логічним продовженням дослідження з попереднього опису "Майбутнє безпекове середовище 2030" [7] розширюючи наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій [4].

В роботі [8] подана методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. Спроба її застосувати на практиці у Військовому інституту телекомунікацій та інформатизації імені Героїв Крут виявилась складною в обчислюванні. На відміну від цієї роботи в [9] подано методика оцінки ризиків інформаційної безпеки розрахована для підприємств малого та середнього бізнеса. Процес оцінки ризиків інформаційної безпеки ґрунтується на використанні методів оцінки ризиків економічної безпеки.

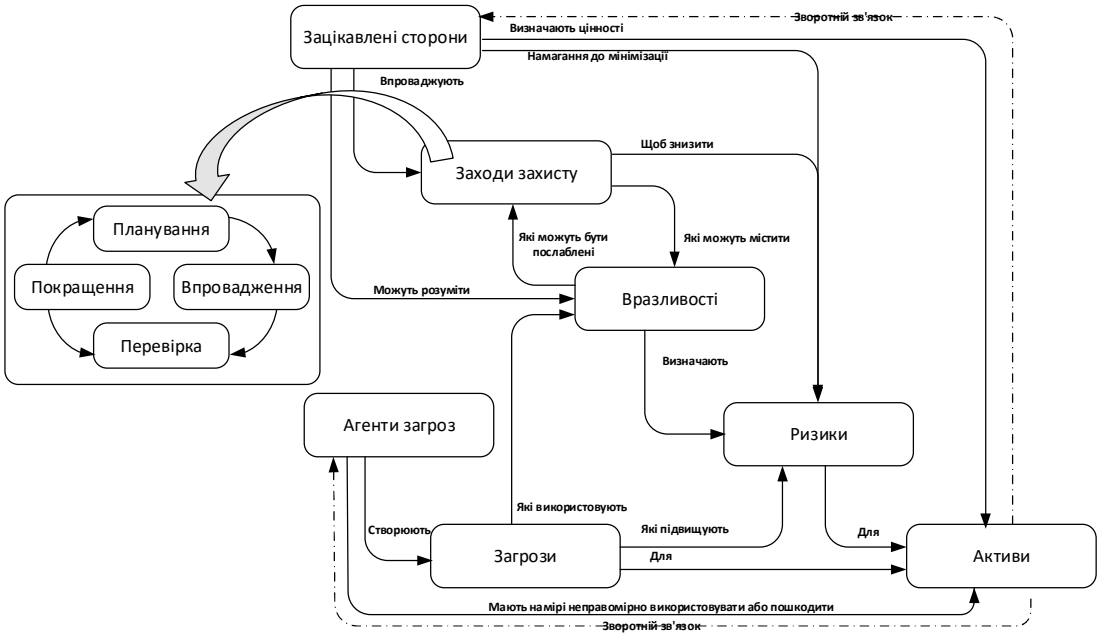

Рисунок 1. Структурна залежність заходів та ризиків у онтології кібербезпеки

Необхідність у методиці оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій обумовлена нестабільністю у часі кібербезпеки на зазначених об'єкта та ризиком втрати активів.

Тому, виходячи з підстав, що перелічені в роботах [8; 9] методики не враховують показник кіберзахищеності $P_{КЗ}(S)$, автори вважають за потребу запропонувати науковому суспільству до обговорення методику оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій на засадах кіберзахищеності.

Мета статті. Апробувати структуру методики оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій.

Виклад основного матеріалу дослідження.

Вихідним положення нашого дослідження є запропонована методика планування заходів кібербезпеки ОКІІ організації [5]. Для неї визначимо логічний етап оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації. У її структури логічним місцем є етап «9 Оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації».

Для об'єктивності оцінювання ефективності виконання заходів кібербезпеки ОКІІ організації необхідно визначити сукупність показників та критеріїв оцінювання. Для цього скористаємося наступними рекомендаціями щодо формування показників та критеріїв оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Розпочинати роботу з формування системи показників слід лише після того, як буде з'ясовано, що саме ми прагнемо виміряти та для чого це необхідно робити.

Зазвичай, потреба у формуванні системи показників пов'язана із здійсненням оцінювання ефективності заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації для забезпечення зворотного зв'язку. Результати оцінювання дають інформацію для прийняття рішення про те, чи варто продовжувати експлуатувати ОКІІ чи її варто припинити та обрати інші заходи для покращення кіберзахищеності.

Одним з відповідальних завдань, що покладається на експертну групу є складання актуального та адекватного переліку показників (індикаторів) та критеріїв для оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Кількість індикаторів $I_{КЗ}$ для різних компонентів засобів Z_i є різною.

В сучасній теорії та практиці оцінювання ефективності заходів використовують різні показники та у відповідності ним критерії в залежності від наявних вихідних даних. Тому це питання актуальне і для оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Перелічимо найбільш вживані показники оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки через показник (ймовірність): ризику кібербезпеки [8]; кіберзахищеності [10]; функціональної працездатності системи (ОКІІ) [11]; кіберстійкості [12]. Вибір тих чи інших зазначених показників оцінювання ефективності виконання заходів залежить від наявних вихідних даних у експертів.

У випадку здійснювання процедури оцінювання ефективності виконання заходів,

спрямованих на забезпечення кібербезпеки через показник (ймовірність) кіберзахищеності, то вихідні дані отримуються за результатом обчислювання значення кіберзахищеності за методикою [10].

Згідно удосконаленої онтології кібербезпеки поданої на рис. 1 [6], виникає необхідність здійснювання процедури оцінювання ефективності виконання заходів, що спрямовані на забезпечення кібербезпеки ОКІІ через показник (ймовірності) ризику кібербезпеки або ймовірних наслідків впливу на активи організації. І тоді логічним є постановка завдання на вирішення зворотної задачі з пошуку оптимальних заходів які несуть мінімальний ризик. Отже, зменшення ризику можливо досягнути за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення кібератаки або зменшити можливі збитки від неї.

Ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків ОКІІ, що дозволяє виключити проведення тієї чи іншої атаки. Наприклад, фізичне відключення від Інтернету сегмента ОКІІ, в якому обробляється конфіденційна інформація, дозволяє уникнути зовнішніх атак на конфіденційну інформацію.

Прийняття ризику, якщо він зменшений до того рівня, на якому вже не становить небезпеку для ОКІІ організації.

При виборі заходів для підвищення рівня захисту ОКІІ враховується одне принципове обмеження – вартість реалізації цих заходів не повинна перевищувати вартості захищених інформаційних ресурсів, а також збитків організації від можливого порушення конфіденційності, цілісності або доступності інформації.

Виходячи із вище розглянутого в статті пропонується здійснювати процедуру оцінювання ефективності виконання заходів забезпечення кібербезпеки через показник (ймовірності) ризику кібербезпеки.

Критерії оцінки ймовірності ризику кібербезпеки ОКІІ $P_{R(ДІВ)}$ подано в табл. 1.

Вихідні значення для розрахунку кіберзахищеності отримують за результатами аудиту ОКІІ, а обчислення здійснюють за формулами методики [10].

В табл. 2 – 4 наведені критерії оцінки ризиків кібербезпеки, в яких для оцінки рівнів збитків та ймовірності кібератаки використовується п’ять понятійних рівнів.

Таблиця 1

Критерії оцінки ймовірності ризику кібербезпеки ОКІІ

№ п/п	Критерій	Ймовірність $P_{R(ДІВ)}$	Опис
1	$0 \le P_{R(ДІВ)} \le 0{,}25$	Дуже низький	Дуже низький рівень ризику
2	$0{,}25 \le P_{R(ДІВ)} \le 0{,}5$	Низький	Низький рівень ризику
3	$0{,}5 \le P_{R(ДІВ)} \le 0{,}75$	Середній	Середній рівень ризику
4	$0{,}75 \le P_{R(ДІВ)} \le 0{,}9$	Високий	Високий рівень ризику
5	$0{,}9 \le P_{R(ДІВ)} \le 1$	Дуже високий	Дуже високий рівень ризику

Таблиця 2

Критерії оцінки кіберзахищеності ОКІІ

№ п/п	Критерій	Рівень	Опис
1	$0 \le P_{КЗ}(S) \le 0{,}25$	незадовільний	Вибрані заходи кібербезпеки ОКІІ забезпечують незадовільний рівень кіберзахищеності, підлягає негайному припиненню експлуатація ОКІІ.
2	$0{,}25 \le P_{КЗ}(S) \le 0{,}5$	низький	Вибрані заходи кібербезпеки ОКІІ забезпечує низький рівень кіберзахищеності
3	$0{,}5 \le P_{КЗ}(S) \le 0{,}75$	середній	Вибрані заходи кібербезпеки ОКІІ забезпечує середній рівень кіберзахищеності
4	$0{,}75 \le P_{КЗ}(S) \le 0{,}9$	високий	Вибрані заходи кібербезпеки ОКІІ в цілому забезпечує високий рівень кіберзахищеності
5	$0{,}9 \le P_{КЗ}(S) \le 1$	найвищий	Вибрані заходи кібербезпеки ОКІІ забезпечують найвищий рівень кіберзахищеності.

Таблиця 3

Критерії оцінки рівня збитків $Z_{(ДІВ)}$

№ п/п	Критерій	Рівень збитку $Z_{(ДІВ)}$	Опис
1	$0 \le Z_{(ДІВ)} < 0{,}25$	Малий	Незначні втрати матеріальних активів, які швидко відновлюються або незначні наслідки для організації
2	$0{,}25 \le Z_{(ДІВ)} < 0{,}5$	Помірний	Помітні втрати матеріальних активів або помірні наслідки
3	$0{,}5 \le Z_{(ДІВ)} \le 0{,}75$	Середній	Суттєві втрати матеріальних активів або значна шкода
4	$0{,}75 \le Z_{(ДІВ)} \le 0{,}9$	Великий	Великі втрати матеріальних активів і велика шкода для організації
5	$0{,}9 \le Z_{(ДІВ)} \le 1$	Критичний	Критична або повна втрата матеріальних активів організації

Таблиця 4

Критерії оцінки ймовірності проведення ДІВ $P_{(ДІВ)}$

№ п/п	Критерій	Ймовірність $P_{(ДІВ)}$	Опис
1	$0 \le P_{(ДІВ)} \le 0{,}25$	Дуже низька	ДІВ практично ніколи не буде проведений
2	$0{,}25 \le P_{(ДІВ)} \le 0{,}5$	Низька	Ймовірність проведення ДІВ досить низький
3	$0{,}5 \le P_{(ДІВ)} \le 0{,}75$	Середня	Ймовірність проведення ДІВ середній
4	$0{,}75 \le P_{(ДІВ)} \le 0{,}9$	Висока	ДІВ швидше за все буде проведений
5	$0{,}9 \le P_{(ДІВ)} \le 1$	Дуже висока	ДІВ буде проведена

Методика оцінювання ефективності виконання заходів. Методика оцінки ризику кібербезпеки ОКІІ базується на визначенні ймовірності реалізації кібератак (ДІВ), а також рівнів їх збитку. Розробка та застосування в діяльності системи виміру оцінювання

ефективності виконання заходів відбувається за такими основними етапами [13, с. 33 – 35]:

Етап 1. Розробка системи показників оцінювання ефективності виконання заходів. Цей етап пов'язаний із процесом вибору показників та визначення системи міри.

Етап 2. Планування процедур збирання вихідних даних для оцінювання ефективності виконання заходів. На цьому етапі здійснюється підготовка до впровадження системи вимірювання значень показників, з плануванням доступу до необхідних даних, розробкою конфігурації обробки та розповсюдження інформації про значення показників.

Етап 3. Обчислення значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ.

Значення ризику обчислюється окремо для кожної кібератаки (ДІВ) і в загальному випадку представляється, як добуток ймовірності проведення кібератаки (ДІВ) на величину можливого збитку від цієї атаки (1):

$$P_{R(\text{ДІВ})} = P_{\text{ДІВ}} \times Z_{\text{ДІВ}} \quad (1)$$

де $P_{\text{R(ДІВ)}}$ – ймовірність ризику кібербезпеки ОКІІ;

$P_{(\text{ДІВ})}$ – ймовірність проведення кібератаки (ДІВ) на ОКІІ;

$Z_{(\text{ДІВ})}$ – збитки активів спеціальних користувачів від успішної проведеної кібератаки (ДІВ) на ОКІІ.

Обчислення ймовірності проведення кібератаки $P_{(\text{ДІВ})}$ для всієї системи S ОКІІ здійснимо за формулою (2):

$$P_{\text{ДІВ}} = 1 - P_{\text{КЗ}}(S) \quad (2)$$

тоді $P_{\text{R(ДІВ)}}$ з урахуванням (2) матимемо (3):

$$P_{R(\text{ДІВ})} = (1 - P_{\text{КЗ}}(S)) \times Z_{\text{ДІВ}}. \quad (3)$$

У методиці можуть використовувати кількісні або якісні шкали для визначення величини ризику кібербезпеки, але пропонується обирати числові вирази. При використанні кількісних шкал ймовірність проведення ДІВ приймаємо числові значення в інтервалі $P_{(\text{ДІВ})} \in [0, 1]$, а збиток $Z_{(\text{ДІВ})}$ може задаватися у вигляді грошового еквівалента матеріальних втрат, які користувачі організації понесуть у випадку успішного пропуску ДІВ.

Етап 4. Інтерпретація значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації.

Цей етап включає практичну роботу з обробки, аналізу та інтерпретації даних для прийняття рішень щодо посилення обраних заходів. Для інтерпретації рівня ризику за якісною шкалою застосуємо таблицю, в якій у першому стовпці задаємо понятійні рівні $Z_{(\text{ДІВ})}$, а в першому рядку – рівні ймовірності кібернетичного ДІВ $P_{(\text{ДІВ})}$. Комірки таблиці, розташовані на перетині відповідних рядків і стовпців, що містять рівень ризику безпеки $P_{\text{R(ДІВ)}}$ (табл. 5). В таблиці введено наступні умовні скорочення: Н – низький рівень ризику; С – середній рівень ризику; В – високий рівень ризику.

При розрахунку значень ймовірності кібератак (ДІВ), а також рівня можливого збитку слід скористатися статистичними методами, експертними оцінками або елементами теорії прийняття рішень. Статистичні методи передбачають аналіз накопичених даних пов'язаних з порушенням кібербезпеки. Проте статистичні методи не завжди вдається застосувати через брак статистичних даних про раніше проведені атаки на ресурси ОКІІ.

При використанні апарату експертних оцінок аналізуються результати роботи групи експертів, компетентних в області кібербезпеки, які на основі наявного у них досвіду визначають кількісні або якісні рівні ризику.

Елементи теорії прийняття рішень дозволяють застосовувати для обчислення значення ризику безпеки більш складні алгоритми обробки результатів роботи групи експертів.

Висновки й перспективи подальших досліджень

В сучасній теорії та практиці для оцінювання ефективності заходів, найчастіше застосовують показник (ймовірність): ризику кібербезпеки, кіберзахищеності, функціональної працездатності системи (ОКІІ), кіберстійкості. Складність застосування математичного апарату оцінювання ефективності заходів, через показник (ймовірність): ризику кібербезпеки, функціональної працездатності системи (ОКІІ) та кіберстійкості змусило до пошуку і підходу до розрахунку через показник кіберзахищеності.

Визначено сукупність показників та критеріїв для оцінювання ефективності заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації. В запропонованій методиці оцінювання ефективності виконання заходів здійснюється за показником кіберзахищеності ОКІІ організації та ризику.

На основі обраного показника та критеріїв обґрунтована структура методики оцінювання ефективності виконання заходів кібербезпеки.

Наукова новизна одержаного результату полягає в тому, що для (обчислювання) оцінювання ефективності обраних заходів кібербезпеки ОКІІ організації застосовано методику яка ґрунтується на обчислюванні показника (ймовірності) ризику кібербезпеки.

Запропонована методика націлена підвищити ефективність вибору заходів на етапі планування заходів кібербезпеки ОКІІ організації.

Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого її вивчення в такому напрямі, як розробка методології оцінки ризиків кібербезпеки у гібридних інформаційних технологій в освіті.

Література

1. Петренко А.Г. План дій щодо впровадження оборонної реформи у 2016 – 2020 роках (дорожня карта оборонної реформи). К.: ДВПСП та МС МО України, 2016. 210 с. **2.** Закон України "Про основні засади забезпечення кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/2163-19. **3.** 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. URL: https://zakon5.rada.gov.ua/laws/show/96/2016. **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", введеного в дію Указом Президента України від 13.02.17 №254/2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17.
5. **Козубцова Л.М.** Обґрунтування структури методики планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організації. *Materials of the XVII International scientific and practical Conference Prospects of world science - 2021 (Sheffield, July 30 - August 7, 2021).* Sheffield. Science and education LTDC, 2021. Volume 3. Pp. 87 – 92. **6. Козубцов І.М., Хлапонін Ю.І., 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"* (Харків, 15 березня 201 р.). Харків. НАНГ України, 2021. С. 86 – 87. **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. Гончар С.Ф.** Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2019. Том 30(69). Ч.1. С.40 – 43. **9. Плетнев П.В., Белов В.М.** Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса. *Доклады ТУСУРа*, № 1(25), Ч 2, июнь 2012. С.83 – 86. **10. Козубцова Л.М.** Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. *Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво"*. Луцьк, 2020. Випуск № 39. С.127 – 135. **11. Захарченко Р.И., Королев И.Д.** Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве. *Наукоемкие технологии в космических исследованиях Земли.* 2018. Т.10. №2. С.52 – 61. **12. Коцыняк М.А., Коцыняк М.М., Лаута О.С., Лаута А.С.** Киберустойчивость информационно-телекоммуникационной сети. *Информационные технологии, связь и защита информации МВД России*. 2015. С.104 – 105. **13. Нили Э., Адамс К., Кеннерли М.** Призма эффективности: Карта сбалансированных показателей для измерения успеха в бизнесе и управления им / пер. с англ. Д.: Баланс-Клуб, 2003. 400 с.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ВЫПОЛНЕНИЯ МЕРОПРИЯТИЙ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОГО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИЙ

***Леся Михайловна Козубцова** (кандидат технических наук)[1]*
***Юрий Иванович Хлапонин** (доктор технических наук, профессор)[2]*
***Игорь Николаевич Козубцов** (доктор педагогических наук, старший научный сотрудник)[1]*

[1]Военный институт телекоммуникаций и информатизации, Киев, Украина
[2]Киевский национальной университет строительства и архитектуры, Киев, Украина

В научной статье обоснована методика оценки эффективности выполнения мероприятий, направленных на обеспечение кибернетической безопасности объектов критической информационной инфраструктуры организаций. Данная работа является продолжением исследования по предварительному описанию "Будущая среда безопасности 2030", расширяя научные пределы по реализации неотложных мер государственной политики по нейтрализации угроз кибербезопасности организаций. Необходимость статьи обусловлена рациональным выбором и применением мер, направленных на обеспечение кибернетической безопасности объектов информационной инфраструктуры организаций. Установлено, что на практике оценить эффективность выполнения мероприятий, направленных на обеспечение кибернетической безопасности можно через следующие показатели (вероятности): риск кибернетической безопасности, киберзахищенисть, функциональная работоспособность системы объекта критической информационной инфраструктуры, киберстийкисть. Для применения принципа преемственности в статье под усовершенствованную онтологию кибербезопасности выбран показатель (вероятность) риска кибернетической безопасности. Методика оценки риска кибербезопасности объектов критической информационной инфраструктуры организаций основывается на определении вероятности реализации кибератак, а также уровней их ущерба. Методика включает следующие этапы: этап разработки системы показателей оценки эффективности выполнения мероприятий; этап планирования процедур сбора исходных данных для оценки эффективности выполнения мероприятий; этап вычисления значения показателя эффективности выполнения мероприятий; этап интерпретации значения показателя эффективности выполнения мероприятий, направленных на обеспечение кибербезопасности объектов критической информационной инфраструктуры организаций. Исходные значения для расчета киберзахищености получают по результатам аудита объектов критической информационной инфраструктуры организаций. При расчете значений вероятности кибератак, а также уровня возможного ущерба следует воспользоваться статистическими методами, экспертными оценками или элементами теории принятия решений. Научная новизна исследования заключается в том, что впервые предложена методика оценки эффективности мероприятий кибербезопасности по показателю (вероятности) риска кибербезопасности, которая будет дополнять методику планирования мероприятий кибербезопасности объектов критической информационной инфраструктуры организаций.

***Ключевые слова:** методика, оценка, эффективность, мероприятия, кибербезопасность, объект критической информационной инфраструктуры, организация.*

METHODS OF EVALUATION OF EFFICIENCY OF IMPLEMENTATION OF CYBER SECURITY MEASURES OF CRITICAL INFORMATION INFRASTRUCTURE BODIES OF THE BODY

***Lesja Kozubtsova** (Candidate of Technical Sciences)[1]*
***Yuri Khlaponin** (Doctor of Technical Sciences, Professor)[2]*
***Igor Kozubtsov** (Doctor of Pedagogical Sciences, Senior Research Fellow)[1]*

[1]Military institute of telecommunications and informatization technologies, Kiev, Ukraine
[2]Kiev National University of Civil Engineering and Architecture, Kiev, Ukraine

The scientific article substantiates the method of assessing the effectiveness of measures aimed at ensuring the cyber security of critical information infrastructure of organizations. This work is a continuation of the study on the preliminary description of "The Future of the Security Environment 2030", expanding the scientific scope for the implementation of urgent public policy measures to neutralize threats to cybersecurity of organizations. The need for the article is due to the rational choice and application of measures aimed at ensuring the cyber security of information infrastructure facilities of organizations. It is established that in practice it is possible to estimate efficiency of performance of the actions directed on maintenance of cyber security through the following indicators (probabilities): risk of cyber security, cybersecurity, functional operability of system of object of critical information infrastructure, cyberstability. To apply the principle of continuity in the article under the improved cybersecurity ontology, the indicator (probability) of cybersecurity risk is selected. The methodology for assessing the risk of cybersecurity of critical information infrastructure of organizations is based on determining the probability of cyber attacks, as well as the levels of their damage. The methodology includes the following stages: the stage of developing a system of indicators for evaluating the effectiveness of activities; the stage of planning the procedures for collecting initial data to assess the effectiveness of the activities; the stage of calculating the value of the performance indicator; stage of interpretation of the value of the indicator of efficiency of performance of the actions directed on maintenance of cybersecurity of objects of a critical information infrastructure of the organizations. The initial values for the calculation of cybersecurity are obtained based on the results of the audit of critical information infrastructure of organizations. Statistical methods, expert estimates, or elements of decision theory should be used to calculate cyber attack probability values as well as the level of possible damage. The scientific novelty of the study is that for the first time a method of evaluating the effectiveness of cybersecurity measures on the indicator (probability) of cybersecurity risk is proposed, which will complement the methodology of planning cybersecurity measures of critical information infrastructure of organizations.

Keywords: methodology, evaluation, efficiency, measures, cybersecurity, object of critical information infrastructure, organization.

References

1. Petrenko A.H. (2016) Action plan for the implementation of defense reform in 2016-2020 (road map of defense reform) [Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016-2020 rokakh (dorozhnia karta oboronnoi reformy)]. K.: DVPSP ta MS MO Ukrainy, 210 p. **2.** Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine". [Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"]. **3.** On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cyber Security Strategy of Ukraine", approved by the Decree of the President of Ukraine dated 15.03.16 №96/2016. [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]. **4.** 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. [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]. **5. Kozubtsova L.M.** (2021) Substantiation of the structure of the methodology of planning cybersecurity measures of the critical information infrastructure of the organization [Obg`runtuvannya struktury` metody`ky` planuvannya zaxodiv kiberbezpeky` ob'yektiv kry`ty`chnoyi informacijnoyi infrastruktury` organizaciyi] *Materials of the XVII International scientific and practical Conference Prospects of world science - 2021* (Sheffield, July 30 - August 7, 2021). Sheffield. Science and education LTDC, 2021. Vol. 3. Pp.87 – 92.**6. Kozubtsov I.M., Khlaponin Yu.I., Kozubtsova L.M.** (2021) The idea of introducing feedback as improving the functional dependence of the implementation of cyber security. [Ideia vprovadzhennia zvorotnoho zviazku yak vdoskonalennia funktsionalnoi zalezhnosti realizatsii kibernetychnoi bezpeky] *Mizhnarodna naukovo-praktychna konferentsiia "Zastosuvannia informatsiinykh tekhnolohii u pidhotovtsi ta diialnosti syl okhorony pravoporiadku"* (Kharkiv, 15 bereznia 2021 r.). Kharkiv. NANH Ukrainy. Pp. 86 – 87. **7. Kozubtsov I.M., Kozubtsova L.M.** (2021) Forecast of possible consequences of the "collapse of special purpose information systems" [Prohnoz mozhlyvykh naslidkiv nastannia "kolapsu informatsiinykh system spetsialnoho pryznachennia"]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy*: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 26 bereznia 2021 r.). Kyiv: NA SBU. S.50 – 53. **8. Honchar S.F.** (2019) Methodology for assessing the risks of cybersecurity of the information system of critical infrastructure facilities [Metodolohiia otsinky ryzykiv kiberbezpeky informatsiinoi systemy obiektiv krytychnoi infrastruktury]. *Vcheni zapysky TNU imeni V.I. Vernadskoho*. Seriia: tekhnichni nauky. Tom 30(69). Ch.1. S.40 – 43. **9. Плетнев П.В., Белов В.М.** Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса. *Доклады ТУСУРа*, № 1(25), Ч 2, июнь 2012. С.83 – 86. **10. Kozubtsova L.M.** (2020) Improved methodology for diagnosing cyber security of an information system taking into account destructive cybernetic influences [Udoskonalena metodyka diahnostuvannia kibernetychnoi zakhyshchenosti informatsiinoi systemy z urakhuvanniam destruktyvnykh kibernetychnykh vplyviv]. *Naukovyi zhurnal "Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo*". Lutsk. Vypusk #39. S. 127 – 135. **11. Zaharchenko R.I., Korolev I.D.** (2018) Methodology for assessing the sustainability of the functioning of critical information infrastructure objects operating in cyberspace [Metodika otsenki ustoychivosti funktsionirovaniya ob'ektov kriticheskoy informatsionnoy infrastrukturyi funktsioniruyuschey v kiberprostranstve]. *Naukoemkie tehnologii v kosmicheskih issledovaniyah Zemli.* T.10. #2. S.52 – 61. **12. Kotsyinyak M.A., Kotsyinyak M.M., Lauta O.S., Lauta A.S.** (2015) Cyber resilience of the information and telecommunication network [Kiberustoychivost informatsionno-telekommunikatsionnoy seti]. *Informatsionnyie tehnologii, svyaz i zaschita informatsii MVD Rossii.* S.104 – 105. **13. Nili E., Adams K., Kennerli M.** (2003) The Performance Prism: A Balanced Scorecard for Measuring and Managing Business Success [Prizma effektivnosti: Karta sbalansirovannyih pokazateley dlya izmereniya uspeha v biznese i upravleniya im] / per. s angl. D.: Balans-Klub. 400 s.