КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.922
УДК 004.056

Хорошко Володимир Олексійович
доктор технічніх наук, професор, професор кафедри технічного захисту інформації
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0001-6213-7086
professor_va@ukr.net

Лаптєв Олександр Анатолійович
доктор технічніх наук, старший науковий співробітник,
доцент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-4194-402X
olaptiev@knu.ua

Браіловський Микола Миколайович
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID: 0000-0002-3148-1148
bk1972@ukr.net

Лаптєва Тетяна Олександрівна
PhD з кібербезпеки, доцентка кафедри кібербезпеки
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
ORCID: 0000-0002-5223-9078
tetiana1986@ukr.net

Лаптєв Сергій Олександрович
PhD з кібербезпеки, асистент кафедри технічного захисту інформації
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0002-7291-1829
salaptiev@gmail.com

ЕФЕКТИВНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЩОДО КІБЕРЗАХИСТУ ДЕРЖАВИ

Анотація. У статті розглянуто метод оцінки ефективності програм кіберзахисту (ПКЗ) з урахуванням кібератак та пов'язаних з ними ризиків, що є продовженням попередніх досліджень авторів. Запропонований підхід ґрунтується на модифікації методу цільового динамічного оцінювання програм на заданому часовому інтервалі, який дозволяє враховувати складну структуру взаємозв'язків між цілями, вплив кібератак, ризиків та запізнення у досягненні результатів. Метод передбачає побудову мережевої ієрархії цілей у три етапи: спочатку здійснюється декомпозиція головної цілі згори донизу шляхом визначення підцілей, що безпосередньо впливають на її досягнення, з визначенням їх типу (кількісні, якісні, визначені, невизначені, кваліфікаційні чи порогові); потім — аналіз знизу вгору для встановлення зворотних зв'язків; на третьому етапі до ієрархії інтегруються моделі кібератак та ризиків. Кібератаки моделюються як спеціальні програми, що негативно впливають на цілі, а ризики — через введення індикаторів у вигляді додаткових цілей. Оцінювання ефективності ПКЗ базується на визначенні ступеня впливу реалізації програм (простих і складних) на досягнення головної цілі. У роботі введено поняття миттєвого показника відносної ефективності, що дозволяє аналізувати динаміку ефективності на різних етапах реалізації. Для обчислення ступеня досягнення цілей використовується ітеративний алгоритм моделювання ієрархії, який враховує нелінійність, зворотні зв'язки та часову залежність параметрів. Особливістю методу є можливість оперативного перерахунку ефективності при зміні структури програм. Метод застосовується для оцінки ефективності напрямків реалізації ПКЗ, множин кібератак і ризиків, а також засобів протидії ним.

Розроблений підхід може використовуватися не лише в сфері кібербезпеки, а й для аналізу складних цільових програм у технічній, економічній та інших галузях.

Ключові слова: кіберзахист, ризики, ієрархія цілей, відносна ефективність, алгоритм, метод, захист інформації.

ВСТУП

Інформація стає одним із найцінніших стратегічних ресурсів, забезпечення кібербезпеки держави та набуває першорядного значення. Зростаюча залежність критично важливих інфраструктур, державних установ, економічних та військових систем від цифрових технологій робить їх уразливими до кібератак, які можуть мати руйнівні наслідки — від масового порушення функціонування систем до втрати конфіденційної інформації та дестабілізації державного управління. У цьому контексті розробка та реалізація ефективних програм кіберзахисту інформації (ПКЗ) стає ключовим напрямом забезпечення національної безпеки. Однак ефективність таких програм не може бути оцінена у відриві від реальних загроз, зокрема кібератак, а також пов'язаних з ними ризиків, які динамічно змінюються під впливом технологічного прогресу, нових тактик атакуючих та еволюції засобів захисту. Тому актуальним є розроблення методологій, що дозволяють комплексно оцінювати ефективність ПКЗ з урахуванням цих чинників [1-3].

Ця стаття є продовженням дослідження, викладеного в роботі [4], і присвячена розробці та викладенню модифікованого методу оцінки загроз від кібератак та ризиків, а також ефективності програм кіберзахисту інформації з урахуванням цих загроз. Запропонований підхід базується на модифікації методу цільового динамічного оцінювання програм на заданому часовому інтервалі, що розроблений у працях [5-7]. Основна відмінність нового підходу полягає в тому, що він враховує не лише позитивний вплив реалізації програм на досягнення стратегічних цілей, але й негативний вплив зовнішніх факторів — зокрема, кібератак і пов'язаних з ними ризиків. Це дозволяє отримати більш реалістичну картину ефективності заходів кіберзахисту, оскільки в умовах постійної загрози навіть добре сплановані програми можуть не досягати очікуваних результатів через дії зловмисників або несподівані події.

Методичні зміни охоплюють як процедуру побудови ієрархії цілей, так і сам спосіб оцінювання показників порівняльної ефективності програм. У традиційних підходах ієрархія цілей часто будується як лінійна або деревоподібна структура з позитивними зв'язками, що відображають підпорядкованість та підтримку цілей. Проте у реальних умовах взаємодія між цілями, проектами та зовнішніми чинниками є значно складнішою: існують зворотні зв'язки, конфліктуючі цілі, негативний вплив (наприклад, відмова системи через атаку) та часові запізнення. Тому запропонований метод розроблено для загального випадку, коли ієрархія має мережеву структуру, містить як позитивні, так і негативні прямі та зворотні зв'язки, а також цілі різних типів — кількісні, якісні, визначені, невизначені, кваліфікаційні та порогові. Особливу увагу приділено врахуванню суміжності цілей (впливу досягнення одних цілей на інші) та часових запізнень у впливі реалізації проектів на досягнення стратегічних цілей, що робить оцінку більш точною та динамічною.

Ключовим елементом методу є інтеграція моделей кібератак та ризиків у загальну ієрархію цілей ПКЗ. Це дозволяє не просто констатувати наявність загроз, а кількісно оцінювати їх вплив на ефективність програм, що, у свою чергу, забезпечує обґрунтованість прийняття управлінських рішень щодо пріоритетів у розподілі ресурсів,

вдосконаленні систем захисту та мінімізації потенційних втрат. Таким чином, стаття пропонує комплексний інструментарій для аналізу та підтримки прийняття рішень у сфері кібербезпеки, який враховує складну взаємодію між захисними заходами, атакуючими діями та невизначеністю зовнішнього середовища.

Постановка проблеми. Основна проблема полягає у тому, що традиційні методи оцінки ефективності програм ґрунтуються на лінійних або деревоподібних ієрархіях цілей із позитивними зв'язками, тоді як реальні системи мають мережеву структуру зі складною взаємодією між цілями, наявністю конфліктів, негативного впливу, ризиків та запізнень. Крім того, відсутність уніфікованого підходу до інтеграції моделей кібератак і ризиків у процес оцінювання унеможливлює комплексну та динамічну оцінку стійкості ПКЗ. Вирішенню цієї проблеми і присвячена дана робота.

Аналіз останніх досліджень і публікацій. Дослідження науково-прикладної проблеми створення методологічного та інструментального забезпечення для комплексного, динамічного та обґрунтованого оцінювання ефективності програм кіберзахисту в умовах дії реальних загроз, що сприяє підвищенню стійкості державної інформаційної інфраструктури, відображена в наукових працях вітчизняних і зарубіжних авторів.

У роботі [4] Розглянуто науково обґрунтовані підходи та методологічні засади оцінки ефективності програм кіберзахисту інформації (ПКЗ) із урахуванням специфіки кібератак, рівня їхньої складності, а також пов'язаних із ними інформаційних, технологічних та організаційних ризиків, що дозволяє забезпечити комплексну та багатофакторну оцінку стійкості захисних механізмів у сучасних умовах цифрової загрози.

Роботи [5–7] є ключові для методів підтримки прийняття рішень, зокрема в умовах невизначеності. Автори пропонують підходи до агрегування експертних даних із врахуванням рівня компетентності експертів, що особливо важливо при оцінці ефективності програм кіберзахисту, де необхідна участь фахівців. Методи, запропоновані в статті, можуть бути інтегровані в системи аналізу ієрархій цілей.

У роботі [8] розглянуто методи кількісної оцінки ризиків у проектах, засновані на інформаційній моделі невизначеності. Автори запропонували формалізовані підходи до виявлення, класифікації та нейтралізації ризиків, що є актуальним для моделювання ризиків у програмах кіберзахисту. Ідеї цієї роботи використані в даній статті при побудові індикаторів ризиків.

Роботи [9,10] присвячені математичним методам прогнозування стохастичних процесів, зокрема в умовах обмеженої інформації. Це важливо для моделювання кібератак, які носять випадковий характер. Методи, зокрема фільтрація та екстраполяція, можуть бути використані для прогнозування моментів реалізації загроз у системах кіберзахисту.

У роботі [11] розглядається розвиток теорії прийняття рішень у 2000–2005 рр. і посилається на ключові дослідження того періоду. У ній розглянуто методи аналізу ієрархій, багатокритеріальну оптимізацію, стохастичні моделі — усе це є основою для розробки методів оцінки ефективності ПКЗ.

У працях В.О. Хорошко та О.А. Лаптєва [5,8,13,15] розглянуто способи та методи оцінки ефективності програм кіберзахисту інформації (ПКЗ) з урахуванням кібератак та пов'язаних із ними ризиків.

Таким чином, літературні джерела, що стосуються теми дослідження, надають достатню наукову базу для розробки та аналізу методів інструментального забезпечення

оцінки ефективності програм кіберзахисту інформації (ПКЗ) з урахуванням кібератак та пов'язаних із ними ризиків

Метою даної статті є підвищення ефективності програм кіберзахисту інформації (ПКЗ) у умовах дії кібератак та пов'язаних з ними ризиків, що є актуальною задачею забезпечення національної кібербезпеки. Для цього треба створити модифікований метод цільового динамічного оцінювання програм на часовому інтервалі, який дозволяє:

– побудувати мережеву ієрархію цілей з урахуванням позитивних і негативних прямих та зворотних зв'язків;

– інтегрувати в цю ієрархію моделі кібератак (як спеціальних шкідливих програм) та ризиків (через введення індикаторів у вигляді додаткових цілей);

– оцінювати відносну ефективність як окремих програм і їхніх сукупностей, так і напрямків реалізації ПКЗ, множин кібератак та засобів протидії їм;

– враховувати часові запізнення, суміжний вплив цілей, різноманітні типи цілей (кількісні, якісні, порогові, кваліфікаційні) та невизначеність у досягненні результатів.

Таким чином, вирішується науково-прикладне завдання створення методологічного та інструментального забезпечення для комплексного, динамічного та обґрунтованого оцінювання ефективності програм кіберзахисту в умовах дії реальних загроз, що сприяє підвищенню стійкості державної інформаційної інфраструктури.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Суттю метода побудови ієрархії цілей ПКЗ з урахуванням кібератак та ризиків полягає у наступному. Побудова ієрархії підцілей здійснюється у три етапи. На перших двох будується ієрархія цілей без урахування кібератак та ризиків, на третьому до ієрархії вводять моделі цих факторів (кібератак та ризиків). При цьому на першому етапі виконується просування зверху униз, а на другому – у зворотному напрямку.

Сутність першої процедури полягає в отримані відповіді на питання: «Досягнення яких підцілей здійснює безпосередній вплив на досягнення головної цілі програми?». Нехай це підцілі S_1, S_2, …, S_n. Відносно будь якої з них поставимо питання: «Чи можливо виразити результат повного досягнення підцілі результатом вимірювання однієї величини (ефектом)?». Якщо – так, то маємо підціль кількісну по входу, інакше – якісну. Якщо підціль – кількісна по входу, то ставиться наступне питання: «Чи достовірно відомо значення ефекту?». Якщо – так, то маємо кількісну по входу визначену підціль, інакше – кількісну по входу невизначеність.

Зараз необхідно отримати відповідь на питання: «Досягнення підцілі позитивно або негативно впливає на досягнення цілі?». Крім визначення множини підцілей, перша процедура передбачає визначення також і типа цілі. Отже необхідно вирішувати проблему: «Чи є можливість виразити умови досягнення цілі (назва цілі) результатом вимірювання деякої однієї реальної величини?». Якщо є позитивна відповідь, то ціль кількісна по входу, у іншому випадку якісна. Якщо ціль кількісна по входу то поставимо перед собою питання: «Чи достовірно відомо значення ресурсу?». Якщо – так, то маємо кількісну по входу визначену ціль, інакше - кількісну по входу невизначену [8].

Зараз розглянемо підціль S_1 і при цьому необхідно отримати відповідь на питання: «Чи є підціль S_1 цілю реалізації якої-небудь програми?». Якщо – так, то подальша декомпозиція підцілі S_1 не потрібна. Якщо – ні, то необхідно поставити таке саме питання, яке відноситься до головної цілі, но тепер замість головної цілі у питанні буде фігурувати підціль S_1. Крім того, при визначенні підцілі для S_1 спочатку спробуємо знайти підціль серед списка цілей, які раніш були названі при аналізі інших цілей. Цей

список може містити і головну ціль програми. За рахунок цього можуть встановлюватись зв'язки між підцілями та цілями.

Спробуємо визначити тип цілі S_1 ставлячи ті самі питання, що відносились до головної цілі. Крім того, поставимо собі питання: «Чи впливає будь-який приріст ступеня підцілі цілі S_1 на ступень її досягнення?». Якщо – так, то маємо кваліфікаційну ціль S_1, інакше, ціль S_1 порогова ($T_1>0$). У останньому випадку спробуємо визначити величину її порога, тобто яка повинна бути ступінь досягнення цілі, щоб це вплинуло на ступень досягнення головної цілі. Повторюючи це процес для усіх підцілей, занесених у список, побудуєм ієрархію підцілей, на досягнення яких впливає реалізація програм ПКЗ інформації. Неважко помітити, що реалізація описаного алгоритму завжди забезпечить включення усіх програм ПКЗ в ієрархію. Но декомпозиція усіх підцілей першого рівня обов'язково завершується якоюсь програмою. Це наслідок того, що у загальному випадку програми ПКЗ інформації можуть відбивати не усі аспекти досягнення головної цілі ПКЗ. Оскільки умовою завершення декомпозиції деякої цілі є збіг якої-небудь її підцілі з цілю програми ПКЗ, то у загальному випадку виявляється хоча б одна підціль першого рівня, декомпозиція якої ніколи не завершиться, оскільки такої програми не має у ієрархії. Щоб алгоритм завершив свою роботу за кінцеву кількість кроків, введемо ще одну умову зупинки його виконання декомпозиції усіх цілей закінчується, якщо тільки ціль будь-якого проєкта співпадає з якою-небудь підцілю. Раніш наведений алгоритм побудови ієрархії цілей щодо відбору найбільш прерогативних програм, які доцільно включати у ПКЗ. Однак, запропонований метод можна використовувати і для визначення найбільш ефективних напрямків реалізації ПКЗ, які доцільно підтримувати задаючи відповіді програми. У цьому випадку ієрархія будується аналогічно, за тим тільки виключенням, що розробник ПКЗ сам визначає достатність ступеня деталізації та припиняє подальшу декомпозицію.

На другому етапі виконання процедури здійснюється просунення знизу угору, полягає у тому, що для кожної підцілі визначаються усі безпосередні цілі, на досягнення яких виявляє безпосередній вплив досягнення аналізуємої підцілі.

На останньому етапі у ієрархію вводяться моделі кібератак та ризиків. У [4] запропонована модель кібератаки у вигляді деякої програми, яка впливає на декілька цілей та, можливо, програм. Щодо встановлення впливу на ці елементи ієрархії будемо послідовно аналізувати усі множини введені у ієрархію на перших двох етапах цілей та програм, та визначим вплив на них відповідної кібератаки, яка є для них загрозою. Відзначимо, що програми, які є моделями кібератак можуть мати підцілі, які служать моделями засобів протидії кібератакам. Вони визначаються так же, як і підцілі звичайних цілей.

Введення моделей ризиків здійснюється наступним чином. Спочатку визначимо фактори ризиків, які повинні бути враховані. Потім у відповідності з [4] будуємо цілі, які виступають як індикатори відповідних ризиків, та визначаються їх параметрами, аналогічно тому як це мало місце щодо основної ієрархії. На останньому кроці встановлюємо зв'язки зовнішніх індикаторів ризиків з елементами побудованої ієрархії (цілей та програм).

Оцінювання відносної ефективності елементів ПКЗ з урахуванням кібератак та ризиків передбачає вирішення таких задач: оцінювання відносної ефективності направленості виконання ПКЗ з урахуванням кібератак та ризиків; відносної ефективності заданої множини кібератак та ризиків; відносної ефективності програм ПКЗ з урахуванням кібератак та ризиків, а також відносної ефективності протидії кібератакам та нейтралізації ризиків.

У основу запропонованого метода покладені дві головні ідеї: використання у якості показників ефективності ступені впливу виконання програми (досягнення цілі) на ступень досягнення головної цілі ПКЗ, та включення у ієрархію ПКЗ програм, які є моделями кібератак або індикаторами ризиків.

Виходячи з цього, викладемо спосіб вирішення вказаних задач оцінки ефективності.

Задача оцінювання відносної ефективності програм на інтервалі часу з урахуванням кібератак та ризиків зводиться до визначення ступеня впливу на досягнення головної цілі виконання оцінюючих програм при наявності цих факторів. Далі будемо використовувати поняття простих (ПР) та складних (СР) програм [14,16]. Простою називається програма, яка розглядається у рамках ПКЗ, як єдине ціле. У той же час складна програма складається з ряду взаємопов'язаних між собою простих програм.

Приватні коефіцієнти впливу підцілей та програм у загальному випадку залежать від часу. Тому ступень досягнення цілей, у тому числі і головної, також залежить від часу. Отже, можна говорити о миттєвих значеннях показників ефективності простих та складних програм.

Визначення 1. Миттєве значення $V_k(t)$ показник по відносної ефективності складної програми CP_k у момент часу t від її реалізації дорівнює:

$$V_k(t) = F\left[D_0(P)_t , D_0(\frac{P}{C\ P_k})_t \right] \quad (1)$$

де P – множина усіх простих програм ПЗК і $D_0(P)_t$ – ступень досягнення головної цілі у момент t при умові включення у ПКЗ усіх простих програм $ПР_i \in P$; $D_0(P\backslash CP_k)_t$ ступень досягнення головної цілі у момент t при умові включення у ПКЗ усіх $ПР_i \in P$, за виключенням простих програм, які входять у складну програму $СР_к$.

Вид функції F не залежить від структури ієрархії і типу цілей та визначається зручністю сприйняття інформації фахівцем, що приймає рішення (ФПР).

Таким чином, СР може бути охарактеризована множинами миттєвих значень її показника відносної ефективності, обчислених, для множини моментів часу на деякому заданому інтервалі θ. При цьому оцінювання множини СР у ході прийняття рішень зводиться до обчислення деякої визначеної ФПР функції θ, яка задана на множені значень показників відносною ефективності програму у момент часу на інтервалі θ. У якості такої функції можуть використовуватись:

$$Q_k(t) = \sup_{0 \le t \le \theta} V_k(t)$$

або

$$Q_k(t) = \int_0^{\theta} V_k(t)^* dt \quad (2)$$

де $V_k(t)^*$ - найкраща у відношенні деякого критерія апроксимації множини миттєвих значень $V_k(t)$ щодо моменту часу з інтервалу $[0,\theta]$.

Крім задачі оцінювання *СР*, виникає задача оцінювання *ПР* у межах заданої *СР*. Тому відносно простої програми CP_i можна говорити о значенні показника V_{ik} його відносної ефективності у межах складної програми CP_k. У загальному випадку $V_{ih} \neq V_{ik}$; $h \neq k$.

Визначення 2. Миттєве значення $V_{ik}(t)$ показника відносної ефективності простої програми $ПР_i$ у складі складної програми CP_k у момент часу t від початку реалізації CP_k дорівнює:

$$V_{ik}(t) = F\left[V_k(t), V_{iGk}(t)\right], \tag{3}$$

де $V_k(t)$ – значення показника відносної ефективності складної програми CP_k у момент часу t;

V_{iGk} – значення у момент часу t показника відносної ефективності складної програми CP_k, який не утримує простої програми $ПР_i$. У загальному випадку маємо $V_{ih}(t) \neq V_{ik}(t)$; $h \neq k$.

Таким чином динамічне оцінювання простої програми $ПР_i \in CP_h$ у ході визначення показника його відносної ефективності на заданому інтервалі часу зводиться до обчислювання показників відносної ефективності двох сигналів програм CP_h та CP_{hi} у деякій множині моментів часу із цього інтервалу. У свою чергу, задача обчислення показника відносної ефективності CP_h зводиться до обчислення у цих моментах часу величин: $D_0(P)_t$ – ступеня досягнення головної цілі у момент t при умові повної реалізації усіх $ПР_i \in P$; $D_0(P \backslash CP_k)_t$ – ступеня досягнення головної цілі у момент часу t при умові повної реалізації усіх $ПР_i \in P$, за виключенням простих програм, які входять у CP_h. Вказані умови, при яких обчислюється ступінь досягнення головної цілі, визначається множиною B аналізуємих програм, які зручно задавати вектором $D_B=\{D_{Br}\}$,r={1, |P|}, ступенів реалізації програм, компоненти якого:

$$D_{BT} = \begin{cases} 1, \textit{якщо } ПР_r \in B; \\ 0, \textit{якщо } ПР_r \notin B; \end{cases} \tag{4}$$

Таким чином, задача обчислення відносної ефективності простих та складних програм зводиться до обчислення у множені моментів часу ступеня досягнення головної цілі при умовах, що ступені реалізації програм $ПР_r \in B \subseteq P$ задані вектором D_B.

Розглянемо спочатку метод оцінювання складності програми у заданий момент часу t. Задача формулюється наступним чином.

Задано момент часу *t* у інтервалі $[0, \theta]$ орієнтований граф ієрархії цілей *H(S,V),* де *S={Sq}, S=(0, m)* – множина вершин, кожна вершина S_q означена функцією $D_q(t)$ ступеня дослідження досягнення цілі [4], для кожної вершини S_q задана множина $S_q=\{S_{qz}\}$ множина сумісних вершин однопопередників; $V=\{V_s\}$, $S=(1, \theta)$ – множина дуг, причому, кожна дуга має вагу (приватний коефіцієнт впливу [1]); вектор D_B визначений виразом (1) у відповідності із значенням у момент часу *t* випадкових процесів, які задають кібератаки та ризики.

Необхідно визначити значення функції $D_0(t)$ ступеня досягнення головної цілі при вимогах, що $\forall S_p \in B \subseteq P \subset S[D_r(t_i) = D_{Br}(t)]$. Визначення компонент вектора B у момент часу t, задающих моделі кібератак та/або ризиків, здійснюється у відповідності із значеннями випадкових процесів, які описують ці фактори, аналогічно тому, як ураховуються вірогідності реалізації решти програм [17,18].

Визначим метод обчислення показника ефективності щодо найбільш загального випадка, коли ієрархія мережева, нелінійна з позитивними та негативними зворотними зв'язками, має як лінійні, так і порогові цілі. Пошук метода побудови аналітичного

виразу, який дозволяє обчислити ступінь досягнення головної цілі, здається безперспективним із-за складності аналітичного опису графа довільної структури. Це погіршується ще і тим, що при практичному використанні такого методу підтримки прийняття рішення виникає необхідність оцінювати ефективність програми відносно різних цілей та оперативно змінювати структуру ієрархії при супроводу системи [11,12]. Тому використовуємо метод вирішення, який базується на моделюванні ієрархії цілей. Моделювання ієрархій цілей здійснюється у відповідності з таким алгоритмом.

Алгоритм.

Крок 1. $\chi = 1; 0 \le q \le m [D_q(t_i)^0 = 0]$, де $D_q(t_i)^0$ – значення функції $D_q(t_i)$ на χ-й ітерації.

Крок 2. $\forall S_p \in B \subseteq P \subset S [D_r(t_i)^\chi = D_{Br}(t)]$

Крок 3. Знайти підмножину $S_u = \{S_q\}$, вершин графа, для яких $D_0(t_i)^\chi \neq D_0(t_i)^{\chi-1}$

Крок 4. Знайти множину S_c вершин графа одноприємників вершин $S_q \in S_u$, використовуючи [1], обчислить значення функцій $D_Q(t_i)^q$ для $S_q \in S_c$.

Крок 5. Якщо $S_0 \in S_c$, то Крок 6, в іншому випадку Крок 7.

Крок 6. Якщо $\left|D_0(t_i)^\chi - D_0(t_i)^{\chi-1}\right| \le \varepsilon$, де ε – припустиме значення похибки обчислення, то Крок 8, інакше $\chi := \chi + 1$

Крок 7. $S_u := S_c$, Крок 4.

Крок 8. Кінець.

Не важко побачити, що при такій процедурі обчислення ступеня досягнення головної цілі при повному виконанні програми P_j повинні обчислюватися ступені досягнення підцілей $S_i \in S^*$, де $S^* = U_j S_j$, $Sj = U_s S_{js}$ де S_{js} – множина підцілей, які входять в q-й шлях у графі ієрархій підцілей ведучий з вершини, визначеної програмою P_j у вершину S_0, визначеної головною цілю ПКЗ.

Визначимо, що у загальному випадку у ієрархіях мережевого типу q>1, може існувати декілька таких шляхів. Це означає, що виконання однієї і тієї ж програми впливає на досягнення декількох підцілей. Досягнення деякої підцілі, як правило, впливає на досягнення не однієї, а декількох цілей. Це і породжує множину шляхів від однієї програми до головної цілі.

Описаний алгоритм виконується N разів, причому кількість повторень залежить від вимагаємої точності обчислень і після цього визначається математичне очікування значення ступеня досягнення головної цілі у момент часу t.

Наступний момент часу t_{i+1}, встановлюється з таких міркувань. Ступінь досягнення головної цілі у той момент однозначно визначається ступенем досягнення усіх підцілей, які знаходяться на шляхах від програм, яким у векторі D_Q відповідають одиниці, та миттєвим значенням їх коефіцієнтів впливу у той момент часу. Оскільки ступені досягнення усіх підцілей, обчислених у момент t, не змінюються на інтервалі t_i - t_{i+1}, то ступінь досягнення головної цілі може змінитися у момент t_{i+1} у порівнянні з моментом t_i, тільки якщо до початку t_{i+1} хоча б у однієї підцілі коефіцієнт впливу замість нуля прийме стаціонарне значення. Тому t_{i+1} будемо визначати з виразу $t_{i+1} = \inf_{j \in T_i^0}(\tau_j)$, де $T_i^0 = (\tau_j \ge t_i)$ – множина значень системних моментів часу, не менших t_i, у яких у ієрархії відбуваються події.

При наявності зворотних зв’язків у мережі підцілей необхідно обчислить ступінь досягнення головної цілі по нескінченної кількості ітерацій, які визначимо виходячи з припустимої точності результатів, тобто з умови [11,12]:

$$\sigma(u+1)=[e_a(u+1)-e_a(u)] \le \varepsilon \quad 1 \qquad (6)$$

$e_a(u+1)$, $e_a(u)$ – значення показників ефективності простої програми P_a, обчислених на $(u+1)$- й та (u)-й ітерацій відповіддю; ε – припустиме значення похибки обчислень.

Вимоги стійкості ітеративного процесу, тобто вимоги, при яких (6) виконується при кінцевому u, визначені у [13,14].

У режимі оцінювання відносної ефективності напрямку виконання ПКЗ з урахуванням кібератак та ризиків компоненти вектора B відповідаючи програмам, які не служать моделями кібератак, вважають рівними нулю, а компоненти, які відповідають моделі кібератак та індикаторам ризиків, визначають способом, який описаний раніше. Після цього визначають показники відносної ефективності кожної з цілей, моделюючих направлення виконання ПКЗ.

Оцінювання відносної ефективності заданої множини ризиків та кібератак, як показано у [4], модель кібератаки – програма, а модель ризика – індикатор ризика, який також є підціль, то режим оцінювання відносної ефективності заданої множини ризиків та кібератак розгляданому раніш режиму оцінки множини програм.

Так як засоби протидії кібератакам та ризикам – програми, то оцінювання відносної ефективності засобів протидії кібератакам та ризикам, аналогічно розглянутому раніш оцінювання програм.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розглянуто метод оцінки ефективності програм кіберзахисту інформації (ПКЗ) з урахуванням кібератак та пов’язаних із ними ризиків. Запропонований підхід є розвитком методу цільового динамічного оцінювання програм на заданому часовому інтервалі та включає модифікацію як процедури побудови ієрархії цілей, так і методу обчислення показників порівняльної ефективності. Метод розроблено для загального випадку, коли ієрархія має мережеву структуру, містить позитивні та негативні прямі й зворотні зв’язки, а також цілі різних типів — кількісні, якісні, визначені, невизначені, порогові та кваліфікаційні. При цьому оцінювання проектів здійснюється з урахуванням суміжності цілей та часових запізнень у їхньому впливі на досягнення головної мети.

Побудова ієрархії цілей ПКЗ здійснюється у три етапи. На першому етапі, рухаючись згори донизу, визначаються підцілі, які безпосередньо впливають на досягнення головної цілі, і встановлюється їхній тип шляхом відповіді на систему питань щодо вимірюваності, визначеності та характеру впливу. Декомпозиція продовжується до тих пір, поки кожна підціль не збігатиметься з ціллю певної програми. На другому етапі, рухаючись знизу вгору, визначаються всі цілі, на які впливає досягнення кожної підцілі, що дозволяє виявити зворотні зв’язки. На третьому етапі до побудованої ієрархії інтегруються моделі кібератак та ризиків. Кібератаки моделюються як спеціальні шкідливі програми, що впливають на певні цілі, а ризики — через введення додаткових цілей-індикаторів, які враховують вплив зовнішніх факторів.

Оцінювання ефективності здійснюється шляхом визначення ступеня впливу реалізації програм на досягнення головної цілі. Розрізняються прості програми (як окремі елементи) та складні програми (як сукупності взаємопов’язаних простих). Запропоновано поняття миттєвого показника відносної ефективності, який дозволяє аналізувати динаміку ефективності на різних етапах реалізації. Для обчислення ступеня досягнення цілей використовується ітеративний алгоритм моделювання ієрархії, який

враховує нелінійність, зворотні зв'язки, часові запізнення та стохастичні фактори, пов'язані з кібератаками та ризиками.

Розроблений метод дозволяє оцінювати ефективність не лише окремих програм, але й напрямків реалізації ПКЗ, множин кібератак, ризиків та засобів протидії їм. Він може бути використаний для підтримки прийняття управлінських рішень у сфері кібербезпеки, зокрема для оптимізації розподілу ресурсів, формування пріоритетів та моніторингу стану захисту. Крім того, технологія є універсальною і може застосовуватися для аналізу складних цільових програм у технічній, економічній та інших галузях, де важливо враховувати динамічні загрози та невизначеність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Brailovskyi, M. M., Khoroshko, V. O., Koziura, V. D., & Blavatska, N. H. (2023). Software for protecting the state against cyberattacks. *Information Protection, 23*(4), 184–191.
5. Laptiev, O. A., Kuzavkov, V. V., & Khoroshko, V. O. (2023). *Systems for detecting covert acoustic information interception devices*. Kyiv: Millennium. ISBN 978-966-8063-76-7.
6. Khoroshko, V. O., Shelest, M. Ye., & Tkach, Yu. M. (2020). Multicriteria evaluation of cybersecurity project effectiveness. *Technical Sciences and Technologies, 1*(19), 141–124.
7. Totsenko, V. H. (2000). Harmonization and aggregation of expert assessments considering competence in group evaluation of alternatives for decision support. *Problems of Control and Informatics, (4),* 128–141. https://doi.org/10.15407/pci2000.04.128
8. Zghurivskyi, M. Z., & Kovalenko, N. I. (2000). Information approach to project risk analysis and management. *Problems of Control and Informatics, (4),* 146–156. https://doi.org/10.15407/pci2000.04.146
9. Novosad, V. P., & Seliverstov, R. H. (2008). *Methodology of expert evaluation*. Kyiv: NAPA.
10. Ivanenko, O. H., & Lapa, V. H. (2000). *Prediction of random processes* (3rd ed., rev.). Kyiv: Naukova Dumka. https://doi.org/10.15407/naukova_dumka.2000.ivanenko
11. Katrenko, A. V., Pasychnyk, V. V., & Pasko, V. P. (2009). *Decision-making theory*. Kyiv: BHV Publishing Group. https://doi.org/10.15407/bhv2009.katrenko
12. Veres, O. M. (2010). *Decision support technologies*. Lviv: Lviv Polytechnic Publishing.
13. Laptiev, O. A., & Khoroshko, V. O. (2024). *Detection, localization, and processing of signals from covert information interception devices*. Kyiv: Millennium.
14. Laptiev, O. A., & Marchenko, V. V. (2025). Using interference to protect information from leakage via radio channel. *Modern Information Protection, (1),* 89–97. https://doi.org/10.31673/2409-7292.2025.013057
15. Khoroshko, V., Khokhlachova, Y., Laptiev, O., & Fowad, A. A. (2025). Mathematical apparatus for finding the optimal configuration of a secure communication network with a specified number of subscribers. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15*(1), 62–66. https://doi.org/10.35784/iapgos.6406
16. Laptiev, O., Laptieva, T., & Brailovskyi, M. (2025). Methods of calculating parameters for detecting signals of covert information acquisition devices. *Cybersecurity: Education, Science, Technology, 4*(28), 575–585. https://doi.org/10.28925/2663-4023.2025.28.812
17. Al-Dalvash, A., Petchenko, M. V., & Laptiev, O. A. (2025). Method for detecting digital radio signals using differential transformation. *Modern Information Protection, (1),* 285–291. https://doi.org/10.31673/2409-7292.2025.014329
18. Kalchuk, I., Laptieva, T., Lukova-Chuiko, N., & Kharkevych, Yu. (2021). Method for building secure data transmission channels using a modified neural network. *Information Technology and Security, 9*(2), 232–243.

Volodymyr Khoroshko
Doctor of Technical Science, Professor,
Professor of the Department of Information Technology Security
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0001-6213-7086
professor_va@ukr.net

Oleksandr Laptiev
Doctor of Technical Science, Senior Researcher
Associate Professor of the Department of Cyber Security and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: 0000-0002-4194-402X
olaptiev@knu.ua

Mykola Brailovskyi
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kiev, Kiev, Ukraine
ORCID: 0000-0002-3148-1148
bk1972@ukr.net

Tetiana Laptieva
PhD in Cybersecurity, Associate Professor of the Department of Cybersecurity
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine
ORCID: 0000-0002-5223-9078
tetiana1986@ukr.net

Serhii Laptiev
PhD in Cybersecurity
Assistant of the Department of Information Technology Security
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0002-7291-1829
salaptiev@gmail.com

EFFICIENCY OF SOFTWARE FOR NATIONAL CYBERSECURITY

Abstract. The article presents a method for assessing the effectiveness of cybersecurity programs (CSP) considering cyberattacks and associated risks, which is a continuation of the authors' previous research. The proposed approach is based on a modification of the target dynamic evaluation method for programs over a specified time interval, enabling the consideration of a complex structure of interrelations between objectives, the impact of cyberattacks, risks, and delays in achieving results. The method involves constructing a network hierarchy of objectives in three stages: first, the main objective is decomposed from top to bottom by identifying sub-objectives that directly influence its achievement, with their types defined (quantitative, qualitative, deterministic, stochastic, qualifying, or threshold); second, a bottom-up analysis is performed to establish feedback loops; third, models of cyberattacks and risks are integrated into the hierarchy. Cyberattacks are modeled as special programs that negatively affect objectives, while risks are accounted for by introducing indicators in the form of additional objectives. The evaluation of CSP effectiveness is based on determining the degree of impact of program implementation (both simple and complex) on the achievement of the main objective. The paper introduces the concept of an instantaneous relative efficiency indicator, which allows analyzing the dynamics of efficiency at different implementation stages. An iterative algorithm for simulating the hierarchy is used to calculate the degree of objective achievement, taking into account nonlinearity, feedback, and time-dependent parameters. A key feature of the method is the ability to promptly recalculate efficiency when program structures change. The method is applied to assess the effectiveness of CSP implementation directions, sets of cyberattacks and risks, as well as countermeasures against them. The developed approach can be used not only in

the field of cybersecurity but also for analyzing complex target programs in technical, economic, and other domains.

Keywords: cybersecurity, risks, goal hierarchy, relative efficiency, algorithm, method, information security

REFERENCES

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Brailovskyi, M. M., Khoroshko, V. O., Koziura, V. D., & Blavatska, N. H. (2023). Software for protecting the state against cyberattacks. *Information Protection, 23*(4), 184–191.
5. Laptiev, O. A., Kuzavkov, V. V., & Khoroshko, V. O. (2023). *Systems for detecting covert acoustic information interception devices*. Kyiv: Millennium. ISBN 978-966-8063-76-7.
6. Khoroshko, V. O., Shelest, M. Ye., & Tkach, Yu. M. (2020). Multicriteria evaluation of cybersecurity project effectiveness. *Technical Sciences and Technologies, 1*(19), 141–124.
7. Totsenko, V. H. (2000). Harmonization and aggregation of expert assessments considering competence in group evaluation of alternatives for decision support. *Problems of Control and Informatics, (4),* 128–141. https://doi.org/10.15407/pci2000.04.128
8. Zghurivskyi, M. Z., & Kovalenko, N. I. (2000). Information approach to project risk analysis and management. *Problems of Control and Informatics, (4),* 146–156. https://doi.org/10.15407/pci2000.04.146
9. Novosad, V. P., & Seliverstov, R. H. (2008). *Methodology of expert evaluation*. Kyiv: NAPA.
10. Ivanenko, O. H., & Lapa, V. H. (2000). *Prediction of random processes* (3rd ed., rev.). Kyiv: Naukova Dumka. https://doi.org/10.15407/naukova_dumka.2000.ivanenko
11. Katrenko, A. V., Pasychnyk, V. V., & Pasko, V. P. (2009). *Decision-making theory*. Kyiv: BHV Publishing Group. https://doi.org/10.15407/bhv2009.katrenko
12. Veres, O. M. (2010). *Decision support technologies*. Lviv: Lviv Polytechnic Publishing.
13. Laptiev, O. A., & Khoroshko, V. O. (2024). *Detection, localization, and processing of signals from covert information interception devices*. Kyiv: Millennium.
14. Laptiev, O. A., & Marchenko, V. V. (2025). Using interference to protect information from leakage via radio channel. *Modern Information Protection, (1),* 89–97. https://doi.org/10.31673/2409-7292.2025.013057
15. Khoroshko, V., Khokhlachova, Y., Laptiev, O., & Fowad, A. A. (2025). Mathematical apparatus for finding the optimal configuration of a secure communication network with a specified number of subscribers. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15*(1), 62–66. https://doi.org/10.35784/iapgos.6406
16. Laptiev, O., Laptieva, T., & Brailovskyi, M. (2025). Methods of calculating parameters for detecting signals of covert information acquisition devices. *Cybersecurity: Education, Science, Technology, 4*(28), 575–585. https://doi.org/10.28925/2663-4023.2025.28.812
17. Al-Dalvash, A., Petchenko, M. V., & Laptiev, O. A. (2025). Method for detecting digital radio signals using differential transformation. *Modern Information Protection, (1),* 285–291. https://doi.org/10.31673/2409-7292.2025.014329
18. Kalchuk, I., Laptieva, T., Lukova-Chuiko, N., & Kharkevych, Yu. (2021). Method for building secure data transmission channels using a modified neural network. *Information Technology and Security, 9*(2), 232–243.