УДК 330.3

В. П. Звєрєв,
к. т. н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет
ORCID ID: https://orcid.org/0000-0002-0907-0705
Д. І. Прокопович-Ткаченко,
к. т. н., доцент, завідувач кафедри кібербезпеки,
Університет митної справи та фінансів
ORCID ID: https://orcid.org/0000-0002-6590-3898
В. І. Саричев,
д. е. н., доцент, професор кафедри економіки та економічної безпеки,
Університет митної справи та фінансів
ORCID ID: http://orcid.org/0000-0002-8544-9901
Б. С. Хрушков,
аспірант кафедри кібербезпеки,
Університету митної справи та фінансів,
ORCID ID: http://orcid.org/0009-0002-3978-5012
В. Г. Бушков,
аспірант кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет
ORCID ID: http://orcid.org/0009-0005-5097-2689

DOI: 10.32702/2306-6814.2024.24.28

ЦИФРОВА ЕКОНОМІКА УКРАЇНИ: АДАПТИВНІ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В УМОВАХ ЗРОСТАННЯ ГІБРИДНИХ КІБЕРЗАГРОЗ

V. Zvieriev,
PhD, Associate Professor, Associate Professor of the Department of Software Engineering and Cybersecurity,
State University of Trade and Economics
D. Prokopovych-Tkachenko,
PhD, Associate Professor, Head of the Department of Cybersecurity, University of Customs and Finance
V. Sarychev,
Doctor of Economics, Associate Professor, Professor of the Department of Economics
and Economic Security, University of Customs and Finance
B. Khruskov,
Postgraduate student of the Department of Cyber Security, University of Customs and Finance
V. Bushkov,
Postgraduate student of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics

THE DIGITAL ECONOMY OF UKRAINE: ADAPTIVE SECURITY MODELS AMID RISING HYBRID CYBER THREATS

У статті досліджено сутність категорії адаптивні моделі кібербезпеки, які забезпечують функціонування цифрових комунікаційних мереж суб'єктів господарювання України в сучасних умовах зростання періодичності та масштабів гібридних кібератак, інтенсивність яких суттєво збільшилася в умовах воєнного часу внаслідок повномасштабної агресії Рф.

Проаналізовано провідні ризики з реалізації прийнятої на національному рівні Концепції розвитку цифрової економіки та громадянського суспільства, а також подальшого його стимулювання через масштабне використання інформаційно-комунікаційних й цифрових технологій.

Визначено ключові принципи побудови адаптивних систем захисту, що включають прогнозування, аналіз ризиків, оптимізацію ресурсів та оперативне реагування. Використання теорії графів, кластерного аналізу та моделей Марківських ланцюгів дає змогу ефективно адаптуватися до змінюваного ландшафту загроз у цифровій економіці, а також зрушити пріоритети національного господарства у бік технологічної трансформації провідних галузей економіки, якісних змін рівня життя населення тощо.

The article examines the essence of the category of adaptive cybersecurity models that ensure the functioning of digital communication networks of Ukrainian business entities. The leading risks associated with the implementation of the nationally adopted Concept for the Development of the Digital Economy and Civil Society, as well as further stimulation through the large-scale use of information and communication technologies (ICT) and digital tools, have been analyzed. In current conditions, the frequency and scale of hybrid cyber attacks have increased significantly. Their intensity has escalated particularly during wartime as a result of Russia's full-scale aggression.

Key principles for constructing adaptive protection systems have been identified, including threat forecasting, risk analysis, resource optimization, and rapid response. The application of graph theory, cluster analysis, and Markov chain models enables effective adaptation to the dynamic threat landscape of the digital economy. This approach facilitates the reprioritization of national economic sectors toward technological transformation of key industries and qualitative improvements in the population's standard of living.

Hybrid threats represent complex, combined attacks on critical network elements that underpin the functioning of Ukraine's digital economy. The methodology of adaptive defense models against such threats incorporates a wide range of analytical, mathematical, and algorithmic approaches to ensure robust cybersecurity.

The modern cyber threat landscape is characterized by high dynamism, multi-vector attacks, and their focus not only on disrupting or disabling network functionality but also on undermining social, economic, and governance stability. In this context, adaptive models are becoming an essential tool for building resilient cybersecurity systems.

Graph theory is a key component for modeling complex network structures. It allows the analysis of network topology, identification of nodes critical to stable functionality, and prediction of attack propagation pathways. This enables the creation of node redundancy scenarios or preemptive enhancement of their protection.

Cluster analysis serves as an effective tool for processing large volumes of data generated by network monitoring systems. It helps identify patterns in attackers' behavior, group threats by type, vector, or attack strategy. Such grouping allows the identification of critical risk clusters whose compromise could cause the most significant damage.

The conducted study proposes an innovative adaptive cybersecurity model that accounts for the specifics of hybrid threats and the unique features of Ukraine's digital economy. This model integrates advanced approaches such as network topology analysis using graph theory, prediction of attacker behavior through Markov chain models, data segmentation via cluster analysis, and resource optimization using algorithmic methods.

The primary advantage of the proposed model lies in its ability to adapt to the dynamic threat landscape, particularly multi-vector combined attacks targeting critical elements of digital networks. The use of mathematical and statistical methods ensures accuracy in attack forecasting and vulnerability identification, while the implementation of optimization techniques allows efficient utilization of limited resources to neutralize threats.

Ключові слова: цифрова економіка, кібербезпека, адаптивні моделі, гібридні кібератаки, система адаптивної стійкості мереж (САСМ), теорія графів, Марківські ланцюги.

Key words: digital economy, cybersecurity, adaptive models, hybrid cyber attacks, adaptive resilience network systems (ARNS), graph theory, Markov chains.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифровізація економіки формує новий ландшафт кіберзагроз, серед яких гібридні кібератаки набувають дедалі складнішого характеру особливо в умовах воєнного часу. Їх багатовекторність і спрямованість на руйнування технологічної, фінансової та соціальної інфраструктури суспільства потребують комплексного адаптивного підходу до кіберзахисту національного простору. В умовах, коли ризики зростають, адаптивні моделі кібербезпеки стають важливим інструментом управління цими викликами у практичній діяльності суб'єктів господарювання.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Аналіз сучасних досліджень свідчить на активний пошук підходів до забезпечення кібербезпеки в умовах гібридних загроз різних сегментів суспільно-економічного життя на національному рівні. Так, згідно з дослідженням Маттіли Дж. (2024), розроблено модель кіберзахисту, засновану на військових багатодоменних операціях, яка інтегрує стратегічний, оперативний і тактичний рівні управління. Модель враховує швидку еволюцію кіберзагроз і адаптована до використання в умовах сучасних збройних конфліктів, повномасштабної війни в Україні зокрема. Вона підкреслює важливість залучення національних і військових ресурсів для створення та використання кіберзахисних можливостей [8].

Дослідження Кумара Р. та Нагара Г. (2024) аналізує виклики для менш технологічно розвинених сторін у кіберконфліктах. Автори пропонують адаптивну модель моделювання загроз, яка включає базові практики кібергігієни, впровадження систем виявлення загроз і розробку ефективних планів реагування на інциденти. Модель була апробована на прикладах кібернападів на Естонію, Грузію та Україну, демонструючи її практичну

цінність. Основний акцент зроблено на міжнародній співпраці, обміні інформацією та інтеграції глобальних підходів у національні стратегії [7].

Решта, переважно закордонних, дослідників підкреслюють критичну важливість використання адаптивних моделей для посилення кібербезпеки та лише побічно торкаються їх використання в економічній сфері [4; 7; 9]. Вони сприяють розробці стратегій, які враховують швидку зміну характеру загроз і необхідність у міжнародній співпраці. Подальші дослідження можуть бути спрямовані на впровадження новітніх технологій та адаптацію існуючих моделей до специфіки української цифрової економіки.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Спираючись на наукові розвідки перелічених дослідників та експертів-практиків у сфері розробки адаптивного підходу до кіберзахисту національного простору, його економічного сегменту зокрема, метою представленої роботи є дослідження переваг використання адаптивних моделей кібербезпеки, які забезпечують функціонування цифрових та інформаційно-комунікаційних мереж суб'єктів господарювання України в сучасних умовах зростання періодичності та масштабів гібридних кібератак.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Методологія адаптивних моделей захисту від гібридних загроз, які представляють собою складні комбіновані атаки на критично важливі елементи мереж, що забезпечують функціонування цифрової економіки України, охоплює широкий спектр аналітичних, економетричних і алгоритмічних підходів для забезпечення надійного кіберзахисту [6]. Сучасний ландшафт кіберзагроз характеризується високою динамічністю, багатовекторністю атак та їхнім спрямуванням не лише на знищення або порушення функціональності мереж, але й на підрив соціальної, економічної та управлінської стабільності [4]. У цьому контексті адаптивні моделі стають важливим інструментом для побудови стійкої системи кіберзахисту [9].

Теорія графів є основним компонентом для моделювання складних мережевих структур. Вона дозволяє аналізувати топологію мережі, визначати вузли, які є найбільш критичними для її стабільного функціонування, і прогнозувати шляхи поширення атак [5]. Завдяки цьому можливо створювати сценарії резервування вузлів або підвищувати рівень їхнього захисту заздалегідь.

Кластерний аналіз є ефективним інструментом для обробки великих обсягів даних, які генеруються системами моніторингу мережі. Він дозволяє виявляти закономірності в поведінці атакуючих, групувати загрози за типом, вектором або тактикою атак. Таке групування дозволяє виділяти ключові кластери ризиків, компрометація яких може завдати найбільшої шкоди [10].

У результаті проведеного дослідження запропоновано інноваційну адаптивну модель кіберзахисту, яка враховує особливості гібридних загроз та специфіку цифрової економіки України [2]. Ця модель базується на інтеграції таких сучасних підходів, як аналіз топології мереж за допомогою теорії графів, прогнозування поведінки атакуючих за допомогою моделей Марківських ланцюгів, сегментація даних через кластерний аналіз та оптимізація ресурсів із використанням алгоритмічних методів.

Основною перевагою запропонованої моделі є її здатність адаптуватися до динамічного ландшафту загроз, зокрема до багатовекторних комбінованих атак, які спрямовані на критично важливі елементи цифрових мереж. Використання математичних і статистичних методів забезпечує точність у прогнозуванні атак і виявленні вразливостей, а впровадження оптимізаційних підходів дозволяє ефективно використовувати обмежені ресурси для нейтралізації загроз.

Реалізація цієї інноваційної моделі можлива шляхом впровадження декількох етапів, серед яких: по-перше, створення інтегрованої системи збору та аналізу даних про загрози, розробка сценаріїв реагування на основі статистичних та прогнозних даних; та, по-друге, впровадження технологій автоматизованого моніторингу мереж у реальному часі.

Особливу увагу слід приділити розробці нормативно-правових стандартів, які б забезпечили підтримку функціонування адаптивної моделі на державному рівні та сприяли її інтеграції в існуючі системи захисту критичної інфраструктури.

Запропонована інноваційна система отримала назву "Система адаптивної стійкості мереж" (САСМ). Вона представляє інтегрований підхід до забезпечення кіберзахисту. САСМ орієнтована на динамічну адаптацію до змін у середовищі загроз, забезпечення стійкості ключових елементів мережі та інтеграцію новітніх технологій в інформаційний простір для виявлення, аналізу і нейтралізації атак (рис. 1).

Запропонована модель має не лише теоретичне, але й практичне значення, оскільки її впровадження дозволить суттєво підвищити рівень кіберзахисту критичних елементів цифрової економіки України [1]. Подальша реалізація цієї моделі вимагає міжсекторальної співпраці, залучення експертного потенціалу в галузі кібербезпеки та активної підтримки з боку держави і приватного сектору. САСМ має стати фундаментом для розвитку стійкої цифрової інфраструктури, здатної ефективно протистояти сучасним викликам у сфері кібербезпеки.

Структура САСМ складається з п'яти основних компонент, які забезпечують функціонування системи та взаємодію між собою у логічному порядку:

1. Моніторинг та збір даних. Ця компонента забезпечує безперервний збір інформації про мережеву активність за допомогою сенсорів мережевої активності, модулів аналізу логів і системи виявлення вторгнень (IDS). Дані, отримані з цього модуля, передаються до компоненти "Аналіз загроз" для подальшої обробки.

2. Аналіз загроз. Ця компонента проводить аналіз зібраних даних для виявлення потенційних загроз. У роботі використовуються методи кластерного аналізу, моделі Марківських ланцюгів для прогнозування поведінки атакуючих та аналіз сценаріїв атак. Виявлені вразливості передаються компоненті "Оптимізація ресурсів".

3. Оптимізація ресурсів. Основне завдання цієї компоненти — забезпечити ефективний розподіл ресурсів. Вона використовує інформацію про вразливості для

побудови стратегій резервування, прискорення реагування на інциденти та оптимального розподілу ресурсів для нейтралізації загроз. Рекомендації передаються компоненті "Інтегрована реакція".

4. Інтегрована реакція. Ця компонента відповідає за реалізацію заходів реагування. Вона забезпечує планування дій, автоматизовану реакцію на загрози та оцінку впливу атак. Інформація про ефективність заходів і стан системи передається компоненті "Управління та координація".

5. Управління та координація. Завершальна компонента системи, яка виконує стратегічне управління усіма іншими компонентами. Вона забезпечує централізоване управління, розробку політик кіберзахисту та контроль відповідності нормативам, а також налаштовує роботу сенсорів компоненти "Моніторинг та збір даних" для адаптації до нових загроз.

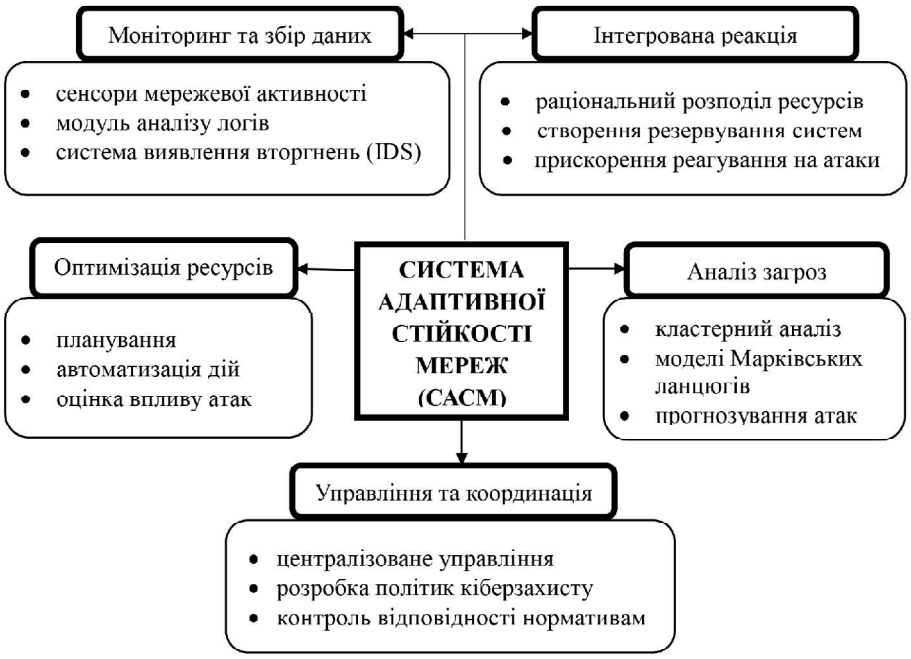

Рис. 1. Структура САСМ та її провідні складові

Джерело: систематизовано, узагальнено та згруповано авторами.

САСМ побудована на принципі безперервної взаємодії між її компонентами, що забезпечує ефективність реагування на сучасні загрози та адаптацію до змінюваного ландшафту кіберзагроз. Моніторинг та збір даних виступає основним джерелом інформації про поточний стан мережі. Ця компонента отримує дані через сенсори мережевої активності, аналізує журнали (логи) та використовує систему виявлення вторгнень (Intrusion Detection System — IDS).

Дані, зібрані цим модулем, передаються компоненті Аналіз загроз. Взаємодія між цими модулями забезпечує своєчасне надходження інформації для оцінки ризиків і вразливостей. В Аналізі загроз зібрані дані проходять детальну обробку. Використовуються кластерний аналіз, моделі Марківських ланцюгів та сценарне прогнозування для ідентифікації потенційних ризиків і шляхів розвитку атак.

Виявлені вразливості та оцінки ризиків передаються компоненті Оптимізація ресурсів. Така передача даних забезпечує зв'язок між аналізом загроз та плануванням ефективного використання ресурсів. Оптимізація ресурсів перетворює результати аналізу на чіткі рекомендації для подальших дій. Цей модуль визначає шляхи ефективного розподілу обмежених ресурсів, включаючи створення резервів систем, прискорення реагування та забезпечення стійкості мережі.

Дані рекомендації передаються до компоненти Інтегрована реакція для реалізації заходів. Інтегрована реакція реалізує безпосереднє виконання дій з протидії загрозам. Ця компонента забезпечує розробку та впровадження планів реагування, автоматизує процеси нейтралізації атак та оцінює вплив інцидентів. Результати реалізованих дій і стратегічні звіти передаються компоненті Управління та координація.

Управління та координація забезпечує стратегічну взаємодію усіх компонент системи. Цей модуль забезпечує розробку політики кіберзахисту, контроль відповідність нормативам та взаємодію між різними складовими системи. На основі отриманих звітів він також регулює роботу компоненти Моніторинг та збір даних, налаштовуючи сенсори і параметри збору даних відповідно до актуальних загроз.

Цілісна інтеграція компонент забезпечує швидкість реакції завдяки оперативному виявленню загроз та реагуванню на них у реальному часі, гнучкість через адаптацію до нових сценаріїв атак, раціональність за рахунок оптимального використання ресурсів на основі рекомендацій системи та стійкість завдяки мінімізації ризиків порушення функціонування мережі навіть у випадку складних багатовекторних атак.

Таким чином, система САСМ представляє собою інтегровану екосистему, яка поєднує аналіз, прогнозування, планування, реагування та управління в єдиній структурі. Така взаємодія дозволяє значно підвищити ефективність захисту критично важливих елементів цифрової інфраструктури України в умовах зростання складності сучасних загроз [3].

Переваги моделі САСМ у протидії гібридним атакам можуть бути посилені через ймовірність підвищення надійності системи.

Нехай $P_{detect\ П}$ позначає ймовірність своєчасного виявлення загрози, P_{react} — ймовірність успішного реагування на загрозу, $P_{mitigate}$ — ймовірність ефективного пом'якшення наслідків атаки, $R_{baseline}$ — базова надійність мережі без впровадження САСМ, R_{SASM} — надійність мережі після впровадження САСМ, $T_{response}$ — середній час реагування на загрозу, а $T_{critical}$ — критичний час, після якого атака завдає незворотних збитків. Формула для оцінки надійності мережі після

впровадження моделі САСМ виглядає так:

$$R_{SASM} = R_{baseline} + \left(P_{detect} \cdot P_{react} \cdot P_{mitigate}\right) \cdot \cdot \left(1 - \frac{T_{response}}{T_{critical}}\right) \quad (1).$$

Тут $\frac{T_{response}}{T_{critical}}$ характеризує швидкість реагування системи відносно допустимого часу для нейтралізації загрози.

За базовим сценарієм для мережі без використання адаптивної моделі середні значення ймовірностей становлять: $P_{detect} = 0.6$, $P_{react} = 0.5$, $P_{mitigate} = 0.4$, $T_{response} = 2$, $T_{critical} = 5$. Виходячи з формули, базова надійність дорівнює:

$$R_{baseline} = 0.6 \cdot 0.5 \cdot 0.4 \cdot \left(1 - \frac{2}{5}\right) = 0.072 \quad (2).$$

У сценарії з впровадженням САСМ показники покращуються завдяки функціональним модулям системи: $P_{detect} = 0.9$, $P_{react} = 0.8$, $P_{mitigate} = 0.85$, $T_{response} = 1.5$, $T_{critical} = 5$. На основі формули надійність мережі з впровадженням САСМ становить:

$$R_{SASM} = 0.072 + (0.9 \cdot 0.8 \cdot 0.85) \cdot \cdot \left(1 - \frac{1.5}{5}\right) = 0.072 + 0.4896 = 0.5616 \quad (3).$$

Це свідчить, що впровадження САСМ суттєво підвищує надійність цифрових мереж із 0.072 до 0.5616, що майже в 8 разів більше. Таким чином, модель значно покращує здатність мереж виявляти, реагувати та пом'якшувати наслідки гібридних атак, зменшуючи час реагування на критичні події. Застосування таких підходів підвищує загальну стійкість цифрової інфраструктури до сучасних загроз.

Методологія адаптивних моделей захисту від гібридних загроз, які становлять складні комбіновані атаки на критично важливі елементи мереж, базується на інтеграції математичних і алгоритмічних підходів для забезпечення високого рівня кіберзахисту.

Основними складовими є теорія графів для аналізу топології мереж, кластерний аналіз для сегментації загроз, моделі Марківських ланцюгів для прогнозування сценаріїв атак, а також оптимізаційні методи для ефективного розподілу ресурсів. Результати аналізу підтверджують, що така інтеграція дозволяє ефективно адаптуватися до змінюваного ландшафту загроз, забезпечуючи стійкість систем до багатовекторних атак.

Теорія графів дає змогу виявляти критичні вузли мережі та прогнозувати наслідки компрометації. Наприклад, у разі атак на ключові вузли прогнозуються шляхи поширення загрози, що дозволяє створювати ефективні резервні сценарії. Кластерний аналіз виявляє закономірності в даних, допомагаючи сегментувати атаки за тактикою та вектором, що знижує ймовірність компрометації критично важливих об'єктів. Моделі Марківських ланцюгів дозволяють передбачати розвиток загроз у реальному часі, а оптимізаційні методи забезпечують зменшення часу реагування на інциденти та мінімізацію впливу атак.

Оцінка базової надійності мережі без впровадження адаптивних підходів становить $R_{baseline} = 0.072$. З використанням компонентів САСМ, таких як автоматизований моніторинг, аналіз даних і оптимізація ресурсів, показник надійності підвищується до $R_{SASM} = 0.5616$. Це свідчить про майже восьмиразове покращення стійкості системи до гібридних атак. Основними факторами успіху є швидкість виявлення загроз ($P_{detect} = 0.9$), ефективність реагування ($P_{react} = 0.8$) та пом'якшення наслідків ($P_{mitigate} = 0.85$).

Для успішної реалізації системи необхідно створити інтегровану платформу збору та аналізу даних, розробити сценарії реагування, що враховують сучасний ландшафт загроз, та впровадити автоматизовані інструменти моніторингу. Важливо забезпечити підтримку моделі на державному рівні, встановивши відповідні нормативи для усіх складових критичної інфраструктури [10]. Запропонована модель САСМ демонструє високу ефективність у забезпеченні стійкості цифрової економіки України та може бути основою для побудови інфраструктури кіберзахисту нового покоління.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Запропонована методологія побудови адаптивних моделей захисту від гібридних загроз демонструє значний потенціал у підвищенні надійності мереж цифрової економіки України. Використання сучасних економетричних та алгоритмічних підходів, таких як теорія графів, кластерний аналіз, моделі Марківських ланцюгів та оптимізаційні методи, дозволяє ефективно адаптувати системи кіберзахисту до змінюваного ландшафту загроз. Інтеграція цих підходів забезпечує можливість прогнозування ризиків, оперативного реагування на атаки та мінімізації впливу на критичну інфраструктуру.

Перевагами запропонованої системи є здатність своєчасно виявляти загрози, ефективно розподіляти ресурси та адаптувати стратегії захисту до нових викликів. Зокрема, використання теорії графів для аналізу мережевої структури дозволяє ідентифікувати критичні вузли та прогнозувати наслідки їх компрометації, що забезпечує можливість превентивного резервування та підвищення стійкості системи. Кластерний аналіз сприяє виявленню закономірностей у поведінці організаторів кібератак, дозволяючи створювати індивідуалізовані стратегії захисту для різних видів загроз, а моделі Марківських ланцюгів є ефективним інструментом для прогнозування розвитку атак у реальному часі, що дає змогу системам кіберзахисту бути на крок попереду тих, хто приймає участь в атаках.

Реалізація запропонованої моделі свідчить про суттєве підвищення надійності цифрових мереж. Зокрема, надійність системи збільшується з 0.072 (без адаптивної моделі) до 0.5616 (з використанням САСМ), що дозволяє досягти майже восьмиразового покращення. Це стає можливим завдяки підвищенню швидкості виявлення загроз, ефективності реагування та зменшенню часу на виконання заходів щодо нейтралізації наслідків атак.

Для впровадження САСМ необхідно створити інтегровану платформу моніторингу та аналізу даних, впровадити автоматизовані інструменти реагування на інциденти та забезпечити нормативно-правову підтримку на державному рівні. Це дозволить не лише підвищити

рівень захищеності цифрової економіки, але й створити стійку основу для розвитку інфраструктури кібербезпеки нового покоління. Таким чином, запропонована модель є ключовим кроком до створення надійної, адаптивної та стійкої цифрової економіки України.

Література:

1. Закон України Про стимулювання розвитку цифрової економіки в Україні № 2811-IX від 01.12.2022. Відомості Верховної Ради України. 2023. № 6-7, ст.18). URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (дата звернення: 23.10.2024).

2. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки. Розпорядження КМ України від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 23.10.2024).

3. Олійник Д. Цифрова трансформація економіки України в умовах війни: жовтень 2024. Національний інститут стратегічних досліджень. 2024. URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-zhovten-2024 (дата звернення: 25.11.2024).

4. Ali, S., & Myeong, S. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. Sensors. URL: https://doi.org/10.3390/s24154888 (дата звернення: 22.11.2024).

5. Alijoyo, F. A., Kaur, C., Anjum, A., Vuyyuru, V. A., & Bala, B. K. (2024). Enhancing cyber-physical systems resilience: Adaptive self-healing security using long short-term memory networks. Proceedings of the International Conference on Advanced Cybersecurity Technologies. URL: https://doi.org/10.1109/accai61061.2024.10602467 (дата звернення: 12.11.2024).

6. Blackwood, A., Carrington, J., Baryshevsky, S., & Morrison, G. (2024). The implementation of a hybrid large language model for adaptive cryptographic cyber defense. Journal of Cyber Defense Studies. URL: https://doi.org/10.21203/rs.3.rs-5120507/v1 (дата звернення: 29.11.2024).

7. Kumar, S. R., & Nagar, G. (2024). Threat modeling for cyber warfare against less cyber-dependent adversaries. Proceedings of the European Conference on Information Warfare and Security. URL: https://typeset.io/papers/threat-modeling-for-cyber-warfare-against-less-cyber-37mao5tfb8 (дата звернення: 29.11.2024).

8. Mattila, J. (2024). Arranging the defence of the cyber environment as a part of military affairs: Tactical, operational and strategic approach in retrospect of the Russian-Ukrainian war 2022. Proceedings of the European Conference on Information Warfare and Security. URL: https://typeset.io/papers/arranging-the-defence-of-the-cyber-environment-as-a-part-of-2rmyeiokck (дата звернення: 29.11.2024).

9. Shypovskyi, V. (2023). Decision-making process model for cybersecurity protection of critical infrastructure objects under the hybrid threats influence. Social Development & Security. URL: https://doi.org/10.33445/sds.2023.13.3.3 (дата звернення: 25.11.2024).

10. Srivastava, A., Parmar, V., Patel, S., & Chaturvedi, A. S. (2023). Adaptive cyber defense: Leveraging neuromorphic computing for advanced threat detection and response. Proceedings of the International Conference on Cybersecurity Science and Systems. URL: https://doi.org/10.1109/ICSCSS57650.2023.10169393 (дата звернення: 25.11.2024).

References:

1. Verkhovna Rada of Ukraine (2022), The Law of Ukraine "On stimulating the development of the digital economy in Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1667-20#Text (Accessed 23.10.2024).

2. Cabinet of Ministers of Ukraine (2018), Resolution "Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020", available at: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (Accessed 23.10.2024).

3. Olijnyk, D. (2024), "Digital Transformation of Ukraine's Economy in Wartime: October 2024", available at: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-zhovten-2024 (Accessed 25.11.2024).

4. Ali, S., & Myeong, S. (2024), "Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application", Sensors. https://doi.org/10.3390/s24154888.

5. Alijoyo, F. A., Kaur, C., Anjum, A., Vuyyuru, V. A., & Bala, B. K. (2024), "Enhancing cyber-physical systems resilience: Adaptive self-healing security using long short-term memory networks", Proceedings of the International Conference on Advanced Cybersecurity Technologies. https://doi.org/10.1109/accai61061.2024.10602467.

6. Blackwood, A., Carrington, J., Baryshevsky, S., & Morrison, G. (2024), "The implementation of a hybrid large language model for adaptive cryptographic cyber defense", Journal of Cyber Defense Studies. https://doi.org/10.21203/rs.3.rs-5120507/v1.

7. Kumar, S. R., & Nagar, G. (2024), "Threat modeling for cyber warfare against less cyber-dependent adversaries", Proceedings of the European Conference on Information Warfare and Security, available at: https://typeset.io/papers/threat-modeling-for-cyber-warfare-against-less-cyber-37mao5tfb8 (Accessed 29.11.2024).

8. Mattila, J. (2024), "Arranging the defence of the cyber environment as a part of military affairs: Tactical, operational and strategic approach in retrospect of the Russian-Ukrainian war 2022", Proceedings of the European Conference on Information Warfare and Security, available at: https://typeset.io/papers/arranging-the-defence-of-the-cyber-environment-as-a-part-of-2rmyeiokck (Accessed 29.11.2024).

9. Shypovskyi, V. (2023), "Decision-making process model for cybersecurity protection of critical infrastructure objects under the hybrid threats influence", Social Development & Security. https://doi.org/10.33445/sds.2023.13.3.3.

10. Srivastava, A., Parmar, V., Patel, S., & Chaturvedi, A. S. (2023), "Adaptive cyber defense: Leveraging neuromorphic computing for advanced threat detection and response", Proceedings of the International Conference on Cybersecurity Science and Systems. https://doi.org/10.1109/ICSCSS57650.2023.10169393.

Стаття надійшла до редакції 03.12.2024 р.