УДК 004.056.5 DOI: 10.31673/2412-4338.2020.015367

Грищук О. М., Грищук Р. В., Охрімчук В. В.
Житомирський військовий інститут імені С. П. Корольова, Житомир

ВЕРИФІКАЦІЯ УЗАГАЛЬНЕНОЇ ДИФЕРЕНЦІЙНО-ІГРОВОЇ МОДЕЛІ ШАБЛОНУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНОЇ КІБЕРАТАКИ

Кіберпростір, як електронне комунікаційне середовище, на сьогодні об'єднав в єдину глобальну мережу передачі даних різні за структурою та функціональним призначенням інформаційно-телекомунікаційні системи та їх складові. Невід'ємною ознакою безпечного використання кіберпростору для задоволення життєво важливих інтересів людини і громадянина, суспільства та держави є стан кібербезпеки, який досягається при використанні таких систем. Світовий досвід та досвід України показує, що існуючі кіберзагрози не тільки наростають кількісно, а й проявляються у більш витончених кібератаках, породжуючи при цьому кіберінциденти, наслідки від яких можуть мати непередбачуваний характер. Практика забезпечення кібербезпеки показує, що особливо високі вимоги до її забезпечення нині висуваються на об'єктах критичної інфраструктури держави. Тому виконання таких вимог потребує пошуку нових та дієвих механізмів її забезпечення. Існуючі технології, на які покладаються завдання із забезпечення кібербезпеки, в своїй сукупності становлять систему інформаційної безпеки об'єкта критичної інфраструктури в контурі функціонування якого задіяно інформаційно-телекомунікаційну систему або її складові. Незважаючи на достатньо ефективну роботу систем інформаційної безпеки інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, більшість з них функціонально неспроможні виявляти потенційно небезпечні кібератаки, сигнатури на які відсутні. Це пов'язано з недоліками принципів, покладених в основу їх функціонування. Інші, альтернативні підходи, які зорієнтовані на виявлення потенційно небезпечних кібератак хоч і мають місце, але не спроможні із заданим ступенем достовірності виявляти такі кібератаки. Тому питання про створення та особливо верифікації нових моделей шаблонів потенційно небезпечних кібератак є важливим як з наукової, так і практичної точки зору. В статті запропоновано один з підходів до верифікації узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки. У результаті всебічного дослідження: обґрунтовано її адекватність; збіжність з відомими результатами; встановлено переваги, порівняно із найближчими аналогами, які використовуються в системах інформаційної безпеки інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Ключові слова: *верифікація, узагальнена диференційно-ігрова модель, шаблон потенційно небезпечної кібератаки, система інформаційної безпеки, інформаційно-телекомунікаційна система, об'єкт критичної інфраструктури.*

Hryshchuk O. M., Hryshchuk R. V., Okhrimchuk V. V.
Korolyov Zhytomyr Military Institute, Zhytomyr

THE VERIFICATION OF GENERALIZED DIFFERENTIAL-GAME MODEL OF POTENTIALLY DANGEROUS PATTERN OF CYBER-ATTACK

Today, cyberspace has integrated information and telecommunications systems and their components, which differ in structure and operation, into a single global data network. An integral feature of the safe use of cyberspace to meet the vital interests of man and citizen, society and the state is the state of cybersecurity. It is achieved by using such systems. The world experience and the experience of Ukraine show that the existing cyber threats not only increase in number, but also manifest themselves in more sophisticated cyber-attacks. This creates cyber incidents, the consequences of which can be unpredictable. The practice of cybersecurity shows that especially high requirements for its provision are currently being put forward at critical infrastructure facilities in the country. That`s why the implementation of such requirements requires the search for new and effective mechanisms to ensure it. Existing technologies, which are responsible for cybersecurity, together constitute the information security system of the critical infrastructure. Despite the sufficiently effective operation of information security systems of information and telecommunication systems of critical

infrastructure, most of them are unable to detect potentially dangerous cyber-attacks, for which there are no patterns. This is due to the shortcomings of the principles underlying their operation. Other alternative approaches that focus on detecting potentially dangerous cyber-attacks are not able to detect such cyber-attacks with a given degree of reliability. Therefore, the question of creating and verifying new models of patterns of potentially dangerous cyber-attacks is important from both a scientific and practical point of view. The article proposes an approach to the verification of generalized differential-game model of potentially dangerous pattern of cyber-attack. As a result of the study substantiated the adequacy of the model, its convergence with the known results and advantages compared to the closest analogues used in modern information security systems of information and telecommunications systems of critical infrastructure of the state.

Keywords: *verification, generalized differential-game model, pattern of potentially dangerous cyber-attack, information security system, information and telecommunication system, object of critical infrastructure*

Грищук О. М., Грищук Р. В., Охримчук В. В.

Житомирский военный институт имени С. П. Королёва, Житомир

ВЕРИФИКАЦИЯ ОБОБЩЕННОЙ ДИФФЕРЕНЦИАЛЬНО-ИГРОВОЙ МОДЕЛИ ШАБЛОНА ПОТЕНЦИАЛЬНО ОПАСНОЙ КИБЕРАТАКИ

Киберпространство, как электронная коммуникационная среда, сегодня объединило в единую глобальную сеть передачи данных разные по структуре и функциональному назначению информационно-телекоммуникационные системы и их составляющие. Неотъемлемым признаком безопасного использования киберпространства для удовлетворения жизненно важных интересов человека и гражданина, общества и государства является состояние кибербезопасности, которое достигается при использовании таких систем. Мировой опыт и опыт Украины показывает, что существующие киберугрозы не только нарастают количественно, но и проявляются в более изощренных кибератаках, порождая при этом киберинциденты, последствия которых могут иметь непредсказуемый характер. Практика обеспечения кибербезопасности показывает, что особенно высокие требования к ее обеспечению сейчас выдвигаются на объектах критической инфраструктуры государства. Поэтому выполнение таких требований требует поиска новых и действенных механизмов ее обеспечения. Существующие технологии, на которые возлагаются задачи по обеспечению кибербезопасности, в своей совокупности составляют систему информационной безопасности объекта критической инфраструктуры, в контуре функционирования которого задействована информационно-телекоммуникационная система или ее составляющие. Несмотря на достаточно эффективную работу систем информационной безопасности информационно-телекоммуникационных систем объектов критической инфраструктуры, большинство из них функционально не могут выявлять потенциально опасные кибератаки, сигнатуры на которые отсутствуют. Это связано с недостатками принципов, положенных в основу их функционирования. Другие, альтернативные подходы, ориентированные на выявление потенциально опасных кибератак, хотя и имеют место быть. Не взирая на это они не в состоянии с заданной степенью достоверности выявлять такие кибератаки. Поэтому вопрос о создании и особенно верификации новых моделей шаблонов потенциально опасных кибератак является важным как с научной, так и практической точки зрения. В статье предложен один из подходов к верификации обобщенной дифференциально-игровой модели шаблона потенциально опасной кибератаки. В результате всестороннего исследования обоснована не только адекватность указанной модели, но и установлена сходимость полученных результатов с известными. Отдельно подчеркнуты преимущества модели по сравнению с ближайшими аналогами, которые закладываются в современные системы информационной безопасности информационно-телекоммуникационных систем объектов критической инфраструктуры государства.

Ключевые слова: *верификация, обобщенная дифференциально-игровая модель, шаблон потенциально опасной кибератаки, система информационной безопасности, информационно-телекоммуникационная система, объект критической инфраструктуры.*

1. Вступ

Повсюдне проникнення інформаційних технологій в усі без винятку сфери діяльності людини, суспільства та держави поряд усіма позитивними аспектами, пов'язаними з їх впровадженням, має й низку ризиків для інформаційної, воєнної та інших складових національної безпеки України [1]. Нерозривний зв'язок, який існує між інформаційними технологіями та інформаційно-телекомунікаційними системами (ІТС) суттєво підвищує існуючий рівень їх небезпеки від кіберзагроз [2]. Особливо гостро стоїть проблема захисту від кібератак тих ІТС або їх складових, які використовуються на об'єктах критичної інфраструктури держави [3]. Це підтверджуються низкою найвідоміших кібератак, які мали місце по відношенню до ІТС об'єктів критичної інфраструктури України, зокрема в енергетичному [4], [5] та транспортному [6] секторах, секторі безпеки та оборони [7], [8] тощо. Саме тому захист від кібератак ІТС об'єктів критичної інфраструктури є нагальною потребою сьогодення в контексті забезпечення їх кібербезпеки, як складової інформаційної безпеки держави. Таким чином, небезпечний характер наслідків від кібератак на ІТС об'єктів критичної інфраструктури висуває підвищені вимоги до якості функціонування їх систем інформаційної безпеки. Отже, підвищення якості функціонування систем інформаційної безпеки ІТС таких об'єктів є *актуальною проблемою* сьогодення.

2. Аналіз літературних даних і постановка проблеми

Ключовою вимогою до якості функціонування систем інформаційної безпеки ІТС об'єктів критичної інфраструктури поряд з усіма іншими відомими вимогами щодо захисту інформації в ІТС [9], [10] [11] та ін. й вимогами щодо забезпечення кібербезпеки [12] та [13], є вимога щодо захисту від кібератак "нульового дня" [14]. Такий захист перш за все повинен полягати в можливості системи інформаційної безпеки ІТС об'єкта критичної інфраструктури ефективно виявляти кібератаки, сигнатури на які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту. У подальшому кібератаки, шаблони поведінки на які є невідомими тут і далі пропонується називати шаблонами потенційно небезпечної кібератаки [15].

Аналіз принципів побудови систем інформаційної безпеки ІТС, які ґрунтуються на сигнатурних методах виявлення кібератак [16] показав, що класичний підхід в основу якого покладено виявлення кібератак за їх сигнатурами не може бути використаний в системах безпеки об'єктів критичної інфраструктури. Основним недоліком, який унеможливлює його застосування є те, що сигнатури – шаблони кібератак розробляються вже постфактум після того, як така кібератака відбулася.

На сьогодні, як показали результати аналізу останніх досліджень [17]–[25] та ін. можна стверджувати, що найбільш перспективним є підхід до побудови систем інформаційної безпеки ІТС об'єктів критичної інфраструктури, який ґрунтується на евристичних методах аналізу подій в системі. Але поряд з цим евристичні методи аналізу подій в системі не дають повної гарантії виявлення кібератак "нульового дня", оскільки не виключаються хибні спрацювання системи інформаційної безпеки. Тому розробленню повинен підлягати такий метод побудови шаблонів потенційно небезпечних кібератак, на основі якого вдасться створювати відповідні адекватні моделі, що доповнюватимуть відомі сигнатури. Як відомо з відкритих джерел нині вже зроблено спробу формалізувати завдання з розроблення такого методу [26], визначено джерела первинних даних для розроблення шаблонів потенційно небезпечних атак [27], а також запропоновано відповідну модель [28]. При цьому, згадана модель та похідні від неї й досі не були верифікованими.

3. Мета і задачі дослідження

Метою дослідження є верифікація та дослідження узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки.

Для досягнення поставленої мети пропонується вирішити такі завдання:

– проаналізувати підходи до верифікації моделей та обґрунтувати спосіб верифікації узагальненої диференціально-ігрової моделі шаблону потенційно небезпечної кібератаки;

– спланувати та провести модельний експеримент;

– проаналізувати результати модельного експерименту, зробити висновки про адекватність досліджуваної моделі та обґрунтувати рекомендації з її практичного використання.

4.1. Аналіз підходів до верифікації моделей та обґрунтування способу верифікації узагальненої диференціально-ігрової моделі шаблону потенційно небезпечної кібератаки

Під верифікацією в контексті дослідження пропонується розуміти процес надання об'єктивних доказів того, що модель, яка досліджується відповідає встановленим вимогам. Така інтерпретація в цілому не суперечить загальноприйнятому розумінню сутності процесу верифікації, зміст якого визначено в Міжнародному словнику з метрології [29].

Вивчення літературних джерел, присвячених питанням верифікації моделей шаблонів кібератак показує, що на сьогодні можливо виокремити кілька основних підходів до верифікації.

Перший підхід до верифікації ґрунтується на загальноприйнятій міжнародній базі стандартів з кібербезпеки. При цьому основними стандартами з кібербезпеки, які можуть бути використані для верифікації прийнято вважати стандарти серій *ISO/IEC 27001, ISO/IEC 27002, NERC, NIST, 4ISO 15408, ANSI/ISA 62443* (*The ISA Security Compliance Institute Conformity Assessment Program* та *SO 17065 and Global Accreditation*) та *IEC 62443* (*IEC 62443 Certification Programs* та *Global Accreditation and Recognition*) [30]. Тобто даний підхід є набором стандартизованих безпекових процедур, політик та технологій, спрямованих на зменшення ризиків від прояву кібератак. Незважаючи на цілу низку існуючих стандартів, верифіковані за ними шаблони кібератак, інтегровані в системи інформаційної безпеки ІТС, дозволяють виявляти кібератаки нульового дня з ймовірністю не вище 0,68 [31].

Другий підхід до верифікації шаблонів кібератак має прикладний характер. Наприклад, міжнародною Організацією зі стандартів тестування шкідливого програмного забезпечення *AMTSO* просувається ідеологія верифікації цілих систем інформаційної безпеки разом з шаблонами відомих та потенційно небезпечних кібератак [32]. Згаданою організацією на безоплатній основі надається ряд інструментів для верифікації моделей шаблонів. Незважаючи на існуючі можливості, даний підхід, як і попередній, також не може бути використаний в роботі через локальний характер моделі, що верифікується.

Третій підхід можна віднести до категорії академічних підходів до верифікації. Згідно з ним на сьогодні існує низка академічних досліджень присвячених верифікації шаблонів кібератак на основі теорії нечітких множин [33], методу "перевірки на моделі" (*Model Checking*), який ґрунтується на темпоральній логіці, що пов'язує часові параметри моделі, яка верифікується [34], методів математичного моделювання з прикладною реалізацією в пакеті прикладних програм *MatLab* (з використанням пакету *Simulink*) [35], технології імітаційного моделювання, що ґрунтується на стохастичних мережах Петрі [36], методах математичної статистики [37], верифікація на модельному прикладі [38] тощо. Як видно, академічний підхід до верифікації має більш локальний характер. Тобто, його використання, з одного боку, не потребує прив'язки до тих чи інших безпекових стандартів, а з іншого – створення, впровадження, супроводження та модернізації систем інформаційної безпеки ІТС. Даний підхід слід розглядати як частинний випадок одного з підходів, описаних вище. Таким чином, процедурно сутність верифікації шаблонів потенційно небезпечних кібератак можна відобразити наступною послідовністю подій:

– верифікація на основі академічного підходу;

– прикладна верифікація;

– верифікація на основі стандартів.

Отже, дотримуючись описаної вище послідовності, а також враховуючи наявну апріорну інформацію про узагальнену диференційно-ігрову модель шаблону потенційно небезпечної кібератаки, пропонується наступний спосіб верифікації. На першому кроці її пропонується провести на основі академічного підходу. При цьому з описаних та проаналізованих вище академічних підходів до верифікації [33]–[38] верифікацію пропонується здійснити на основі методів математичного моделювання, але на відміну від прикладного пакету, описаного в [35]

вважається за доцільне використання системи комп'ютерної математики *Maple*. Використання системи комп'ютерної математики *Maple* дозволить здійснити аналітичні та числові розрахунки з одночасною візуалізацією останніх, що є перевагою порівняно з іншими пакетами прикладних програм [39].

4.2. Планування та проведення модельного експерименту

Метою проведення експерименту є одержання на основі обраного вище способу верифікації набору вихідних даних, достатніх для прийняття рішення про адекватність узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки.

Модельний експеримент пропонується здійснити з дотриманням основних вимог, що висуваються до його проведення, а саме розробленню підлягає:

– план експерименту;

– програма експерименту.

Окремим пунктом, що стосується проведення модельного експерименту є обговорення одержаних результатів та обґрунтування рекомендацій з практичного використання верифікованої моделі.

Розглянемо послідовно визначені пункти.

До ***плану модельного експерименту*** пропонується включити такі пункти, як:

– мету експерименту;

– задачі експерименту;

– обґрунтування вибору множини контрольованих параметрів;

– обґрунтування вибору засобу збору експериментальних даних, місця та часу проведення експерименту.

Метою модельного експерименту є верифікація (перевірка адекватності) узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки, який планується до використання в системах інформаційної безпеки ІТС об'єктів критичної інфраструктури держави. *Об'єктом дослідження* визначено рівень захищеності ІТС, який досягається за рахунок використання її системою інформаційної безпеки шаблону потенційно небезпечної кібератаки при різних стратегіях кіберзахисту та кібернападу, під час якого реалізується той чи інший вид кібератаки.

Для досягнення мети модельного експерименту визначимо такі його *основні задачі*:

– розроблення плану та схеми експерименту;

– збір експериментальних даних шляхом проведення математичного моделювання на системі комп'ютерної математики *Maple*;

– оброблення експериментальних даних;

– дослідження адекватності узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки та обґрунтування рекомендацій з її практичного застосування в системах інформаційної безпеки ІТС об'єктів критичної інфраструктури.

Обґрунтування вибору множини контрольованих параметрів. Керуючись відомою методологією синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу, вперше запропонованою в [40], у якості множини контрольованих параметрів для верифікації узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки в термінології диференціальних ігор [41], оберемо стратегії гравців кібернападу λ та кіберзахисту μ відповідно

$$\lambda_{\min} \le \lambda_i \le \lambda_{\max},\ i = \overline{1,n}, \tag{1}$$

$$\mu_{\min} \le \mu_j \le \mu_{\max},\ j = \overline{1,m}. \tag{2}$$

Фізично стратегії гравців (1) та (2) описують інтенсивність трафіку в ІТС [42]. На прикладі кібератак типу *SYN-flood* або *ICMP-flood* інтенсивність трафіку – це кількість пакетів даних на секунду.

Обґрунтування вибору засобу збору та оброблення експериментальних даних, місця та часу проведення експерименту. Як засіб збору та оброблення експериментальних даних обрано персональний комп'ютер з характеристиками: процесор *Intel(R) Core(TM) i5-7200U*;

CPU 2.50 GHz, 2.70 GHz; оперативна пам'ять *8 ГБ.* Місцем збору експериментальних даних обрано Кіберполігон кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С П. Корольова (ЖВІ). Час для збору експериментальних даних: 27.04.2020 р.

Програма модельного експерименту регламентує порядок його організації та проведення. Так гравцем кібернападу (КБн) через центр командування і управління ботами C&C Web-сервера моделюються запити на сайт об'єкта критичної інфраструктури. На рис. 1 як приклад ІТС об'єкта критичної інфраструктури обрано інформаційний ресурс ЖВІ.

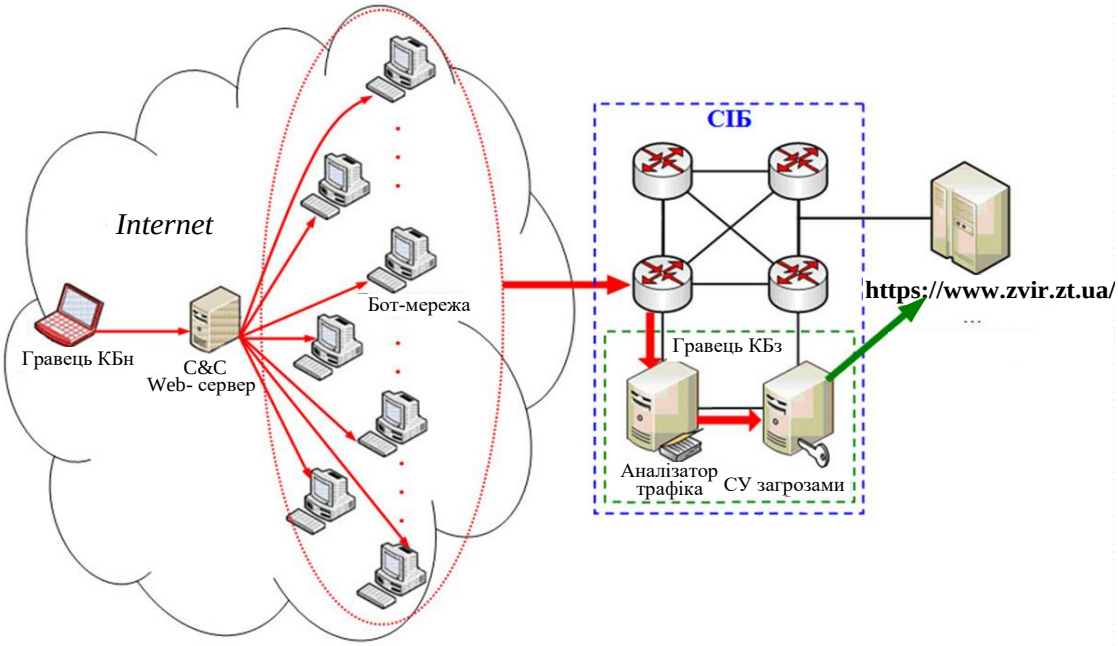

Рис. 1. Схема модельного експерименту

Гравець кіберзахисту (КБз) для захисту зазначеного інформаційного ресурсу використовує систему інформаційної безпеки з узагальненим диференційно-ігровим шаблоном потенційно небезпечної кібератаки $P_0(t)$ вигляду:

$$P_0(t)=1-t(\mu_{СІБ}+\mu_{ІТС})+\frac{1}{2}t^2\left(\lambda_{СІБ}\mu_{СІБ}+\lambda_{ІТС}\mu_{ІТС}+\mu_{СІБ}^2+2\mu_{СІБ}\mu_{ІТС}+\mu_{ІТС}^2\right)-$$
$$-\frac{1}{6}t^3\left(\lambda_{ІТС}^2\mu_{ІТС}+3\lambda_{ІТС}\mu_{ІТС}^2+2\lambda_{ІТС}\mu_{ІТС}\mu_{СІБ}+\lambda_{СІБ}^2\mu_{СІБ}+2\lambda_{СІБ}\mu_{ІТС}\mu_{СІБ}+\right. \quad (3)$$
$$\left.+3\lambda_{СІБ}\mu_{СІБ}^2+\mu_{ІТС}^3+3\mu_{ІТС}^2\mu_{СІБ}+3\mu_{СІБ}^2\mu_{ІТС}+\mu_{СІБ}^3\right),$$

де $P_0(t)$ – узагальнений диференційно-ігровий шаблон потенційно небезпечної кібератаки, який описує ймовірність перебування ІТС в незахищеному стані у визначений момент часу t;

$\lambda_{СІБ}$, $\lambda_{ІТС}$ – стратегії гравця кібернападу на систему інформаційної безпеки та інформаційний ресурс ІТС відповідно, пак. дан./с.;

$\mu_{СІБ}$, $\mu_{ІТС}$ – стратегії гравця кіберзахисту системою інформаційної безпеки та інформаційного ресурсу ІТС відповідно на основі обраного шаблону $P_0(t)$, пак. дан./с.

Під час модельного експерименту для моніторингу та виявлення потенційно небезпечної кібератаки в системі інформаційної безпеки передбачається використання відповідного узагальненого диференційно-ігрового шаблону (3). Системою інформаційної безпеки передбачається здійснення аналізу вхідного трафіка на предмет його порівняння з шаблоном потенційно небезпечної кібератаки. У разі збіжності система повинна здійснювати виявлення такої кібератаки з заданим ступенем достовірності ($\geq 51\%$). В реальних умовах функції фільтрації шкідливого трафіку можуть здійснюватися на прикладному рівні, як приклад із застосуванням системи управління *Threat Management System* програмно-апаратного

комплексу *Arbor Peakflow SP* (див. рис. 1).

Проведення модельного експерименту.

1. Узагальнений диференційно-ігровий шаблон потенційно небезпечної кібератаки (1), який верифікується відповідає графовій моделі, поданій на рис. 2.

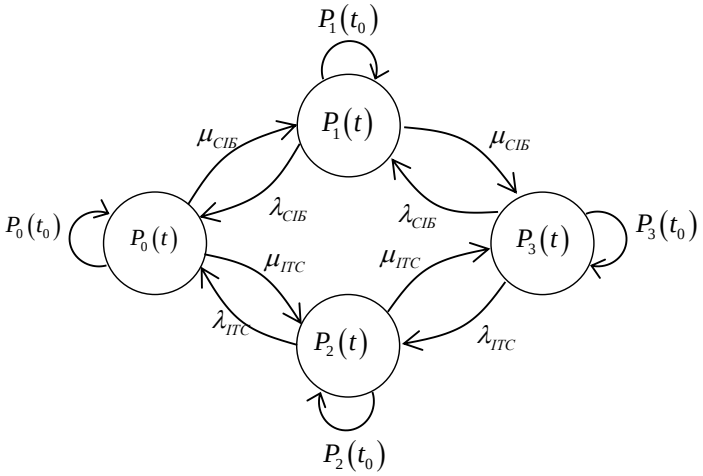

Рис. 2. Узагальнена графова модель шаблону потенційно небезпечної кібератаки

При виборі гравцями оптимальних стратегій

$$\lambda_{СІБ}^{opt} = \frac{1}{3T};\ \lambda_{ІТС}^{opt} = \frac{1}{3T};\ \mu_{СІБ}^{opt} = \frac{2}{3T};\ \mu_{ІТС}^{opt} = \frac{2}{3T} \tag{4}$$

узагальнена диференційно-ігрова модель шаблону потенційно небезпечної (3) набуває вигляду:

$$P_0(t) = 1 - \frac{4}{3}\left(\frac{t}{T}\right) + \frac{10}{9}\left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3, \tag{5}$$

де T - тривалість кібератаки на інтервалі спостереження t, $t \in (0, T]$, с.

При цьому рівень захищеності ІТС I від потенційно небезпечної кібератаки при виборі гравцями оптимальних стратегій (4) за шаблоном (5) дорівнюватиме 0,46, тобто $I = 0,46$. У всіх інших випадках при відхиленні гравців від оптимальних стратегій рівень захищеності ІТС від потенційно небезпечної кібератаки, яка описуватиметься шаблоном (4) підвищуватиметься, що приймається як гіпотеза.

2. Збір експериментальних даних шляхом проведення математичного моделювання на системі комп'ютерної математики *Maple.* Для збору експериментальних даних пропонується скористатися матрицею верифікації, загальний вигляд якої подано в табл. 1. В якості критерію прийняття рішення про адекватність моделі обрано принцип Парето. Як варіюємі параметри обрано діапазон зміни стратегій гравців від оптимальних в діапазоні від 0% до 20% з кроком 10%.

Використання системи комп'ютерної математики *Maple* згідно з матрицею верифікації дозволило одержати експериментальні дані, які подано у табл. 2.

5. Обговорення результатів верифікації узагальненої диференціально-ігрової моделі та обґрунтування рекомендацій з її практичного використання

Систематизуємо одержані вище в результаті модельного експерименту дані (див. табл. 2) та подамо їх для наглядності у вигляді ряді рис. 3. Подані у табл. 2 та рис. 3 дані дозволяють зробити такі основні висновки щодо адекватності моделі, яка верифікується:

– *по-перше,* модель є адекватною на усьому інтервалі спостереження T протягом якого моделюється потенційно небезпечна кібератака. Графіки ймовірності перебування ІТС в незахищеному стані під час потенційно небезпечної кібератаки при виборі гравцями різних стратегій перебувають у визначених межах (див. рис. 3 а);

Таблиця 1

Матриця верифікації

Гравець			
кіберзахисту		*кібернападу*	
$\mu_{СІБ}$	$\mu_{ІТС}$	$\lambda_{СІБ}$	$\lambda_{ІТС}$
при виборі гравцями оптимальних стратегій			
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
при відхиленні гравців на 10% від оптимальних стратегій			
$1{,}1\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}1\cdot\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
$1{,}1\cdot\mu_{СІБ}^{opt}$	$1{,}1\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}1\cdot\lambda_{ІТС}^{opt}$
при відхиленні гравців на 20% від оптимальних стратегій			
$1{,}2\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$0{,}2\cdot\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$
$1{,}2\cdot\mu_{СІБ}^{opt}$	$1{,}2\cdot\mu_{ІТС}^{opt}$	$\lambda_{СІБ}^{opt}$	$0{,}2\cdot\lambda_{ІТС}^{opt}$

Таблиця 2

Експериментальні дані щодо верифікації моделі,
зібрані за допомого системи комп'ютерної математики Maple

Гравець				Рівень захищеності ІТС
кіберзахисту		*кібернападу*		
$\mu_{СІБ}$, пак. дан./с	$\mu_{ІТС}$, пак. дан./с	$\lambda_{СІБ}$, пак. дан./с	$\lambda_{ІТС}$, пак. дан./с	I
при виборі гравцями оптимальних стратегій				
0,67	0,67	0,33	0,33	0,46
при відхиленні гравців на 10% від оптимальних стратегій				
0,73	0,67	0,33	0,33	0,48
0,73	0,73	0,33	0,33	0,51
0,73	0,73	0,03	0,33	0,51
0,73	0,73	0,03	0,03	0,51
0,67	0,73	0,33	0,33	0,48
0,67	0,73	0,03	0,33	0,49
0,67	0,73	0,03	0,03	0,49
0,67	0,67	0,03	0,33	0,47
0,67	0,67	0,03	0,03	0,47
0,73	0,67	0,03	0,03	0,49
0,67	0,67	0,33	0,03	0,47
0,73	0,67	0,33	0,03	0,49
0,73	0,73	0,03	0,03	0,51
при відхиленні гравців на 20% від оптимальних стратегій				
0,8	0,67	0,33	0,33	0,51
0,8	0,8	0,33	0,33	0,55
0,8	0,8	0,07	0,33	0,55
0,8	0,8	0,07	0,07	0,55
0,67	0,8	0,33	0,33	0,51
0,67	0,8	0,07	0,33	0,51
0,67	0,8	0,07	0,07	0.51
0,67	0,67	0,07	0,33	0,46
0,67	0,67	0,07	0,07	0,47
0,8	0,67	0,07	0,07	0.51
0,67	0,67	0,33	0,07	0,46
0,8	0,67	0,33	0,07	0.51
0,8	0,8	0,33	0,07	0,55

– *по-друге,* початкові умови, для яких розроблено узагальнену диференційно-ігрову модель шаблону потенційно небезпечної кібератаки (3) та її модифікації при виборі гравцями кіберзахисту та кібернападу різних стратегій (4) у визначеному діапазоні (1) та (2) передбачають найгірший з позиції захисту варіант розвитку подій в ІТС, тобто варіант за якого в ІТС є потенційно вразливою від кібератаки нульового дня, тобто $P_0\left(t_0=0\right)=1$ (див. рис. 3 а);

– по-третє, модель є чутливою до вхідних даних, що підтверджується виглядом графіків ймовірності перебування ІТС в незахищеному стані під час потенційно небезпечної кібератаки не тільки при виборі гравцями оптимальних стратегій (3) та (4), а й відхиленні від них в діапазоні до 20 % як у бік збільшення, так і зменшення;

– по-четверте, результати верифікації показують, що у разі відхилення гравця

кібернападу від своєї оптимальної стратегії кібернападу на систему інформаційної безпеки $\lambda_{СІБ}^{opt}$ та ІТС $\lambda_{ІТС}^{opt}$ об'єкта критичної інфраструктури ймовірність перебування системи в незахищеному стані зменшується. При цьому збільшується рівень захищеності ІТС за рахунок більш оперативного – до 1,6 рази (з $0,37 \cdot T$ с. до $0,58 \cdot T$ с.) реакції системи на потенційно небезпечну кібератаку, що як наслідок призводить до її виявлення (див. рис. 3 а);

– по-п'яте, для досягнення порогу виявлення в $0,51$ системі інформаційної безпеки та ІТС достатньо на 10 % і більше відхилитися від свої оптимальних стратегій $\mu_{СІБ}^{opt}$ та ІТС $\mu_{ІТС}^{opt}$ відповідно (див. рис. 3 б);

– по-шосте, верифікація моделі (див. рис. 3 б) на кращому за ефективністю серед діючих зразків систем інформаційної безпеки *NOD32 Eset*, які використовується на об'єктах критичної інфраструктури, дозволяє стверджувати таке. З одного боку будь-яка ІТС обєкта критичної інфраструктури вразлива від потенційно небезпечної кібератаки (рівень захищеності системи не перевищує 0,46). З іншого боку – модель має запас стійкості щодо виявлення потенційно небезпечних кібератак, що на практиці забезпечуватиме виявлення потенційно небезпечних кібератак не гірше за найближчі серед найкращих аналогів. У разі варіювання параметрами моделі в межах заданих обмежень використання моделі дозволяє перевищувати відомі найкращі аналоги за ефективністю до 15 % (див. рис. 3 б).

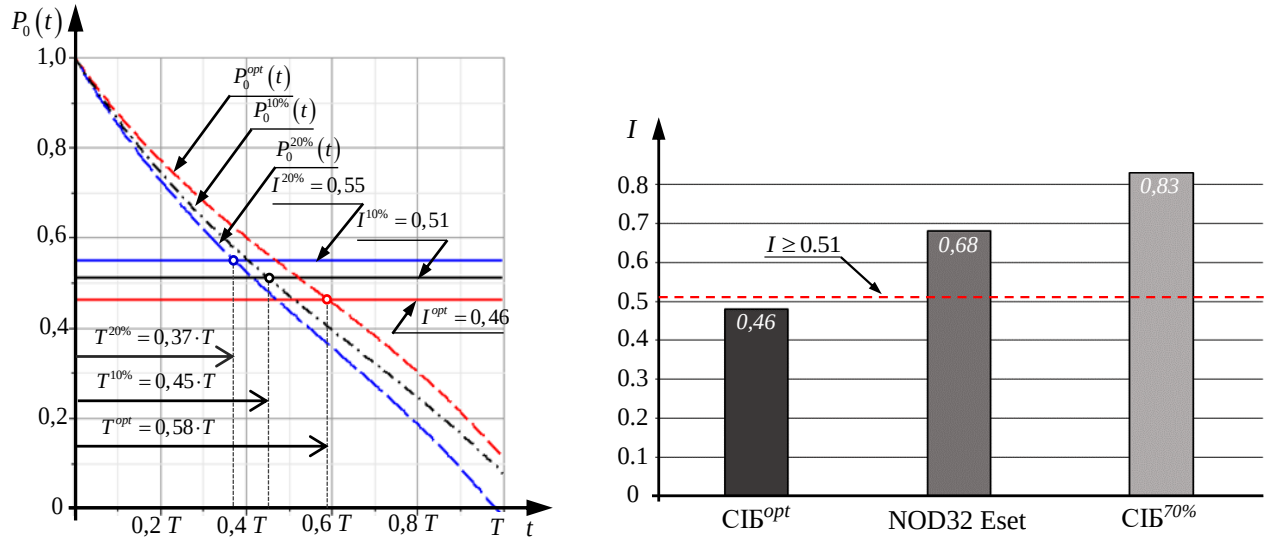

Рис. 3. Результати верифікації узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки: а – графік ймовірності перебування ІТС в незахищеному стані під час потенційно небезпечної кібератаки при виборі гравцями різних стратегій; б – рівень захищеності ІТС при використанні СІБ узагальненого диференційно-ігрового шаблону потенційно небезпечної кібератаки

Використання узагальненої диференційно-ігрової моделі на практиці дозволяє одержати ряд важливих рекомендацій:

– по-перше, через потенційну вразливість ІТС об'єктів критичної інфраструктури до нових кібератак, на які відсутні сигнатури доцільно використовувати кілька механізмів захисту як тих, які реалізує власне система інформаційної безпеки, так і тих які функціонально закладені на програмному рівні комплексу засобів захисту ІТС (розмежування доступу на підставі атрибутів доступу тощо);

– по-друге, підвищення захищеності ІТС від потенційно небезпечних кібератак досягається комплексним використанням джерел первинних даних для побудови шаблонів потенційно небезпечних кібератак (*KDD-99*, *CAPEC*, стандартні функціональні профілі захищеності, різноманітні класифікатори кібератак тощо);

– по-третє, для проходження системою інформаційної безпеки порогу виявлення $I \geq 0,51$ рекомендується підвищувати вдвічі частоту моніторингу подій в системі від мінімально встановлених вендором характеристик. Наприклад, якщо частота моніторингу подій в системі встановлена один раз на добу, то згідно наданих рекомендацій вона повинна складати не менше двох разів.

6. Висновки

У результаті проведеного дослідження одержано такі основні наукові та практичні результати:

– проведено аналіз сучасних підходів до верифікації шаблонів потенційно небезпечних кібератак. На основі їх переваг та недоліків обґрунтовано вибір академічного підходу до верифікації, який ґрунтується на загальновідомих принципах математичного моделювання;

– з додержанням усіх необхідних процедур, які передбачені при проведенні експерименту з заданим ступенем достовірності верифіковано узагальнену диференційно-ігрову моделі шаблону потенційно небезпечної кібератаки. Результати верифікації показали, що усі гіпотези та вихідні припущення, які було сформульовано на етапі постановки задачі розроблення моделі є справедливими. Точність моделювання за верифікованою моделлю відповідає необхідним вимогам, оскільки результати, які одержують на основі моделі (ймовірність перебування системи в захищеному стані та рівень захищеності від потенційно небезпечних кібератак) є збіжними з результатами інших відомих досліджень;

– практичне використання запропонованої моделі дозволяє вивчати процеси кіберзахисту та кібернападу в ІТС об’єктів критичної інфраструктури при різних вхідних даних, не проводячи натурного експерименту через його потенційну небезпеку для об’єкта. Модель, що верифікована є першим кроком на шляху розроблення фізичних шаблонів потенційно небезпечних кібератак, наприклад за методологією KDD-99, CAPEC або ін.

Список використаної літератури

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.

2. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир: ЖНАЕУ, 2019. 280 с.

3. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах. Сучасна спеціальна техніка. 2011. № 1 (24). С. 61–66.

4. Грищук Р., Галущенко А., Барановский А. Кибервызов: по когтю узнать льва. НТЦ Психея: Терминал. 2017. http://oilreview.kiev.ua/2017/12/18/kibervyzov-po-kogtyu-uznat-lva/ (дата звернення 02.03.2020).

5. Корченко А. О. Методи ідентифікації аномальних станів для систем виявлення вторгнень : монографія. Київ: ЦП “Компринт”, 2019. 361 с.

6. Лахно В. А. Кібербезпека комп’ютерних систем транспорту. Електротехнічні та комп’ютерні системи. 2016. № 21 (97). С. 76–80.

7. Uroburos : Highly Complex Espionage Software With Russian Roots. G Data Discovers Alleged Intelligence Agency Software https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf (дата звернення 02.03.2020).

8. Хакерські атаки на Україну [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2017. URL: https://is.gd/6lkWHY (дата звернення: 02.03.2020).

9. Закон України від 5 липня 1994 року № 80/94-ВР “Про захист інформації в інформаційно-телекомунікаційних системах”. (із змінами). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. (дата звернення: 02.03.2020).

10. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”. https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF. (дата звернення: 02.03.2020).

11. НД ТЗІ 1.1-002-99. “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу”. https://tzi.com.ua/downloads/1.1-002-99.pdf. (дата звернення: 02.03.2020).

12. Закон України 5 жовтня 2017 року № 2163-VIII “Про основні засади забезпечення кібербезпеки України”. https://zakon.rada.gov.ua/laws/show/2163-19. (дата звернення: 02.03.2020).

13. Указ Президента України від 15 березня 2016 року № 96/2016 “Стратегія кібербезпеки України”. https://zakon.rada.gov.ua/laws/show/96/2016. (дата звернення: 02.03.2020).

14. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 “Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури”. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF. (дата звернення: 02.03.2020).

15. Грищук Р. В., Охрімчук В. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак. Безпека інформації. 2015. Том 21. (№ 3). С. 276–282.

16. Чередниченко О.Ю., Процюк Ю. О., Шемендюк О. В., Мальцева І. Р. Способи вдосконалення схем захисту від кібернетичних атак в інформаційно-телекомунікаційних системах. Збірник наукових праць ВІТІ. 2019. № 3. С. 103–109.

17. Лукацкий А. Можно ли защититься от 90 % кибератак одним решением. 2019. https://www.cnews.ru/special_project/2019/cisco/. (дата звернення: 02.03.2020).

18. Song J., Lee Y., Kim K., Kim S., Kim SK., Choi SS. Automated Verification Methodology of Security Events Based on Heuristic Analysis. International Journal of Distributed Sensor Networks. https://journals.sagepub.com/doi/full/10.1155/2015/817918. (дата звернення: 02.03.2020).

19. Tosh D., Sengupta S., Kamhoua C., Kwiat K., Martin A. An evolutionary game-theoretic framework for cyber-threat information sharing. IEEE International Conference on Communications (ICC). 2015. Pp. 7341–7346.

20. Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них. Фундаментальные исследования. 2017. № 10-3. С. 507–511.

21. Зубок В. Ю., Захарченко О.І., Бєланов Ю.О. Розпізнання аномальних станів в інформаційно-телекомунікаційних системах при нечіткому описі подій. Материалы XVII Международной научно-практической конференции ИТБ-2017. г. Киев, 30 ноября 2017 г. Киев. С. 92–96.

22. Vorobiev S. A., Petrenko I. V., Kovaleva I. K., Abrosimov. Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017. 2017. Pp. 369–371.

23. Detecting script-based malware using emulation and heuristics. Patent No.: US 9 , 858 , 414 B2: US009858414B2. Filed: 10.03.2015; Prior Publication Data: 29.10.2015, US 2015 / 0310212 A1 Oct. 29, 2015.

24. Nguyen T., Wright M., Wellman M., Singh S. Multistage Attack Graph Security Games: Heuristic Strategies,with Empirical Game-Theoretic Analysis. Security and Communication Networks. 2018. Pp. 1–28.

25. Sakhnini J, Karimipour H, Dehghantanha A (2019) Smart Grid Cyber Attacks Detection using Supervised Learning and Heuristic Feature Selection. arXiv preprint arXiv:190703313.

26. Грищук Р. В., Охрімчук В. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак. Безпека інформації. 2015. Т. 21. № 3. С. 276–282.

27. Грищук Р. В. Охрімчук В. В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак. Захист інформації. 2016. Том 18. №1. С. 21–29.

28. Охрімчук В. В. Модель шаблону потенційно небезпечної кібератаки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2018.

№ 1 (35). С. 30–37.

29. Международный словарь по метрологии: основные и общие понятия и соответствующие термины: пер. с англ. и фр. СПб.: НПО «Профессионал», 2010. 82 с.

30. Cybersecurity standards. https://en.wikipedia.org/wiki/Cybersecurity_standards. (дата звернення 03.03.2020).

31. Goodin D. Anti-virus protection gets worse. 2007. https://web.archive.org/web/20110511081703/ http://www.channelregister.co.uk/2007/12/21/dwindling_antivirus_protection/ (дата звернення 03.03.2020).

32. Verify if your desktop security software Detects Potentially Unwanted Applications (PUAs). https://www.amtso.org/feature-settings-check-potentially-unwanted-applications/. (дата звернення 03.03.2020).

33. Корченко О. Г., Терейковський І. А., Казмірчук С. В. Верифікація нейромережевих методів розпізнавання кібератак. Управління розвитком складних систем. 2014. № 17. С. 168–172.

34. Полубелова О. В., Котенко, И. В. Верификация правил фильтрации с временными характеристиками методом “проверки на модели”. Труды СПИИРАН. 2012. Вып. 3 (22). С.113–138.

35. Бритов Г. С. Верификация, валидация и тестирование компьютерных моделей линейных динамических систем. Информационно-измерительные системы. 2013. № 2. С. 75–82.

36. Стеценко И.В. Алгоритм імітації Петрі-об’єктної моделі. Математичні машини і системи. 2012. № 2. №1. С. 154–165.

37. Погосов А. Ю., Деревянко О. В. Модели прикладной информатики учета кинетики кибернетических угроз в системе физической защиты АЭС. Радіоелектроніка, інформатика, управління. 2017. № 2. С. 53–60.

38. Грищук Р. В. Верифікація і дослідження спектральних P- та гібридних P-L-моделей процесу нападу на інформацію. Вісник ЖДТУ. 2009. № 2 (49). С. 69–77.

39. Mathematics-based software & services for education, engineering, and research. https://www.maplesoft.com/. (дата звернення 03.03.2020).

40. Грищук Р. В., Корченко О. Г. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу. Захист інформації. 2012. Том 14, № 3 (56). С. 115–122.

41. Айзекс Р. Дифференциальные игры : монография. М. : Мир. 1967. 479 с.

42. Федевич О. Ю. Інформаційна технологія прогнозування трафіку в комп’ютерних мережах. Автореф. дис. канд. техн. наук. зі спец. 05.13.06 – інформаційні технології. Львів, Національний університет “Львівська політехніка”. 2018. 20 с.

References

1. Hryshchuk R.V., Danik Yu. H. (2016) Basics of cybernetic security. Monograph. Zhytomyr: ZNAEU. 636 p.

2. Hrabar I. H., Hryshchuk R.V., Molodetska K. V. (2019) Security synergetics: cybernetic and information aspects: monograph. Zhytomyr: ZNAEU. 280 p.

3. Hryshchuk R.V. (2011) Attacks on information in the information and communication systems. Suchasna spetsialna tekhnika. № 1 (24). Pp. 61–66.

4. Hryshchuk R., Halushchenko A., Baranovskyi A. (2017) Cybercall: recognize the lion by the claw. NTTs Psykheia: Terminal. http://oilreview.kiev.ua/2017/12/18/kibervyzov-po-kogtyu-uznat-lva/ (date of the application 02.03.2020).

5. Korchenko A. O. (2019) Methods of identification of anomalous states for intrusion detection systems: monograph. Kiev: TsP “Komprynt”. 361 p.

6. Lakhno V. A. (2016) Cybersecurity of computer transport systems. Electrical and computer systems. № 21 (97). P. 76–80.

7. Uroburos: Highly Complex Espionage Software With Russian Roots. G Data Discovers

Alleged Intelligence Agency Software https://public.gdatasoftware.com/Web/Content/INT/Blog /2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf (date of the application 02.03.2020).

8. Hacker attacks on Ukraine (2017). Wikipedia: [site]. Kiev. URL: https://is.gd/6lkWHY (date of the application: 02.03.2020).

9. Law of Ukraine of July 5, 1994 № 80/94-VR "On information protection in information and telecommunication systems". (with changes). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. (date of the application: 02.03.2020).

10. Resolution of the Cabinet of Ministers of Ukraine of March 29, 2006 № 373 "On Approval of the Rules for Ensuring Information Protection in Information, Telecommunication and Information-Telecommunication Systems". https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=373-2006-%EF. (date of the application: 02.03.2020).

11. ND of TPI 1.1-002-99. "General provisions for the protection of information in computer systems from unauthorized access". https://tzi.com.ua/downloads/1.1-002-99.pdf. (date of the application: 02.03.2020).

12. Law of Ukraine of October 5, 2017 № 2163-VIII "On Basic Principles of Ensuring Cyber Security of Ukraine". https://zakon.rada.gov.ua/laws/show/2163-19. (date of the application: 02.03.2020).

13. Decree of the President of Ukraine of March 15, 2016 № 96/2016 "Cyber security strategy of Ukraine". https://zakon.rada.gov.ua/laws/show/96/2016. (date of the application: 02.03.2020).

14. Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019 № 518 "On approval of the General requirements for cyber protection of critical infrastructure facilities".https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF. (date of the application: 02.03.2020).

15. Hryshchuk R.V., Okhrimchuk V. V. (2015) Setting a scientific task to develop templates for potentially dangerous cyber attacks. Information security, 21(3), p. 276–282.

16. Cherednychenko O., Protsiuk Yu., Shemendiuk O. , Maltseva I. (2019) The ways to improve protection schemes against cyber attacks in information and telecommunication systems. Collection of scientific works VITI. № 3. p. 103–109.

17. Lukatskyi A. (2019) Is it possible to protect against 90% of cyber attacks with one solution. https://www.cnews.ru/special_project/2019/cisco/. (date of the application: 02.03.2020).

18. Song J., Lee Y., Kim K., Kim S., Kim SK., Choi SS. Automated Verification Methodology of Security Events Based on Heuristic Analysis. International Journal of Distributed Sensor Networks. https://journals.sagepub.com/doi/full/10.1155/2015/817918. (date of the application: 02.03.2020).

19. Tosh D., Sengupta S., Kamhoua C., Kwiat K., Martin A. An evolutionary game-theoretic framework for cyber-threat information sharing. IEEE International Conference on Communications (ICC). 2015. P. 7341–7346.

20. Palaeva L.V., Khafizov A.M., Gilyazetdinova A.M., Vakhitova A.R., Davydova K.N., Sirotina E.R. (2017) The main types of cyberattacks on automated process control systems and means of protection against them. Basic research. № 10-3. P. 507–511.

21. Zubok V. Yu., Zakharchenko O. I, Bielanov Yu.O. (2017) The recognition of anomalous stations in informational-telecommunication systems with an unclear description. Materials of the XVII International scientific and practical conference ITS-2017. Kiev. P. 92–96.

22. Vorobiev S. A., Petrenko I. V., Kovaleva I. K., Abrosimov (2017) Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017. 2017. P. 369–371.

23. Detecting script-based malware using emulation and heuristics. Patent No.: US 9, 858, 414 B2: US009858414B2. Filed: 10.03.2015; Prior Publication Data: 29.10.2015, US 2015 / 0310212 A1 Oct. 29, 2015.

24. Nguyen T., Wright M., Wellman M., Singh S. (2018) Multistage Attack Graph Security

Games: Heuristic Strategies,with Empirical Game-Theoretic Analysis. Security and Communication Networks. P. 1–28.

25. Sakhnini J, Karimipour H, Dehghantanha A (2019) Smart Grid Cyber Attacks Detection using Supervised Learning and Heuristic Feature Selection. arXiv preprint arXiv:190703313.

26. Hryshchuk R.V., Okhrimchuk V. V. (2015) Setting a scientific task to develop templates for potentially dangerous cyber attacks. Information security, 21(3). P. 276–282.

27. Hryshchuk R.V., Okhrimchuk V. V. (2016) The sources of primary data for the development potentially dangerous patterns of cyber-attacks. Information protection, 1(18). P. 21–29.

28. Okhrimchuk V. V. (2018) Model of potentially dangerous pattern of cyber-attack. Legal, regulatory and metrological support of the information protection system in Ukraine. Scientific and Technical Collection. № 1 (35). P. 30–37.

29. International Dictionary of Metrology: Basic and General Concepts and Related Terms. SPb: NPO "Professional", (2010). 82 p.

30. Cybersecurity standards. https://en.wikipedia.org/wiki/Cybersecurity_standards. (date of the application 03.03.2020).

31. Goodin D. Anti-virus protection gets worse. 2007. https://web.archive.org/web/20110511081703/ http://www.channelregister.co.uk/2007/12/21/dwindling_antivirus_protection/ (date of the application 03.03.2020).

32. Verify if your desktop security software Detects Potentially Unwanted Applications (PUAs). https://www.amtso.org/feature-settings-check-potentially-unwanted-applications/. (date of the application 03.03.2020).

33. Korchenko O. H., Tereikovskyi I. A., Kazmirchuk S. V. (2014) Verification of neural network methods for cyber attack recognition.. Management of complex systems development. № 17. P. 168–172.

34. Polubelova O. V., Kotenko, I. V. (2012) Verification of filtering rules with time characteristics using the "model validation" method. Works of SPIIRAN. №. 3 (22). P.113–138.

35. Britov G. S. (2013) Verification, validation and testing of computer models of linear dynamic systems. Information measuring systems. № 2. P. 75–82.

36. Stetsenko I. V. (2012) Petri object model simulation algorithm. Mathematical Machines and Systems. № 2. №1. P. 154–165.

37. Pogosov A. Yu., Derevyanko O. V. (2017) Applied informatics models of accounting for the kinetics of cyber threats in the physical protection system of nuclear power plants. Radio electronics, informatics, control. № 2. P. 53–60.

38. Hryshchuk R.V. (2009)Verification and study of spectral P- and hybrid P-L-models of the information attack process. Herald of ZhSTU. № 2 (49). P. 69–77.

39. Mathematics-based software & services for education, engineering, and research. https://www.maplesoft.com/. (date of the application 03.03.2020).

40. Hryshchuk R.V., Korchenko A. O. (2012) Methodology of synthesis and analysis of differential game models and methods of modeling cyber attack processes. Information protection. Volume 14, № 3 (56). P. 115–122.

41. Ajzeks R. Differential games: monograph. M.: Mir. 1967. 479 p.

42. Fedevych O. Yu. (2018) Information technology for forecasting traffic in computer networks. Abstract of the dissertation Ph.D. in the special. 05.13.06 – Information Technology. Lviv. Lviv Polytechnic National University. 20 p.