phase plane method. With the help of this method, the characteristics of special points, isolated closed trajectories and separatrices are found, which in turn allows to evaluate the dynamics of the studied nonlinear dynamic system in a wide range of possible initial conditions. The phase plane illustrates the full variety of possible states of the system, and describes the picture of its dynamics. The paper presents simulation results that prove the adequacy of the developed model. It is confirmed that the developed model of personal data protection is stable, taking into account the attack termination time and the assigned modeling parameters. Using the phase plane method is a new method for researching the stability of the information protection model.

Keywords: phase portrait, information technologies, nonlinear system, stability, confidentiality, availability, forecasting, algorithm.

Лаптєв Сергій Олександрович, аспірант кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна

Serhii Laptiev, PhD student of the department of cyber security and information protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
E-mail: salaptiev@gmail.com.
Orcid ID: 0000-0002-7291-1829.

DOI: 10.18372/2410-7840.26.18826
УДК 004.056(477)

МЕТОДИЧИЙ ПІДХІД ДЛЯ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТРУРИ В УМОВАХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Володимир Шиповський

В ході широкомасштабного вторгнення російської федерації на територію України, вагоме місце займають деструктивні кібервпливи з боку російських кібервійськ на критичну інфраструктуру держави. Цілями Кібератак є не лише військові об'єкти, а й цивільні об'єкти критичної інфраструктури України. Такі дії мають на меті підрив морального духу населення країни та нанесення значної шкоди економіці країни. Відповіддю на це є необхідність розробки ефективних методів кіберзахисту об'єктів критичної інфраструктури (далі – ОКІ) та удосконалення інструментів оцінювання кіберстійкості цих об'єктів, з метою забезпечення їх захисту та оперативного відновлення після можливих атак. Представлена стаття фокусується на розробці методики оцінювання кіберстійкості ОКІ в умовах загроз національній безпеці держави з метою створення сприятливих умов для запобігання та своєчасного реагування на деструктивні кібервпливи з боку ворога та містить рекомендації щодо оцінювання кіберстійкості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. Методика включає в себе розрахунки з використанням теорії ймовірності та методичних рекомендацій, затверджених державними органами України, для категоризації об'єктів критичної інфраструктури з метою оцінювання їх критичності. Методика призначена для оперативного виявлення потенційних цілей ворога та удосконалення рівня кіберзахисту ОКІ у визначеному регіоні країни.

***Ключові слова**: кіберзахист, кіберстійкість, кібероборона, інформаційні системи, кіберзахищеність, інформаційно-телекомунікаційні системи, стійкість, об'єкти критичної інфраструктури, оцінювання, технологія, безпека мереж, національна безпека, гібридні загрози, оцінка, методичний підхід, методика, система, загрози національній безпеці, моделювання, математична модель.*

ВСТУП.

З моменту початку повномасштабного вторгнення Росії у лютому 2022 року ми стали свідками декількох інновацій у веденні війни, коли безпілотні засоби в повітрі, на землі та на морі змінили підходи до розвідки та тактичних і оперативних бойових дій. Проте, російсько-українська війна не перетворилася на науково-фантастичне протистояння між автоматизованими роботизованими системами. Однак, інформаційні технології трансформували природу війни і продовжують це робити. Військові доктрини та правила ведення бойових дій, що були розроблені раніше, потребують оновлення відповідно до сьогоднішніх і майбутніх викликів.

Інтеграція інформаційних технологій зі збройною боротьбою не лише змінила арсенал наявної зброї, але й розмила межі між фізичним та кіберпростором. Традиційні військові арсенали, що раніше складалися з танків, літаків та піхоти, тепер доповнені потужними кіберзасобами. Сучасні ландшафти кібератак дозволяють проникати в інформаційні системи як військових об'єктів, так і критичної інфраструктури держави, значно розширюючи можливості впливу. Урядовою командою реагування на комп'ютерні надзвичай-

ні події України CERT-UA в березні 2024 року розкрито зловмисний задум угрупування Sandworm, спрямований на порушення сталого функціонування інформаційно-комунікаційних систем (ІКС) близько двадцяти підприємств галузі енергетики, водо та теплопостачання (ОКІ) у десяти регіонах України [1].

ПОСТАНОВКА ПРОБЛЕМИ

Стрімкий розвиток кібердомену вимагає розробки ефективного методичного підходу щодо кіберзахисту ОКІ. Для підвищення рівня кібербезпеки цих важливих об'єктів та аналізу поточних кіберзагроз, прогнозування ймовірності здійснення кібератак з боку ворога та для реалізації механізмів захисту інформаційні системи (далі – ІС) ОКІ, оцінювання кіберстійкості в умовах сучасних війн, необхідно оцінити спроможності ОКІ щодо забезпечення працездатності в умовах деструктивних кібервпливів та здатності відновити роботу після втручання в роботу ІС ОКІ. Розробка рекомендацій щодо інструментів оцінювання кіберстійкості дозволить підвищити рівень безпеки та захисту критичної інфраструктури в умовах загроз національній безпеці держави.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Поняття "стійкості" – як здатність "відновлюватися" після несприятливої події – є відносно новим поняттям та актуальним в умовах сьогодення, тому активно досліджується у багатьох освітніх та наукових установах світу. У статті [2] розглянуто поняття кіберстійкості та її важливості для об'єктів критичної інфраструктури та проаналізовано існуючі підходи до оцінювання кіберстійкості, зокрема запропоновано матрицю стійкості. Стаття містить загальний опис підходу до оцінювання кіберстійкості, але без детальної практичної реалізації та впровадження.

У [3] авторами запропоновано не тільки понятійний апарат для цієї предметної області, але і системи, на основі яких можна більш-менш об'єктивно та кількісно оцінювати рівень кіберстійкості. В роботі [4] запропоновано модель загроз для стійкості до відмов роботи інформаційних систем; розглянуті архітектурні рівні або домени, до яких можна застосувати методи аудиту кіберстійкості; також розглянуті аспекти вартості, які слід розглядати як частину компромісного аналізу для альтернативних стратегій щодо реалізації кіберзахисту інформаційних систем. Однак у вищезазначених дослідженнях розглядалось окремі інформаційні системи та вплив внутрішніх загроз, метою даної статті є створення інструменту для оцінювання певної кількості ОКІ в заданих географічних межах.

Метою статті є розробка та представлення комплексної методики оцінювання кіберстійкості об'єктів критичної інфраструктури, яка базується на аналізі кіберзахищеності та відновлюваності інформаційно-телекомунікаційних систем цих об'єктів. Методика має на меті забезпечити оперативну оцінку критичної інфраструктури в умовах гібридних загроз національній безпеці держави та мінімізувати ризики, які пов'язані з кіберзагрозами шляхом прогнозування черговості ураження ОКІ.

АКТУАЛЬНІСТЬ

З початком повномасштабного вторгнення росії в Україну у 2022 році, спостерігалося значне зростання кібератак з боку росії або проросійських хакерських груп на об'єкти критичної інфраструктури України.

Основними видами кібератак з боку РФ з початку широкомасштабного вторгнення були:

-атаки типу "відмова в обслуговуванні" (DDoS) на урядові, банківські, медійні та інші важливі сайти;

-викрадення та оприлюднення конфіденційної інформації;

-встановлення шкідливого ПЗ на комп'ютери об'єктів критичної інфраструктури;

-атаки на енергосистему, зокрема на об'єкти електропостачання;

-спроби зламу систем управління технологічними процесами на промислових об'єктах [5].

Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критично важливій інфраструктурі.

Згідно [6] забезпечення максимального охоплення об'єктів критичної інфраструктури негласною перевіркою стану їх готовності до можливих кібератак та кіберінцидентів з метою превентивного усунення передумов до реалізації кіберзагроз є ефективним інструментом впливу на рівень кіберзахисту ОКІ.

У статті [7] запропоновано модель оцінювання ІС ОКІ, що задовольняє більшості галузей критичної інфраструктури та забезпечує узгоджені та неперервні функцій ОКІ, а саме:

1. Ідентифікацію – розробку підходу організації для управління ризиком інформаційної безпеки (далі – ІБ);

2. Захист – розробку та реалізацію відповідних дій для забезпечення безпеки при надані послуг об'єктами критичної інфраструктури;

3. Виявлення – розробку та реалізацію відповідних заходів для ідентифікації появи інцидентів. (Даний етап сприяє своєчасному виявленню кібератак);

4. Реагування – розробку та реалізацію відповідних заходів для своєчасного виявлення аномалій в роботі інформаційних систем;

5. Відновлення – розробку та реалізацію відповідних заходів для застосування планів стійкості та відновлення характеристик чи діяльності, що була порушена в ході кібервпливу. На основі моделі оцінювання ІС ОКІ будуть побудовані елементи методики.

ОСНОВНА ЧАСТИНА

Зі зростанням кількості кібератак і загроз в мережах об'єктів критичної інфраструктури, виникає необхідність використовувати ефективні моделі комплексного кіберзахисту, які допоможуть захистити інформацію і системи від несанкціонованого доступу і пошкоджень. Враховуючи велику кількість ОКІ в Україні, захист таких об'єктів набуває особливо важливого значення. У статті розглядається проблематика забезпечення кіберзахисту об'єктів ОКІ, акцентуючи увагу на необхідності комплексної оцінки ризиків, що впливають на властивості інформаційних систем ОКІ.

У [6] кіберстійкість визначається як – здатність швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, та підтримувати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури. Основними складовими кіберстійкості є кіберзахищеність (здатність забезпечувати функціонування ОКІ під час деструктивних кібервпливів, підтримуючи конфіденційність, цілісність та доступність інформаційних систем ОКІ) та відновлюваність (швидкості повернення систему до такого стану інформаційних систем, коли ІС функціонували до наслідків кібервпливу). Впливаючи на кіберзахищеність або відновлюваність, кіберстійкість буде змінюватись.

Представлений алгоритм ранжування ІС ОКІ, який показує послідовність розрахунків показників для визначення об'єктів, які є пріоритетними щодо заходів кіберзахисту (рис. 1).

Алгоритм складається з наступних блоків:

1. Визначення переліку ОКІ, які знаходяться на визначеній території (області або кількох областей) та мають інформаційно-комунікаційні системи, на які можуть здійснюватися деструктивні кібервпливи;

2. Визначення кіберстійкості кожного ОКІ шляхом визначення кіберживучості та відновлюваності ІС ОКІ;

3. Оцінювання вагомості кожного ОКІ у визначеній зоні для пріоритезації захисту, враховуючи можливі деструктивні наслідки кібератаки;

4. Ранжування ОКІ за показниками кіберстійкості та вагомості.

У контексті кібербезпеки, кіберзагрози, які впливають як на кіберзахищеність так і кібервідновлюваність, класифікуються на зовнішні та внутрішні, кожна з яких має певні характеристики та потенціал впливу на інформаційні системи. Зовнішні кіберзагрози походять ззовні організації та включають атаки з боку хакерів, фішинг, розповсюдження шкідливого програмного забезпечення та інші форми кібернападів, що мають на меті несанкціонований доступ до корпоративних даних або їх знищення. Натомість, внутрішні кіберзагрози виникають внаслідок дій або бездіяльності співробітників організації, включаючи ненавмисне розголошення конфіденційної інформації, помилкове використання систем або зловмисне втручання зсередини. Відмінність між зовнішніми та внутрішніми загрозами полягає у їх джерелі походження та механізмах реалізації, що вимагає різноманітних стратегій захисту та відповіді.

Рис 1. Алгоритм ранжування ОКІ

Для визначення кіберстійкості системи необхідно обрати математичний вираз, який врахує кіберзахищеність та відновлюваність інформаційної системи включаючи як внутрішні так і

зовнішні загрози. Нижче представлені деякі види зовнішніх та внутрішніх загроз (табл. 1).

Таблиця 1

Зовнішні та внутрішні загрози ІС ОКІ

Внутрішні загрози – α	**Зовнішні загрози – β**
Недбалість або помилки працівників (випадкове або навмисне розголошення конфіденційної інформації, встановлення шкідливого ПЗ тощо)	Кібератаки зловмисників (DDoS-атаки вимагателі, хакери)
Неавторизований доступ до інформаційних систем всередині організації	Цілеспрямовані атаки конкурентів або державних суб'єктів
Неналежне управління доступом та правами користувачів	Шкідливе ПЗ (віруси, хробаки, трояни)
Відсутність належного контролю та аудиту дій користувачів	Фішинг та інженерія соціальних мереж
Недоліки в конфігурації систем та мереж	Вразливості та експлойти в ПЗ та обладнанні
Несанкціонований фізичний доступ до мереж та систем	« – »

В подальших розрахунках α – внутрішні загрози, β – зовнішні загрози. Тоді показник кіберстійкості системи буде виражений у вигляді представленому (рис. 2) та залежить від відновлюваності та кіберзахищеності ІС, який в свою чергу враховує внутрішні та зовнішні загрози.

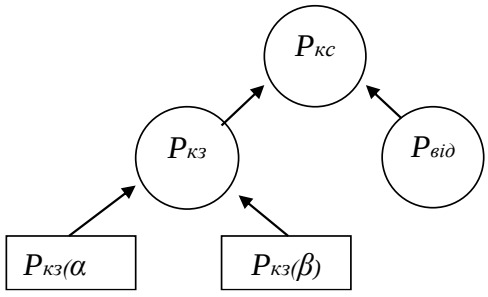

Рис.2. Залежність визначення показника кіберстійкості ІС ОКІ

Розглянемо певну ділянку місцевості, яка визначена як зона, яка потребує оцінювання кіберстійкості в географічних межах зони розташовано *r* – об'єктів критичної інфраструктури.

Введемо показник для відображення кіберстійкості інформаційної системи $P_{кс}$, під яким будемо розглядати ймовірність того, що ОКІ буде функціонувати під зовнішніми та внутрішніми кібервливами на його інформаційні системи.

Аналізуючи кібератаки з боку російських спецпідрозділів та хакерських груп описані в [8] та [9], можемо визначити перелік найчастіше реалізованих атак ОКІ України під час широкомасштабного вторгнення російської федерації:

– завантаження шкідливого програмного забезпечення (далі – ПЗ) з функціями альтернативної оперативної системи з розширеними повноваженнями;

– несанкціоноване копіювання інформації;

– несанкціонована модифікація інформації;

– використання хибного довіреного об'єкта;

– підміна системного ПЗ;

– перенаправлення мережевого трафіку;

– маніпулювання даними у віддаленому режимі;

– розтин електронної поштової скриньки;

– блокування електронної поштової скриньки;

– підміна Web-браузерів;

– використання помилок в алгоритмах прикладного ПЗ;

– блокування хоста користувача;

– блокування маршрутизатора;

– обхід міжмережевого екрану.

Враховуючи те що реалізація внутрішніх та зовнішніх загроз можуть бути подіями як сумісними так і несумісними теорема додавання ймовірностей, яка пропонує рішення лише для несумісних подій, не може бути використана в даному випадку. Для ситуації в які події можуть бути як сумісними так і не сумісними використовуємо вираз для (1) який описаний у [11]:

$$P(A+B)=P(A)+P(B)-P(AB), \quad (1)$$

де подія *A* може бути як сумісною так і несумісною з подією *B*.

Для нашої методики використовуємо формулу (2):

$$P_{кс}=P_{кз}+P_{від}-P_{кз}\cdot P_{від}, \quad (2)$$

де $P_{кз}$ – ймовірність того що ІС ОКІ захищений від кібервпливу, а $P_{від}$ – ймовірність того що ІС ОКІ відновить свою роботу після кібервпливу. Ймовірність кіберзахищеності системи – $P_{кз}$ може бути виражена як повна ймовірність показника захисту від внутрішніх – $P_{кз(а)}$ та зовнішніх загроз – $P_{кз(\beta)}$.

Нехай на ОКІ здійснюється *n* внутрішніх кібервпливів, тоді ймовірність захисту від внутрішніх загроз може бути виражений наступним чином:

$$P_{кз(\alpha)} = \prod_{i=1}^{n}(1-P(\alpha_i)), i=\overline{1,n}, \quad (3)$$

де n – кількість внутрішніх кіберпливів на систему; $P(\alpha_i)$ – ймовірність ураження системи i-им внутрішнім кібервпливом.

Ймовірність захисту від зовнішніх загроз може бути представлена аналогічно:

$$P_{кз(\beta)} = \prod_{j=1}^{m}(1-P(\beta_j)), j=\overline{1,m}, \quad (4)$$

де m – кількість зовнішніх кібервпливів на систему; $P(\beta j)$ – ймовірність ураження системи j – *им* зовнішнім кібервпливом.

$$P_{кз} = P_{кз(\alpha\beta)} = \prod_{i=1}^{n}(1-P(\alpha_i)) + \prod_{j=1}^{m}(1-P(\beta_j)) - \prod_{i=1}^{n}(1-P(\alpha_i)) \cdot \prod_{j=1}^{m}(1-P(\beta_j)) \quad (5)$$

Вираз (5) відображає ймовірність кіберзахисту від внутрішніх та зовнішніх кібервпливів. Процес відновлення системи після кібервпливу – *Рвід* може бути представлений виразом (6):

$$P_{від} = 1 - e^{-\lambda_{від} t}, \quad (6)$$

де $\lambda_{від}(t)$ – інтенсивність відновлення, який розраховується за допомогою виразу (7), в якому *tвідн* – середній час відновлення системи після ураження; *е* – число Ейлера (е=2,71…).

$$\lambda_{від}(t) = \frac{1}{t_{від}}. \quad (7)$$

Отримавши результат з (5) та (6), підставляємо у формулу (2) та отримаємо оцінку критичності *Ркс* для кожного з *r* ОКІ. Кількість ОКІ в зоні оцінювання може бути досить значною, а час на заходи щодо підвищення кіберстійкості під час планування оборонної операції обмеженим, враховуючи це необхідно є необхідність оцінити ОКІ за трьома рівнями критичності:

- $0 \le P_{КС} \le 0,9$ – допустимий рівень;
- $0 \le P_{КС} \le 0,6$ – низький рівень;
- $0 \le P_{КС} \le 0,3$ – критичний рівень.

Аналіз кібератак інформаційних систем ОКІ з початку широкомасштабного вторгнення РФ доводить що ОКІ з критичним рівнем кіберстійкості були уражені російськими кібервійськами з найбільш масштабними наслідками [8] та [9], тому захист ОКІ з допустимим рівнем не потребує дій щодо забезпечення кіберстійкості.

Головною причиною віднесення певних об'єктів до об'єктів критичної інфраструктури є визнання того, що наслідки порушення сталого функціонування одного або низки об'єктів критичної інфраструктури можуть спричинити надзвичайні ситуації та/або мати негативний вплив на стан екологічної, енергетичної, економічної, фінансової безпеки, на стан обороноздатності держави, порушити систему управління нею. Тому необхідно визначити важливість інфраструктурних об'єктів для надання основних послуг у всіх секторах економіки та сферах діяльності задля впровадження низки заходів щодо захисту таких об'єктів від реалізації можливості виникнення кризових ситуацій. Після розрахунку показників кіберстійкості кожного із *r* ОКІ присвоюємо вагові коефіцієнти, які визначать пріоритетність щодо заходів для кіберзахисту критичної інфраструктури, для розрахунків використовуємо Методику категоризації ОКІ [10]. Методика визначає процедуру віднесення об'єктів критичної інфраструктури до певної категорії критичності що являє собою розрахунок узагальненої нормованої оцінки рівня критичності за такою формулою (8):

$$W_{кр} = \frac{\sum W_r}{\sum W_{\max}}, \quad (8)$$

де $\sum W_r$ – сума балів, які отримав ОКІ за всіма критеріями критичності (додатки 1 та 2 Методики [10]); $\sum W_{\max}$ – максимальна можлива сума балів (розраховується, виходячи з того, що об'єкт отримає максимальні бали за всіма критеріями оцінки рівня негативного впливу). Згідно цієї методики кожному ОКІ присвоюються категорія критичності, але в нашому випадку ми використовуємо оцінку критичності окремо для можливості ранжування всіх об'єктів в певному регіоні країни.

Після розрахунків отримуємо ваговий коефіцент – *Wкр* та показник кіберстійкості – *Ркз* для кожного з *r* ОКІ на заданій місцевості. Результат являє собою таблицю 2.

В залежності від розміру географічних обмежень зони оцінювання кількість ОКІ може досягати досить великої кількості, тому для пріоритезації щодо кіберзахисту об'єктів використовуємо наступні формули:

$$W_{кр} = \max_i \{W_{крі}\}, i=\overline{1,r}, \quad (9)$$

$$P_{кс} = \min_{i} \{P_{ксі}\}, i = \overline{1,r}. \quad (10)$$

Таблиця 2

Результати обчислення показників

	Перелік ОКІ	**Ркз**		**Рвід**	**Wкр**
1	ОКІ - 1	*Ркз(а)1*	*Ркза(β)1*	*Рвід1*	*Wкр1*
2	ОКІ - 2	*Ркз(а)2*	*Ркз(β)2*	*Рвід2*	*Wкр2*
…	…	…	…	…	…
r	ОКІ - *r*	*Ркз(а)r*	*Ркз(β)r*	*Рвідr*	*Wкрr*

Для ранжування отриманих результатів можно використати код мови програмування *Phyton*. У коді обидва списки *data_min* – для показника кіберстійкості та *data_max* – для коефіцієнта критичності сортуються окремо, де *data_min* сортується у порядку зростання, а *data_max* – у порядку убування.

Після сортування результати поміщаються у відповідні колонки *DataFrame* з бібліотеки *pandas*, що дозволяє зручно відобразити обидва набори даних у вигляді таблиці.Код для даної операції буде мати наступну послідовність:

```
# Завантажимо бібліотеки pandas та numpy
import pandas as pd
import numpy as np
# Припустимо, маємо два списки даних з однаковою кількістю елементів
data_min = [Ркз1, Ркз2, Ркз3, Ркз4, …, Ркзr] # Дані для знаходження мінімальних значень, в нашому випадку показники кіберстійкості ІС ОКІ
data_max = [Wкр1, Wкр2, Wкр3, Wкр4, …, Wкрr] # Дані для знаходження максимальних значень для показників критичності
# Сортуємо data_min у порядку зростання та data_max у порядку убування
sorted_min = np.sort(data_min)
sorted_max = np.sort(data_max)[::-1]
# Створюємо DataFrame
df = pd.DataFrame({
    'Мінімальні значення (зростання)': sorted_min,
    'Максимальні значення (убування)': sorted_max
})
# Виводимо інформацію про обидва показники.
print(df)
```

Такий підхід дозволяє легко визначити мінімальні та максимальні значення з двох різних наборів даних та представити їх у вигляді структурованої таблиці, спрощуючи аналіз та порівняння даних. Представлена блок-схема методики оцінювання кіберстійкості об'єктів критичної інфраструктури (рис. 4). Методика відповідає поставленим завданням алгоритму рис. 1 та складається з трьох основних модулів та окремих блоків:

1. Модуль №1 призначений для оцінювання кіберстійкості кожного ОКІ шляхом визначення кіберзахищеності та відновлюваності ІС ОКІ;

2. Модуль №2 виконує функцію оцінювання вагомості ОКІ шляхом визначення оцінки вагомості кожного ОКІ;

3. Модуль №3 проводить ранжування показників кіберстійкості та оцінки критичності серед визначеної кількості ОКІ в зоні оцінювання. Після чого блок прийняття рішення дозволяє визначити найбільш вразливі об'єкти, які потребують підвищення кіберстійкості.

Отже, підсумовуючи результати дослідження та враховуючи вразливості які були використані ворогом під час широкомасштабного вторгнення, пропонуємо наступні рекомендації щодо оцінювання кіберстійкості інформаційної системи об'єкта критичної інфраструктури. План оцінювання містить наступні пункти:

1. Перевірка наявності та актуальності документації з інформаційної безпеки - політики, процедури, плани реагування.

2. Аналіз відповідності організації інформаційної безпеки чинним стандартам і нормативним вимогам.

3. Оцінка процесів управління доступом та ідентифікації користувачів.

4. Аудит наданих користувачам прав та рівнів доступу до інформаційних ресурсів.

5. Аналіз заходів з мережевої безпеки - периметр захисту, сегментація мережі, міжмережеві екрани тощо.

6. Перевірка захисту інформаційних систем від шкідливого коду.

7. Оцінка процесів криптографічного захисту інформації.

8. Аудит систем реєстрації та моніторингу подій безпеки.

9. Аналіз процесів управління вразливостями та оновленнями безпеки.

10.Перевірка планів забезпечення безперервності діяльності та відновлення після інцидентів.

11.Оцінка рівня обізнаності персоналу з питань інформаційної безпеки.

Результати оцінювання за запропонованим переліком дозволять виявити критичні вразливості ІС ОКІ, оцінити кіберстійкість системи та змоделювати сценарії ймовірних кібератак.

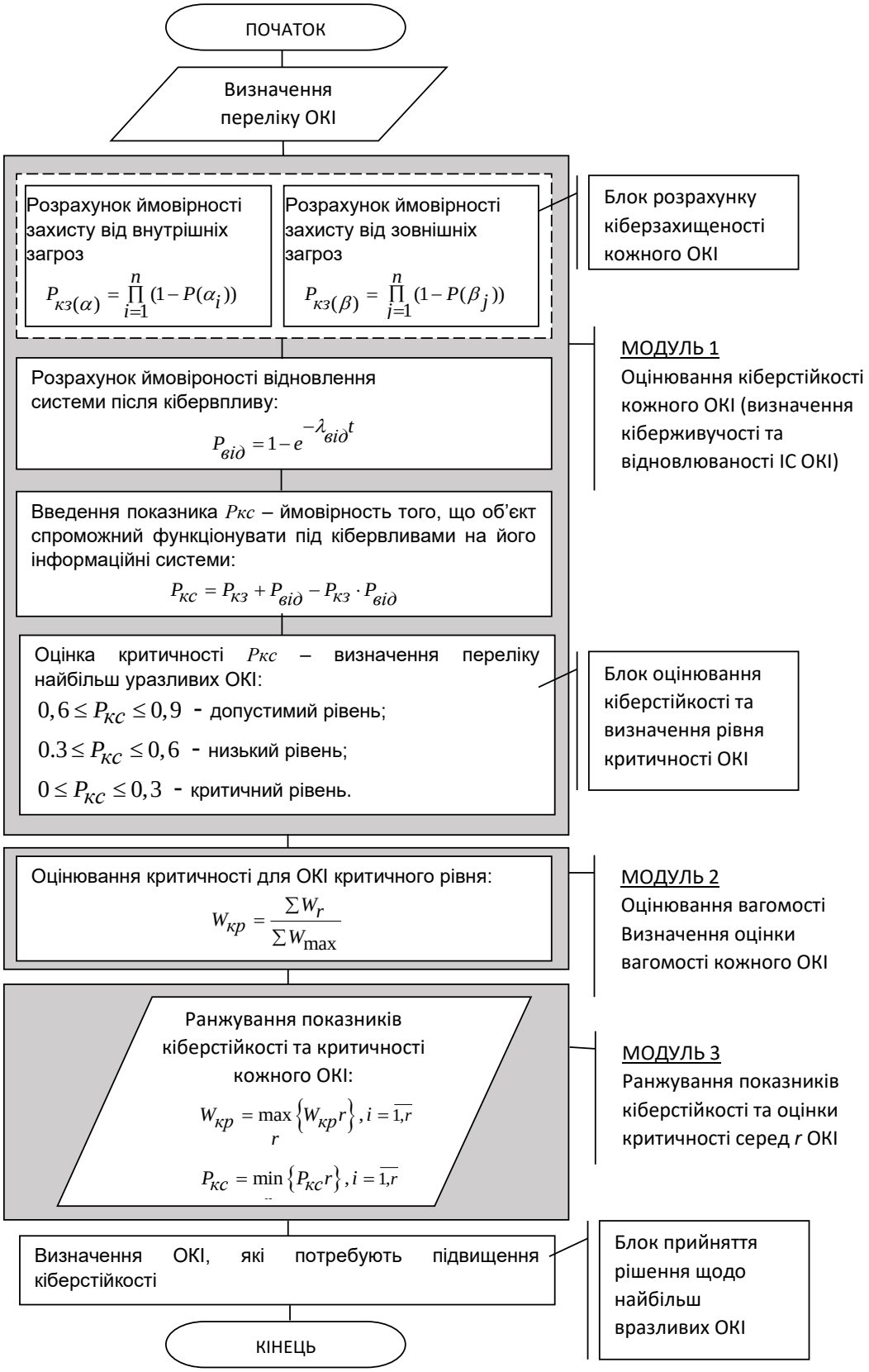

Рис 4. Блок-схема оцінювання кіберстійкості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури

ВИСНОВКИ.

Ця стаття представляє розробку комплексної методики для оцінювання кіберстійкості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури в умовах загроз національній безпеці держави. Методика включає кількісну оцінку потенційних кіберзагроз і їх впливу, використовуючи теорію ймовірності. Це дозво-

ляє об'єднати технічні та організаційні аспекти кібербезпеки для всебічної оцінки кіберстійкості.

Запропонована методика охоплює декілька ключових етапів. По-перше, проводиться ідентифікація і класифікація вразливостей в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури. Важливим аспектом є розгляд не лише технічних вразливостей, але й організаційних і людських факторів, що можуть впливати на загальний рівень кіберстійкості.

По-друге, здійснюється моделювання загроз за допомогою теорії ймовірності, що дозволяє оцінити ймовірність реалізації різних кіберзагроз та їх потенційний вплив на функціонування критичної інфраструктури. Це включає розробку сценаріїв можливих кіберінцидентів та оцінку їх наслідків.

По-третє, методика передбачає розробку і використання системи індикаторів для моніторингу стану кібербезпеки. Ці індикатори включають як кількісні, так і якісні показники, що дозволяють своєчасно виявляти загрози та оцінювати ефективність заходів з кібербезпеки.

Практичне застосування методики підтвердило її ефективність на прикладі конкретних об'єктів критичної інфраструктури. Результати дослідження показали, що використання розробленої методики дозволяє значно підвищити рівень кіберстійкості інформаційно-телекомунікаційних систем. Запропоновані рекомендації включають удосконалення організаційних заходів, підвищення обізнаності персоналу та впровадження сучасних технологічних рішень для забезпечення більш високого рівня кібербезпеки.

Таким чином, розроблений методичний підхід забезпечує всебічну оцінку кіберстійкості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури та може бути використаний для підвищення ефективності захисту від сучасних кіберзагроз. Подальші дослідження можуть зосередитися на адаптації методики до специфічних умов різних секторів критичної інфраструктури та розвитку нових інструментів оцінювання кіберстійкості, зокрема через аналіз її практичного застосування у різних сценаріях.

ЛІТЕРАТУРА

[1]. Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України // URL: https: // cert.gov.ua/article/6278-706 (дата звернення: 07.06.2024).

[2]. Харламова К. Оцінювання кіберстійкості об'єктів критичної інфраструктури України / Харламова К. // Interdisciplinary research: scientific horizons and perspectives. Вільнюс, 2022. No 7. С. 118-120.

[3]. Igor Linkov, Daniel A Eisenberg, Kenton Plourde, Thomas P Seager, Resilience metrics for cyber systems December 2013 Environment Systems and Decisions33(4) URL: https://link.springer.com/article/10.1007/s10669-013-9485-y. (дата звернення: 01.05.2024).

[4]. Deborah J. Bodeau & Richard Graubart September /2011//Cyber Resiliency Engineering Framework MITRE TECHNICAL REPORT. URL: https: // apps.dtic.mil/sti/trecms/pdf/AD1108457.pdf (дата звернення: 07.04.2024).

[5]. Війна Росії проти України: хронологія кібератак/ Європейський парламент 2022 // https: // www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf. (дата звернення: 05.02.2024).

[6]. Стратегія кібербезпеки України / Затверджено Указом Президента України від 26 серпня 2021 року № 447/2021 // URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 02.02.2024).

[7]. Shypovskyi V. Decision-making process model for cybersecurity protection of critical infrastructure objects under the hybrid threats influence/ Shypovskyi V. // Journal of Scientific Papers "Social Development and Security", Vol. 13, No. 3, 2023 // URL: https://paperssds.eu/index.php/JSPSDS/article/view/550.

[8]. Урядова команда реагування на комп'ютерні надзвичайні події України / CERT_UA / URL: https: //www.president.gov.ua/documents/4472021-400-13 (дата звернення: 02.02.2024).

[9]. REPORT ON CYBER LESSONS LEARNED DURING THE WAR IN UKRAINE / NATIONAL CYBER SECURITY CENTRE / URL: https:// www.nksc.lt/doc/rkgc/report_on_cyber_lessons_learned_during_the_war_in_ukraine.pdf (дата звернення: 02.05.2024).

[10]. Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури/ затвердженої постановою Кабінету Міністрів України від 09 жовтня 2020 року № 1109/ URL: https://zakon.rada.gov.ua/rada/show / v0023519-21#Text (дата звернення: 21.02.2024).

[11]. Е. С. Вентцель / Теорія імовірності / підручник / М. 1969 р

METHODOLOGICAL APPROACH FOR ASSESSING THE CYBER RESILIENCE OF INFORMATION AND TELECOMMUNICATION SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS UNDER NATIONAL SECURITY THREATS

Since the onset of Russia's full-scale invasion in February 2022, we have witnessed several innovations in warfare, where unmanned systems in the air, on land, and at sea have transformed approaches to reconnaissance and tactical and operational combat operations. However, the Russo-Ukrainian war has not evolved into a sci-fi battle

between automated robotic systems. Nevertheless, information technologies have transformed the nature of war and continue to do so. Military doctrines and combat rules, previously developed, need to be updated to address current and future challenges. The integration of information technologies with armed conflict has not only changed the arsenal of available weapons but also blurred the lines between the physical and cyber domains. Traditional military arsenals, once dominated by tanks, aircraft, and infantry, are now supplemented by powerful cyber capabilities. Modern cyberattack landscapes allow for penetration into the information systems of both military targets and critical state infrastructure, significantly expanding the scope of influence. The rapid development of the cyber domain requires the development of an effective methodological approach to the cyber protection of critical infrastructure objects (CIOs). To enhance the cybersecurity level of these vital objects, analyze current cyber threats, forecast the likelihood of enemy cyberattacks, and implement protection mechanisms for the information and communication systems of CIOs, it is essential to assess the CIOs' capabilities to maintain functionality under destructive cyber influences and to restore operations after interference with the information and communication systems of CIOs. Developing recommendations for tools to assess cyber resilience will enhance the security and protection level of critical infrastructure under national security threats.

Keywords: cybersecurity, cyber resilience, cyber defense, information systems, cyber protection, information and telecommunication systems, resilience, critical infrastructure objects, assessment, technology, network security, national security, hybrid threats, evaluation, methodological approach, methodology, system, threats to national security, modeling, mathematical model.

Шиповський Володимир Володимирович, ад'юнкт кафедри інформаційно-аналітичних технологій Інституту інформаційно-телекомунікаційних технологій та кібероборони Національного університету оборони України імені Івана Черняховського.

Volodymyr Shypovskyi, adjunct of the Department of Information and Analytical Technologies of the Institute of Information and Telecommunication Technologies and Cyber Defense of the National Defense University of Ukraine named after Ivan Chernyakhovsky.
E-mail: stratcom.ndl@gmail.com.
Orcid ID: 0000-0003-3743-3064.

DOI: 10.18372/2410-7840.26.18827
УДК 336.71:004.056

МОДЕЛЬ ТОЧНОСТІ ПРОГНОЗУ ВИЯВЛЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ У РЕАЛЬНОМУ ЧАСІ

Сергій Зибін, Андрій Собчук, Володимир Ровда

Інформаційна безпека Держави це актуальне завдання для країни яка проводить військові дії. Забезпечення інформаційної безпеки Держави актуальне наукове завдання для усіх країн. Проблема інформаційного протиборства, інформаційна війна завжди займала першочергове місце у загальної безпеки Держави. За допомогою злочинного інформаційного впливу можливо керувати соціумом, суспільним настроїм. Тому розробка та удосконалення науково-методичного апарату, а саме розробка моделі точності прогнозу виявлення неправдивої інформації у реальному часі, як засіб введенню інформаційного протиборства, є актуальним науковим завданням. Вирішенню цього наукового завдання і присвячена дана наукова робота. У роботі досліджується математичний апарат виявлення та блокування неправдивої інформації у реальному часі. Саме вирішенню проблеми виявлення неправдивої інформації і присвячена стаття. Розглянута ситуація, коли реконструйований сигнал генерується моделлю Мандельброта, далі використовую метод самонавчання Кохонена. Уточнюючі невідомі параметри за допомогою стандартного метода Утадроу – Хоффа отримали модель точності прогнозу виявлення неправдивої інформації. Яка дозволяє виявляти неправдиву інформації у реальному часі. Напрямком подальших досліджень може бути завдання оптимізації критеріїв оцінки точності прогнозу.

***Ключові слова**: неправдива інформація, виявлення, блокування, реальний час.*

ВСТУП

Для вирішення задачі виявлення та блокування розповсюдження неправдивої інформації необхідно розуміти принципи, за якими вона поширюється. В цьому допомагають методи комп'ютерної лінгвістики для того, щоб зрозуміти правила та шаблони, за якими можна ідентифікувати елементи дезінформації в потоці текстових даних. Дослідження показали, що для створення фейкової інформації набір тексту використовується за певними правилами, щоб новина здавалася правдивою [1]. Неправдивий контент має певні особливості, такі як скорочення, передача меншої кількості інформації, негативний характер. Також прослідковуються елементи не аналітичної думки, а більш неформального мислення. Особливістю інформаційної загрози є поява тенденції до багаторазового сталого повто-