[28] Chose, P., Joux, A., & Mitton, M. (2002). Fast correlation attacks: An algorithmic point of view. In Advances in Cryptology – EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28-May 2, 2002 Proceedings 21 (pp. 209-221). Springer Berlin Heidelberg.
[29] ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation URL: https://www.iso.org/standard/54945.html.
[30] ISO/IEC 18032:2020 Information security – Prime number generation. URL: https://www.iso.org/standard/72009.html.
[31] ДСТУ ISO/IEC 19790:2015 Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (ISO/IEC 19790:2012, IDT). URL: http://shop.uas.org.ua/ua/informacijni-tehnologii-metodi-zahistu-vimogi-bezpeki-do-kriptografichnih-moduliv.html.
[32] NIST SP 800-22 Version 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; NIST: Gaithersburg, MD, USA, (2010); p. 131. Available online: https:// nvlpubs.nist.gov / nistpubs / Legacy/SP/ nistspecialpublication800-22r1a.pdf (accessed on 20 April 2023).
[33] Min, Lequan et al. "Analysis of FIPS 140-2 Test and Chaos-Based Pseudorandom Number Generator." (2013).

ANALYSIS OF THREATS TO GENERATORS OF PSEUDO-RANDOM NUMBERS AND PSEUDO-RANDOM SEQUENCES AND PROTECTION MEASURES

In the modern digital world with diverse applications, including cryptography, cybersecurity, and data protection, the issue of building reliable and secure pseudorandom number and sequence generators has become particularly significant. These generators create numerical sequences that appear random but are, in fact, deterministic and possess a certain structure, making them valuable in various fields. They are used for generating secret keys, ensuring confidentiality, data integrity, and transaction security, so their security is critical for applications that employ such generators. However, as the popularity and scope of pseudorandom number generators and pseudorandom sequence generators grow, so does their vulnerability to different types of attacks. Attacks on these generators can lead to the exposure of secret parameters and the compromise of security systems. Malicious actors and hackers seek various vulnerabilities in the methods and algorithms used to construct such generators to partially or fully disclose their operational principles. In this work, based on a thorough analysis of scientific publications by experts involved in the development, research, evaluation of quality, and application of pseudorandom number and sequence generators, the main vulnerabilities of these generators have been identified and described. Different types of attacks have been classified and described, and their impact on these generators has been determined. Security recommendations have been provided, and standards and testing methods have been identified to enhance the reliability, protection, and mitigation of vulnerabilities of such generators.
Keywords: generators of pseudo-random numbers, generators of pseudo-random sequences, cyber security, generation, vulnerabilities, attacks, quality assessment.

Хомік Марія Анатоліївна, студентка 3-го курсу, спеціальності «Кібербезпека» Національного університету «Львівська політехніка».
Mariia Khomik, A third-year student the Department of Information Security, National University "Lviv Polytechnic".
E-mail: mariia.khomik.kb.2021@lpnu.ua.
Orcid ID: 0009-0004-6031-5618.

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».
Oleh Harasymchuk, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".
E-mail: oleh.i.harasymchuk@lpnu.ua.
Orcid ID: 0000-0002-8742-8872.

DOI: 10.18372/2410-7840.25.18223
УДК 004.621.5

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЩОДО КІБЕРЗАХИСТУ ДЕРЖАВИ ВІД КІБЕРАТАК

Наталія Блавацька, Микола Браіловський, Валерій Козюра, Володимир Хорошко

Захист об'єктів критичної інфраструктури держави від кібератак, тим більше в умовах бойових дій, вимагає від державних органів вжити ефективних заходів кіберзахисту. В основі таких заходів лежить розробка державних цільових програм кіберзахисту. При формуванні вимог до сучасних систем кіберзахисту

необхідно вирішити ряд завдань, до основних з яких відносяться визначення характеристик впливу кібератак на системи кіберзахисту, кількісних показників ефективності систем захисту реалізації кіберзагроз та оптимального розподілу обмежених ресурсів на реалізацію ефективного кіберзахисту. На основі модифікації відомих методів цільової оцінки альтернатив у роботі розробляється метод підтримки прийняття рішень при формуванні комплексних цільових програм кіберзахисту об'єктів критичної інфраструктури в умовах реалізації противником кібератак, різних загроз та ризиків. Основна ідея запропонованого підходу до аналізу впливу кібератак при виконанні програми з кіберзахисту є у тому, що події, які сприяють кібератакам, розглядаються як складова частина системи кіберзахисту, тобто як вплив зовнішнього середовища. Тому такі моделі кібератак включають у ієрархію цілей програми кіберзахисту, установлюються їх зв'язки з іншими системами та цілями державних цільових програм. Ефективність таких програм оцінюється при умові наявності кібератак з урахуванням їх ймовірних характеристик. Запропоновані моделі кібератак та ризиків. Моделлю кібератаки є проект програми, що включається у ієрархію цілей комплексної програми, яка описується степенем та вірогідністю реалізації. Модель ризика будується з двох компонентів: фактора ризика, який описується випадковим процесом, та деякою фіктивною ціллю – індикатором ризику.

***Ключові слова**: кіберзагроза, кібератака, цільова програма, система кіберзахисту, програма кіберзахисту, модель кібератаки, модель ризику.*

ВСТУП

При розробці вимог до систем кібернетичного захисту (СКЗ) держави слід враховувати виникнення кібератак, загроз та ризиків, аналізувати їх вплив і на цієї основі передбачати міри щодо їх відбиття.

При формулюванні вимог з урахуванням кібератак виникають наступні задачі:

- визначення кількісних характеристик кібервпливу на ефективність СКЗ;
- визначення кількісних показників відносної ефективності СКЗ при наявності кібератак;
- розподіл ресурсів між системою відбиття кібератак і системою , яка має створювальну спрямованість.

Відомі методи вирішення першої задачі передбачають ідентифікацію загроз і кібератак (кількісний аналіз) [1], а також оцінювання імовірностей та розмірів можливого збитку (кількісний аналіз) [2]. Однак при цьому задача оцінки ефективності захисту з урахуванням кібератак не вирішується та залишається як уділ особи, яка приймає рішення (ОПР). Більш того, визначення збитку у абсолютному вимірі дуже часто не можливо для складних систем та СКЗ.

Метод вирішення задачі відносної ефективності кіберзахисту при наявності кібератак природно розробляється на основі методів розв'язання даної задачі без урахування цих факторів. Найбільш розповсюдженими у теперішний час є мультікритеріальні методи оцінки [3, 4]. Область їх застосування обмежується, принаймні, двома необхідними умовами, яким повинна задовольняти конкретна задача.

Перша умова – наявність великої кількості критеріїв, але за кожним з них необхідно оцінити кожну альтернативу.

Друга умова – здатність ОПР оцінювати тим або іншим образом кожну альтернативу за кожним критерієм, тобто повністю розібратися у проблемі [5].

Перша умова у більшості випадків формування складних СКЗ не виконується, тому що існує суттєва різниця природи підсистем захисту, які входять до їх складу. Виконання другої умови проблематично, коли вибір найкращої альтернативи з кількох десятків або ранжування такої кількості альтернатив потребує обліку їх оцінок за декілька десятків взаємопов'язаних критеріїв. Така ситуація має місце при прийнятті рішення щодо формування складних комплексних цільових програм державного масштабу, програм побудови СКЗ та систем захисту інформації банків, корпорацій та державних підприємств.

Тому методи підтримки прийняття рішень при формуванні комплексних цільових програм по кіберзахисту в умовах кібератак, різних загроз і ризиків будемо розробляти шляхом модифікації методів цільової оцінки альтернатив [6]. При підтримки рішення по розробці таких програм з кіберзахисту відносна ефективність захисту повинна оцінюватись як функція часу, яка задана на інтервалі проектування [6]. Тому можливість урахування фактора часу при оцінці програм з кіберзахисту

принципова щодо вирішення задач підтримки рішення такого роду.

Основна ідея запропонованого підходу до аналізу впливу кібератак при виконанні програми з кіберзахисту (ПКЗ) є у тому, що події, які сприяють кібератакам, розглядаються як складова частина СКЗ, тобто як вплив зовнішнього середовища. Тому такі моделі кібератак включають у ієрархію цілей ПКЗ [7], установлюються їх зв'язки з іншими системами та цілями ПКЗ. Таким чином, кожна з цих моделей кібератак має хоча б одну ціль або програму, на розгляд якої (степінь виконання яких) вона виявляє безпосередній вплив. Відповідно [7], визначимо такі цілі (програми) як визначальні над цілями моделі кібератак. При цьому вплив кібератак, як й інших ПКЗ, оцінюється як вплив на розгляд головної мети програми.

Ефективність ПКЗ оцінюється при умові наявності кібератак з урахуванням їх ймовірних характеристик. Такий підхід дає можливість розподілити ресурси на відбиття кібератак на рівні з розподілом ресурсів на програми, які являють собою суть ПКЗ.

Для вирішення запропонованого підходу необхідно розв'язати ряд задач. Перша пов'язана з розробкою математичних моделей кібератак, які дозволять включити події, вичліняючих кібератаки в ієрархію цілей ПКЗ. Суть другої задачі складається у розробці кількісної оцінки кібератаки.

ОСНОВНА ЧАСТИНА

Кібератаки можна розподілити на зовнішні та внутрішні, які діють на СКЗ [8, 9]. Аналіз кібератак дозволяє виявити деякі властивості, які характеризують це поняття.

По-перше, слід відзначити, що кібератака – це наслідок події, яка полягає у виникненні ситуації, що впливає на виконання ПКЗ. Однак кібератака є результатом діяльності певної групи людей у відміни від ризиків (атак), які в основному є слідством випадкової події.

По-друге, інтенсивність впливу кібератаки на виконання ПКЗ – випадкова і змінюється у часі.

Загальним щодо поняття «кібератаки» є впливом зовнішнього середовища на виконання ПКЗ і то, що вони – наслідок її впливу на виконання ПКЗ своїх функцій.

Визначення 1. Загроза впливає на ефективність ПКЗ станом середи, у якої виконується комплексна цільова програма. Крім того, можна зробити висновок щодо існування засобів відбиття кібератаки, які можуть впливати на рівень її кіберзагрози. З цього виходить можливість побудови моделі кібератаки, яка являє собою деяку ПКЗ, причому існує хоча б одна програма або мета, рівень досягнення яких залежить від рівня виконання моделі кібератак (МКА). Крім того, МКА може мати у якості підпрограм інші програми, які впливають на її ефективність, тобто міри відбиття кібератаки.

Таким чином, модель кібератаки має усі властивості ПКЗ з деякими особливостями, що розглядаються у подальшому.

Встановимо у відповідність кібератаці Z_i деяке число $0 \le D \le 1$, яке називається степенем реалізації кібератаки, причому $D = 0$ при повної відсутності кібератаки та $D = 1$ при максимально можливому її проявленню. Крім того, будемо характеризувати кібератаку Z_i імовірністю $p_i(t)$ її реалізації у момент часу t. Цю величину повинні визначити експерти за вимогою групових методів експертного оцінювання [10].

Визначення 2. Частинний коефіцієнт W_{ij} впливу кібератаки Z_i на досягнення її безпосередньої підцілі S_j (степінь виконання програми P_j) є приріст степені досягнення підцілі S_j, отриманий в наслідок повної реалізації кібератаки Z_i.

У подальшому, якщо це не викликає різні поняття, то будемо використовувати термін підцілі щодо забезпечення як цілі, на степінь досягнення якої безпосередньо впливає модель кібератаки, так і на програму, на степінь виконання якої впливає кібератака.

Для більш адекватного опису задач підтримки рішень відносно комплексного цільового планування з урахуванням кібератак доцільно враховувати зміни у часі та їх впливи. Тому у подальшому будемо говорити о миттєвих значеннях t у часі коефіцієнта впливу $W_{ih}(t)$ кібератаки Z_i по досягнення її безпосередньої підцілі S_h [11], яке визначається з виразу:

$$W_{ih}(t) = \begin{cases} 0, & \text{якщо } t < \tau_{ih}; \\ y(w_{ih}, t), & \text{інакше,} \end{cases} \quad (1)$$

де w_{ih} – стаціонарне значення коефіцієнта впливу кібератаки Z_i на безпосередньо підціль S_h; τ_{ih} – експертна оцінка затримки впливу кібератаки Z_i на підціль S_h; y – поліноміальна функція, що описує зміни коефіцієнта впливу у часі.

Оскільки достовірна інформація відносно точності експертних оцінок коефіцієнтів полінома $y(w_{ih}, t)$ відсутня, поліном у виразу (1) вважаємо стаціонарним $y(w_{ih}, t) = w_{ih}$, тобто його величина визначається експертами [10, 11].

Стаціонарні значення коефіцієнтів впливу $w_{ih} \in w_h, i = \overline{1, n_h}$, безпосередніх підцілей підцілі S_h, серед яких можуть бути кібератаки, які задовольняють умові $\sum_{i=1}^{n_h} |w_{ih}| = 1$.

В загальному випадку кібератак Z_i є менш споріднена підціль кількох підцілей $S_1, S_2, \cdots, S_h, \cdots, S_r$, причому будь-яка підціль S_h має деяку множину $S_h = \{S_{hk}\}$ альтернативних підмножин сумісних підцілей, $S_{hk} \cap S_{hl} \neq \emptyset$, $k \neq l$. Тому можливий випадок, коли $s_l \in S_{hk}, s_l \in S_{hl}, k \neq l$, і одна і таж кібератака Z_i буде мати різні стаціонарні значення W_{ihk}, W_{ihl} коефіцієнта впливу на одну і ту ж її безпосередню підціль S_h, які вирахувані для різних альтернативних підмножин S_{hk}, S_{hl} сумісних підцілей.

Якщо досягнення пілцілі S_i сприяє досягнення її безпосередньої підцілі S_h, то її стаціонарний коефіцієнт впливу $W_{ihk} > 0$, інакше $W_{ihk} < 0$. З змісту поняття кібератак витікає, що часткові коефіцієнти впливу програм, які є моделями відповідних кібератак, від'ємні.

Відметемо, що напочатку процесу визначення стаціонарні коефіцієнти впливу підцілей ієрархій повинні бути перетворені таким чином, щоб для усіх підцілей вони були додатними. Це досягається заміною підцілей, які негативно впливають на відповідні підцілі, їх логічними інверсіями.

Першою характеристикою, яка визначає тип кібератаки, є спосіб вираження умов та наслідків її реалізації. Якщо вимоги реалізації кібератаки можна виразити результатом вимірювання деякої однієї конкретної величини – ресурса, то тоді кібератака має назву кількісної по входу, інакше – якісної [12].

Оскільки вплив моделі кібератаки на досягнення їх безпосередніх підцілей негативний, то щодо найгіршого випадку степінь їх виконання при відсутності комплексованого впливу приймається рівної 1. При цьому ресурс визначається як кількісний вираз умов компенсації кібератаки, яка призводить до того, що степінь виконання моделі кібератаки буде рівнятися нулю.

Якщо значення ресурсу кількісне по входу кібератаки і відомо, то будемо її називати «кількісною по входу визначеною». Значення ресурсу такої кібератаки однозначно визначається експертами при побудові ієрархії цілей. Якщо ж значень її ресурсів вірогідно не відомо, то таку кібератаку будемо називати «кількісною по входу невизначеною». Для таких кібератак визначаються погоджувальними узагальненими експертними оцінками кількості потрібних ресурсів. Методи її визначення наведені в [1, 6, 8].

Так як модель кібератаки завжди є безпосередньою підцілю будь-якої цілі або програми, вона характеризується результатом її виконання. Якщо результат повного впливу кібератаки можна виразити ефектом, тобто результатом деякої однієї величини, то кібератаку називають кількісною по входу, а у протилежному випадку – якісною по входу. Тобто ефект від використання моделі кібератаки можна експертно оцінити збитками у грошовому вимірі.

Визначення 3. Безпосередні підцілі S_i та S_j, у тому числі і кібератаки деякої підцілі S_s, називаються спільними, якщо досягнення однієї підцілі не виключається можливим або доцільним досягнення другої, та несумісними у протилежному випадку.

Зрозуміло, що при визначенні степені досягнення підцілі повинно враховуватись ефект від досягнення тільки множини її сумісних цілей. Так як кібератака діє незалежно від виконавців СКЗ, слід враховувати її сумісність з кожною із підцілей. Тому модель кібератаки входить в кожну підмножину сумісних підцілей тієї підцілі, на досягнення якої безпосередньо впливає кібератака.

Миттєве значення $D_h(t)$ степені реалізації кібератаки Z_h у мить часу t визначається наступним чином:

$$D_h(t) = \begin{cases} 0, \text{ якщо } \sup\limits_k \sum\limits_i W_{ihk}(t)D_i(t) < T_h; \\ T_h, \text{ якщо } \sup\limits_k \sum\limits_i W_{ihk}(t)D_i(t) = T_h; \\ f\left(\sup\limits_k \sum\limits_i W_{ihk}(t)D_i(t)\right), \\ \quad \text{якщо } T_h < \sup\limits_k \sum\limits_i W_{ihk}(t)D_i(t) < 1 - \sum\left|W_{shk}^{(-)}(t)\right|; \\ 1, \text{ якщо } \left[1 - \sum\left|W_{shk}^{(-)}(t)\right|\right] \le \sup\limits_k \sum\limits_i W_{ihk}(t)D_i(t) \le 1, \end{cases} \quad (2)$$

де T_h – це поріг загрози кібератаки Z_h; $f\left(\sup\limits_k \sum_i W_{ihk}(t)D_i(t)\right)$ – функція степені реалізації загрози кібератаки Z_h; k – номер підмножини S_{hk} сумісних безпосередніх підцілей загрози кібератаки Z_h; i – номера підцілей $s_i \in S_{hk}$; $W_{ihk}(t)$ – миттєве значення частинного коефіцієнта впливу підцілей $s_i \in S_{hk}$ до досягнення загрози кібератаки Z_h, обраховане при умові, що підціль s_i розглядається як елемент підмножини S_{hk} сумісних безпосередніх підцілей загрози кібератаки Z_h; $D_i(t)$ – миттєве значення степені досягнення підцілі s_i у момент часу t; $W_{shk}^{(-)}(t)$ – миттєве значення частинного коефіцієнта впливу підцілі $s_s \in S_{hk}$ від'ємного впливу на Z_h.

Важливі частинні випадки загроз кібератак – квазілінійні та порогові загрози [11, 13].

Степінь D_j виконання квазілінійної моделі кібератаки Z_j визначається виразом:

$$D_j = \begin{cases} \sup\limits_h \sum\limits_q W_{qhj}D_{qhj}, \text{ якщо } \sup\limits_h \sum\limits_q W_{qhj}D_{qhj} \le 1; \\ 1, \text{ якщо } \sup\limits_h \sum\limits_q W_{qhj}D_{qhj} > 1, \end{cases}$$

де h – номер підмножини S_{hj} сумісних безпосередніх підцілей моделі кібератаки Z_j; q – номера підцілей $s_{qhj} \in S_{hj}$; W_{qhj} – частинний коефіцієнт впливу підцілі $s_{qhj} \in S_{hj}$ на досягнення загрози кібератаки Z_j.

Вираз щодо обчислення D_i досягнення порогової загрози кібератаки Z_i має вигляд:

$$D_i = \begin{cases} 1, \text{ якщо } \sup\limits_h \sum\limits_q W_{qhj}D_{qhj} \ge \left|1 - \sum\limits_{j \in J_i^-} w_j\right|; \\ 0, \text{ інакше,} \end{cases}$$

де J_i^- – множина номерів підцілей загроз кібератак Z_i з від'ємним впливом.

Поняття ризик характеризується невизначеністю, пов'язане з можливістю виникнення у ході реалізації програми з кіберзахисту державних об'єктів та наслідків від кібератак [14].

Інакше кажучи, ризик є наслідком випадкових подій, що полягають у виникненні ситуації, які впливають на функціонування СКЗ. У більш загальній трактовці ці події – наслідок впливу на СКЗ зовнішнього, тобто усього того, що непідвласне СКЗ [12, 13].

Таким чином, під ризиком будемо розуміти наслідок випадкової події, викликаний зовнішніми відносно СКЗ факторами, який складається у виникненні ситуації, що впливає на виконання кіберзахисту.

Оскільки ризик є наслідком випадкової події, яка небудь відбудеться або ні, то в залежності від того, є розробник СКЗ оптимістом або песимістом, суть подій, які викликають ризик, можуть сформулювати у одному випадку так, що його виникнення викликає негативний вплив на функціонування кіберзахисту, або так, що він буде мати позитивний вплив.

В залежності від природи події, яка викликає ризик, розрізняють: техніко-технологічні, фінансові, соціальні, політичні, екологічні ризики учасників програми (виконавців створення СКЗ), ризики обставин невизначеної сили (форс-мажор), специфічні ризики [14, 15]. При цьому одна і таж подія може викликати ризики, які мають зовсім різні наслідки щодо виконання різних операцій з кіберзахисту.

Прикладом може бути такий вплив зовнішнього середовища, як різке коливання температури цього середовища h. Випадкові події при $h < h_{\min}$ викликають відказ або зміну параметрів апаратури при зниженні температури, що дозволяє несанкціоновано отримати інформацію, що захищається. При $h > h_{\max}$ також має місце ризик відказу або зміни параметрів апаратури щодо перегріва, що дозволяє проникнути на охоронну територію. При $h_{\min} \le h \le h_{\max}$ мають місце нормальні умови. Таким чином, розглянуті випадкові події утворюють повну групу, тому вини, як викликані цими ризики, полярно сумісні [12].

Приклад свідчить, що ризики повинні оцінюватись, виходячи з системного підходу, з урахуванням цілі кіберзахисту, самої СКЗ та її структури.

Отже, сформулюємо деякі поняття.

Визначення 4. Фактором ризику Φ щодо СКЗ P називається випадковий процес $\varphi_\Phi(t)$, такий, що:

$$\exists p_i \in P[\nu(p_i)\varphi_\Phi(t) \neq \nu(p_i)\overline{\varphi_\Phi}],$$

де $\nu(p_i)\varphi_\Phi(t) \neq \nu(p_i)\overline{\varphi_\Phi}$ – відносна ефективність програми $p_i \in P$ з урахуванням фактора ризику $\varphi_\Phi(t)$ та без його урахування відповідно.

Визначення 5. Індикатором ризику Φ є фіктивна ціль S_Φ. єдиною підцілью якої є фактор ризику Φ.

Повертаючись до розгляду прикладу, відмітимо, що фактор ризику зміни температурних характеристик навколишнього середовища, є підціль щодо таких індикаторів ризику, як S_{Φ_1} – зміна характеристик СКЗ при зниженої температурі; S_{Φ_2} – зміна характеристик СКЗ при підвищеної температурі.

Підцілі S_{Φ_1} та S_{Φ_2} – індикатори ризику, повністю описуються функціями степені досягнення цілі. В загальному випадку миттєво значення $D_h(t)$ степені досягнення безпосередньої підцілі S_h у мить часу t визначається виразом (2).

При заданої функції степені досягнення цілі – індикатора ризику, необхідно враховувати такі особливості:

1. Оскільки пороги цілей задовольняють вимогі $0 \leq T_h \leq 1$ [6, 7], то значення випадкового процесу $\varphi_\Phi(t)$, що задають фактор ризику Φ, повинно також задовольняти вимогі $0 \leq \varphi_\Phi(t) \leq 1$;

2. Якщо $[\partial D(S_{\Phi_1})/\partial\varphi_\Phi(t)] < 0$ (як це має місце щодо приклада ризика при зниженої температурі навколишнього середовища), а у якості фактора ризику щодо цілі S_{Φ_1}, є індикатором цього ризику, необхідно брати $[1 - \varphi_\Phi(t)]$, замість $\varphi_\Phi(t)$.

Таким чином, моделі ризиків, які обумовлені рівнем h температури навколишнього середовища, наступні:

а) фактори ризика $\varphi_\Phi^{(1)}(t) = h(t)/\ h_{\max}$; $\varphi_\Phi^{(2)}(t) = 1 - h(t)/h_{\max}$;

б) індикатор ризику зниженої температури – ціль S_{Φ_1} з порогом $T_{S_{\Phi_1}} = h_{min}/h_{\max}$, а підціль – фактор ризика $\varphi_\Phi^{(2)}(t)$ з частковим коефіцієнтом впливу, який рівняється 1;

в) індикатор ризику підвищеної температури S_{Φ_2} з порогом $T_{S_{\Phi_2}} = 1$, а підціль – фактор ризика $\varphi_\Phi^{(1)}(t)$ з частковим коефіцієнтом впливу, який дорівнює 1.

Для більш детального опису ризиків, які пов'язані з фактором ризика температурних коливань навколишнього середовища можна внести декілька індикаторів ризику, причому для любого з цих сформованих цілій відповідає своє значення порога.

ВИСНОВКИ

Запропонований підхід до підтримки прийняття рішень при формуванні комплексних цільових програм з урахуванням кібератак та ризиків. Під кібератакою, у даному випадку, розуміється вплив на ефективність системи зовнішнього середовища (як природних впливів, так і створених), в якої функціонує комплексна цільова програма.

При цьому ризик визначений як наслідок випадкової події, викликаної впливом зовнішніх відносно СКЗ факторів, які стоять у виникненні ситуації, що впливає на виконання системою кіберзахисту своїх функціональних обов'язків.

Запропоновані також моделі кібератак та ризиків. Моделлю кібератаки є проект програми, що включається у ієрархію цілей комплексної програми, яка описується степенем та вірогідністю реалізації. Модель ризика будується з двох компонентів: фактора ризика, який описується випадковим процесом, та деякою фіктивною ціллю, називаємої індикатором ризику, єдиною підціллю якої є фактор ризику. Ці компоненти включаються у граф, який описує ієрархію цілей комплексної програми, та використовується для визначення відносної ефективності її програми з урахуванням кібератак та ризиків.

ЛІТЕРАТУРА

[1] Капустян М.В. Качественная оптимизация информационных структур корпоративных сетей / М.В. Капустян, В.А. Кудинов, Л.Т. Пархуць, В.А. Хорошко // Вісник ДУІКТ, т. 5, № 3, 2007. С. 290-300.

[2] Капустян М.В. Кількісна оптимізація інформаційних структур корпоративних мереж / М.В. Капустян, В.А. Кудінов, Л.Т. Пархуць, В.О. Хорошко //

Комп'ютерні технології друкарства, Зб. наук. праць. Львів, № 16, 2006. С. 24-33.
[3] Герасимов Б.М. Системы поддержки принятия решений: проектирование применение, оценка эффективности / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. К.: Изд. центр НАДУ, 2004. 319 с.
[4] Тарасов В.А. Интеллектуальные системы поддержки принятия решений. Теория, синтез, эффективность / В.А. Тарасов, Б.М. Герасимов, И.А. Левин, В.А. Корнейчук. К.: МАКНС, 2007. 336 с.
[5] Новосад В.П. Методологія експертного оцінювання / В.П. Новосад, Р.Г. Селіверстов. К.: НАДУ, 2008. 48 с.
[6] Тоценко В.Г. Согласование и агрегация оценок экспертов с учетом их компетенции при групповом оценивании альтернатив для поддержки принятия решений / В.Г. Тоценко // Проблемы управления и информатики, № 4, 2000. С. 128-141.
[7] Хорошко В.О. Багатокритеріальна оцінка ефективності проектів із забезпечення кібербезпеки / В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач // Технічні науки та технології, № 1 (19) 2020. С. 114-124.
[8] Катренко А.В. Теорія прийняття рішень / А.В. Катренко, В. .В. Пасічник, В.П. Пасько. К.: Вид. група BHV, 2009. 448 с.
[9] Катренко А,В. Прийняття рішень: теорія та практика : підручник / А.В. Катренко, В.В. Пасічник. Львів: «Новий Світ – 2000», 2020. 447 с.
[10] Верес О.М. Технології підтримання прийняття рішень / О.М. Верес. Львів: Вид. Львівської політехніки, 20210. 252 с.
[11] Баранов В.Л. Відновлення та оптимізація інформації в системах прийняття рішень / В.Л. Баранов, М.М. Браіловський, А.А. Засядько та інші. К.: Вид. ДУІКТ, 2009. 134 с.
[12] Козюра В.Д. Процеси та технології в інформаційних системах / В.Д. Козюра, Л.М. Скачек, Ю.М. Ткач та інші. Ніжин: ТПК «Орхідея», 2020. 278 с.
[13] Dubois D., Prade H. Fuzzy sets and systems. Theory and Applications. New York? Acad. Press, 1998. 420 p.
[14] Корнійчук М.Т. Ризик і безпека: кореляція категорій / М.Т. Корнійчук, В.О. Хорошко, Д.В. Чирков // Захист інформації, Спец. випуск, 2008. С. 15-21.
[15] Зибін С.В. Підтримка прийняття рішень при формуванні програм безпеки держави. Моделі загроз і ризиків / С.В. Зибін, В.О. Хорошко // Інформатика та математичні методи в моделюванні, т. 5, № 1, 2015. С. 77-84.

SOFTWARE FOR CYBER PROTECTION OF THE STATE AGAINST CYBER ATTACKS

The protection of the state's critical infrastructure objects from cyber-attacks, especially in the conditions of hostilities, requires state bodies to take effective cyber protection measures. The basis of such measures is the development of state targeted cyber protection programs. When forming requirements for modern cyber protection systems, a number of tasks must be solved, the main ones of which include determining the characteristics of the impact of cyber-attacks on cyber protection systems, quantitative indicators of the effectiveness of cyber threat protection systems, and the optimal allocation of limited resources for the implementation of effective cyber protection. Based on the modification of known methods of target assessment of alternatives, the work develops a method of supporting decision-making in the formation of complex target programs of cyber protection of critical infrastructure objects in the conditions of the enemy's implementation of cyber-attacks, various threats and risks. The main idea of the proposed approach to the analysis of the impact of cyber-attacks when implementing a cyber-defense program is that the events that contribute to cyber-attacks are considered as an integral part of the cyber-defense system, that is, as an influence of the external environment. Therefore, such models of cyberattacks are included in the hierarchy of goals of the cyber defense program, their connections with other systems and goals of state target programs are established. The effectiveness of such programs is evaluated in the presence of cyber-attacks, considering their probable characteristics. Proposed models of cyber-attacks and risks. A model of a cyberattack is a program project, which is included in the hierarchy of goals of a comprehensive program, which is described by the degree and probability of implementation. The risk model is built from two components: a risk factor, which is described by a random process, and some fictitious target – a risk indicator.

Keywords: cyber threat, cyber-attack, target program, cyber defense system, cyber defense program, cyber-attack model, risk model.

Блавацька Наталія Миколаївна, к.т.н., доцент, доцент кафедри УІАЗ ОСД центру стратегічних комунікацій Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України.
Nataliya Blavatska, Ph.D., associate professor, associate professor of the UIAZ Department of the Center for Strategic Communications of the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security of Ukraine.
E-mail: blavats1971@gmail.com.
Orcid ID: 0000-0003-2247-8008.

Браіловський Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і захисту інформації Київського національного університету імені Тараса Шевченка.
Mykola Brailovskyi, PhD in Engineering Science, Associate Professor, Associate Professor of department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

Козюра Валерій Дмитрович, к.т.н., доцент, доцент кафедри ТЗІ центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України.
Valeriy Kozura, Ph.D., associate professor, associate professor of the Department of Technical and Scientific Research of the Cyber Security Center of the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security of Ukraine.
E-mail: kozval1948@gmail.com.
Orcid ID: 0000-0002-4769-448X.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

DOI: 10.18372/2410-7840.25.18224
УДК 336.71:004.056

МОДЕЛІ БЕЗПЕКИ СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМ

Станіслав Мілевський

Об'єктом дослідження є процес побудови многоконтурних систем захисту елементів інфраструктури соціокіберфізичних систем на основі модифікації моделі Лотки-Вольтерию У статті подано формування моделей безпеки соціокіберфізичних системах на основі моделі Лотки-Вольтери, що дозволяє визначити превентивні заходи системи безпеки проти цільових (змішаних) атак з комплексуванням з методами соціальної інженерії та можливістю ознак гібридності та синергізму. Такий підхід дозволяє на основі вихідних даних о соціополітичної (економічної) складової визначити можливість впливу на загальну думку як окремого соціуму, так й окремих вікових груп. Крім цього, визначення ознак гібридності та синергізму кіберзагроз у основних складових соціокіберфізичних систем: соціальних мережах, хмарі та фізичної складової дозволяє визначити основні принципи побудови многоконтурних систем безпеки з урахуванням на кожної платформі системи зовнішнього та внутрішнього контуру безпеки. Для формування многоконтурних систем захисту інформації соціокіберфізичних систем враховуються можливі сценарії реалізації цільових атак та їх направленість. А також можливість впливу на соціопсихологічний стан за рахунок соціальних мереж формальних та неформальних "лідерів" соціума.

***Ключові слова**: соціокіберфізичні системи, модель Лотки-Вольтери, гібридність, синергія, цільові атаки.*

ВСТУП

Розвиток сучасних технологій та бурхливе зростання інформаційних технологій на основі об'єднання смарт-, Інтернет- технологій та речей з мобільними та бездротовими стандартами сформувало поєднання соціальних мереж з кіберфізичними системами. Крім цього, з'єднання штучного інтелекту з дата-центрами та нейронними мережами значно поширює можливості таких змін в рамках диджиталізації та цифровізації суспільства. Окремим питанням у таких системах є необхідність нових концепцій на основі нових та/або модифікованих підходів побудови та /або формування/модифікації систем захисту.

Крім цього, еволюційне зростання обчислювальних можливостей дозволяю формувати моделі загроз на основі повномасштабного квантового комп'ютера, що на основі алгоритмів Гровера та Шора дозволять значно погіршити рівень забезпечення послуг безпеки. У таких умовах використання нестандартних/нових підходів побудови моделей безпеки – багатоконтурних систем, забезпечать нове рішення щодо протидії сучасним загрозам [1-5].