КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.113123
УДК 004.056.5

Охрімчук Володимир Васильович
старший викладач
Житомирський військовий інститут ім. С. П. Корольова, Житомир, України
ORCID: 0000-0001-7518-9993
okhrimchuk84@ukr.net

УЗАГАЛЬНЕНА ДИФЕРЕНЦІЙНО-ІГРОВА МОДЕЛЬ ШАБЛОНУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНОЇ КІБЕРАТАКИ

Анотація. На сьогодні в світі відбувається суттєве збільшення кількості кібератак. При цьому пропорційно зростає їх технологічна складність. В найближчому майбутньому не виключається поява нових потенційно небезпечних кібератак, що в свою чергу може призвести до погіршення їх виявлення й нейтралізації та, як наслідок, негативно вплинути на рівень захищеності інформаційних та інформаційно-телекомунікаційних систем критичної інформаційної інфраструктури. Виходячи із зазначеного у статті вирішується актуальної задачі виявлення та нейтралізації потенційно небезпечних кібератак яка зводиться до розроблення диференціально-ігрової моделі їх шаблону. В основу створеного шаблону потенційно небезпечної кібератаки запропоновано покласти деннінгову модель захисту інформації та метод диференціально-ігрового моделювання процесів кібернетичного нападу на інформацію. У статті показано, що моделювання шаблону потенційно небезпечної кібератаки здійснюється в умовах апріорної невизначеності вхідних даних, оскільки потенційні кібератаки, які матимуть місце можуть бути досить різноманітними. У зв'язку з цим через неможливість висунення коректних вимог до вхідних параметрів моделі запропоновано як узагальнену модель шаблону потенційно небезпечної кібератаки використовувати гібридну модель. Такий підхід забезпечує моделі, що розробляється, адекватність, тобто збіжність з реальними фізичними явищами та процесами в інформаційних та інформаційно-телекомунікаційних системах. У результаті застосування методу диференціально-ігрового моделювання в аналітичному вигляді узагальнену диференціально-ігрову модель шаблону потенційно небезпечної кібератаки. Таким чином в статті набула подальшого розвитку узагальнена диференціально-ігрова модель шаблону потенційно небезпечної кібератаки в основу якої покладено деннінгову модель захисту інформації та методи диференціально-ігрового моделювання процесів нападу на інформацію, яка на відміну від існуючих враховує інтенсивності дій порушника та сторони, що захищається. Це дає змогу оцінювати рівень незахищеності інформаційно-телекомунікаційної системи в умовах апріорної невизначеності вхідних даних. Застосування моделі на практиці дозволяє створювати ефективні системи захисту інформації , які будуть здатні з мінімальними похибками першого роду виявляти потенційно небезпечні кібератаки в інформаційно-телекомунікаційній системі критичної інфраструктури.

Ключові слова: потенційно небезпечна кібератака; кіберзагроза; шаблон; диференціально-ігрова модель; диференційні перетворення; Р-перетворення; інформаційно-телекомунікаційна система; критична інформаційна інфраструктура;

1. ВСТУП

На сьогодні спостерігається зростання кількості кібератак (КбА) на інформаційні (ІС) та інформаційно-телекомунікаційні системи (ІТС) об'єктів критично інформаційної інфраструктури провідних країн світу та України. При чому відбувається не тільки збільшення їх кількості, а й зростання технологічної складності таких атак. Це в свою чергу призводить до погіршення їх виявлення та нейтралізації,

ISSN 2663 - 4023

що негативно впливає на рівень захищеності ІС та ІТС. Таким чином, задача виявлення та нейтралізації потенційно небезпечних КбА на ІС та ІТС набуває особливої актуальності.

Аналіз останніх досліджень і публікацій. В результаті аналізу досліджень і публікацій [1]–[6] та інших встановлено, що в якості основного елементу системи захисту інформації для запобігання КбА на ІТС, на практиці, як правило, використовуються системи виявлення атак (вторгнень) (СВА). Незважаючи на велике різноманіття таких систем [3], [4] принципи функціонування більшості з них й надалі ґрунтуються на сигнатурних методах побудови та виявлення КбА. Як наслідок, наявність "ефекту запізнення", що виникає через часові затримки, зумовлені потребами пошуку та вироблення потрібної сигнатури (шаблону), суттєво знижує захищеність ІТС від нових потенційно небезпечних КбА, особливо тих з них, які мають високу технологічну складність.

Наразі для побудови шаблонів, як нормальної поведінки так і КбА, на практиці використовуються різні методи. Зокрема до них належать методи статистичного виявлення [7], застосування нейронних мереж [8], теорії масового обслуговування [9] тощо. Поряд з існуючими перевагами більшості з них притаманні такі недоліки як: велика кількість помилкових спрацювань системи, яка обумовлена помилками першого та другого роду; існування потреб тривалого навчання інтелектуальних СЗІ за рахунок великої кількості спроб та помилок. При цьому головним недоліком залишається не можливість виявляти на основі закладених в них моделей потенційно небезпечні КбА [10].

Однією з причин, яка обумовлює відсутність методу побудови шаблонів потенційно небезпечних КбА, є значна кількість вхідних параметрів, їх різна розмірність, та, як наслідок, складність формалізації. Таким чином, задача побудови моделі шаблону потенційно небезпечної КбА має ряд особливостей [11]-[13], головною х яких є невизначеність параметрів моделі.

Отже, з проведеного аналізу встановлено, що задача виявлення потенційно небезпечних КбА на ІС та ІТС може бути зведена до розроблення їх шаблонів, а тому її розв'язання є нагальною потребою сьогодення.

Метою статті є розроблення узагальненої диференціально-ігрової моделі шаблону потенційно небезпечної КбА на ІТС.

2. МЕТОДИКА ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ.

Твердження. Під потенційно небезпечною КбА будемо розуміти атаку, яка призводить до порушення нормального функціонування ІТС, та як наслідок ускладнює або унеможливлює виконання нею завдань за призначенням. При чому вважається, що відомості про таку КбА в базах даних сигнатур СЗІ відсутні.

З метою розроблення узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної КбА розглянемо модель захисту інформації запропоновану Деннінгом [14]. Вона являє собою ієрархічну багаторівневу модель захисту, в центрі якої знаходиться об'єкт захисту (ОЗ), навколо якого створюються рівні захисту у вигляді концентрованих кіл (рис. 1). У якості рівнів захисту СЗІ можуть виступати програмні, апаратні засоби захисту, системи технічного захисту інформації, конструкції будівель тощо [14].

ISSN 2663 - 4023

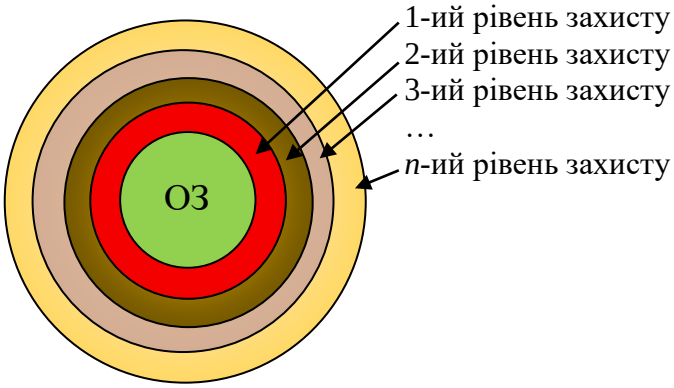

Рис. 1. Модель багаторівневого захисту (за Деннінгом)

У даній роботі, на відміну від відомих моделей, пропонується обмежитися виключно програмними засобами СЗІ та ІТС. Тому модель багаторівневого захисту в умовах апріорної невизначеності (див. рис. 1) може бути зведена до однорівневої системи захисту та надання у вигляді рис. 2.

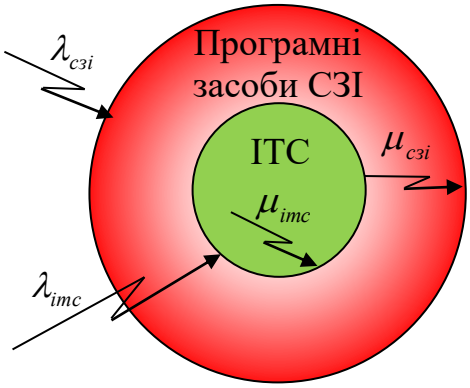

Рис. 2. Однорівнева модель захисту інформаційно-телекомунікаційної системи в умовах апріорної невизначеності

Процес проведення порушником КбА та захисту від неї стороною, що захищається, в загальному випадку може бути охарактеризований деякими параметрами. До них можна віднести інтенсивності виникнення та реалізації загроз в СЗІ – $\lambda_{сзі}$ та в ІТС – λ_{imc} відповідно, а також інтенсивності виявлення та усунення наявних та потенційних загроз в СЗІ – $\mu_{сзі}$ та ІТС – μ_{imc}. Практика [5] показує, що порушник своїми діями намагається максимізувати ймовірність перебування ІТС під впливом потенційно небезпечної кібератаки, а сторона, що захищається навпаки – мінімізувати ймовірність перебування у такому стані. При чому, згідно до запропонованої однорівневої системи захисту, порушник може досягти своєї мети двома шляхами: через виявлення та реалізації вразливості в СЗІ та в ІТС відповідно (див. рис. 2).

Спираючись на запропоновану однорівневу модель захисту ІТС, а також використовуючи як вихідну відому графову модель процесу кібернетичного нападу на інформацію [15] - [18] розроблюваний узагальнений шаблон потенційно небезпечної КбА можна подати графовою моделлю вигляду, який подано на рис. 3.

ISSN 2663 - 4023

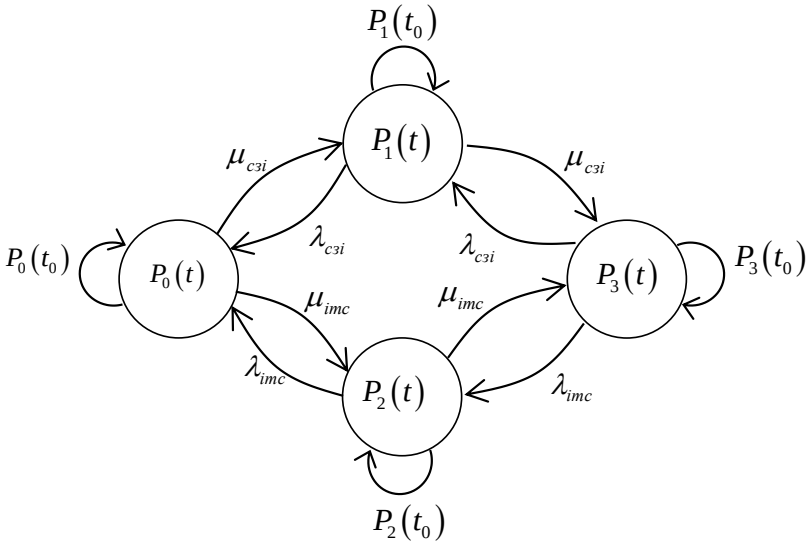

Рис. 3. Узагальнена графова модель шаблону потенційно небезпечної кібератаки

На рис. 3 використовуються такі позначення:

$P_0(t)$ – ймовірність перебування ІТС під впливом потенційно небезпечної КбА (ймовірність перебування системи в незахищеному стані);

$P_3(t)$ – ймовірність перебування ІТС в захищеному стані;

$P_1(t)$ – ймовірність виявлення та реалізації порушником загроз в програмних засобах СЗІ;

$P_2(t)$ – ймовірність виявлення та реалізації порушником загроз в програмних засобах ІТС;

$\lambda_{сзі}, \lambda_{imc}, \mu_{сзі}, \mu_{imc}$ – інтенсивності проведення потенційно небезпечної КбА та захисних дій відповідно.

У будь-який момент часу *t* система може перебувати в одному з зазначених станів. У формалізованому вигляді узагальнена модель шаблону потенційно небезпечної КбА (див. рис. 3) може бути описана системою диференційних рівнянь Колмогорова-Чепмена, яка виходячи з [15], зводиться до:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -(\mu_{сзі} + \mu_{imc})P_0(t) + \lambda_{сзі}P_1(t) + \lambda_{imc}P_2(t); \\ \dfrac{dP_1(t)}{dt} = -(\mu_{сзі} + \lambda_{сзі})P_1(t) + \mu_{сзі}P_0(t) + \lambda_{сзі}P_3(t); \\ \dfrac{dP_2(t)}{dt} = -(\lambda_{imc} + \mu_{imc})P_2(t) + \mu_{imc}P_0(t) + \lambda_{imc}P_3(t); \\ \dfrac{dP_3(t)}{dt} = -(\lambda_{сзі} + \lambda_{imc})P_3(t) + \mu_{сзі}P_1(t) + \mu_{imc}P_2(t). \end{cases} \quad (1)$$

ISSN 2663 - 4023

При цьому умови нормування для (1) будуть мати вигляд $P_0(t)+P_1(t)+P_2(t)+P_3(t)=1$, а початкові умови – $P_0(t)=1, P_1(t)=P_2(t)=P_3(t)=0$.

Отримання узагальненого шаблону потенційно небезпечної КбА $P_0(t)$ за зазначеною системою в аналітичному вигляді є складною математичною процедурою. Крім того існує потреба отримання шаблону реальному (квазіреальному) масштабі часу. Існуючи методи, як показано в [18] не дозволяють вирішити згадане завдання. Тому для забезпечення вимог щодо моделювання в реальному масштабі часу при одночасному збереженні точності вихідної моделі слід застосувати відомий метод диференціально-ігрового моделювання процесів кібернетичного нападу [19] - [21]. Застосувавши згаданий метод, який ґрунтується на диференціальних перетвореннях академіка Національної академії наук України Г. Пухова отримаємо систему спектральних рівнянь вигляду:

$$\begin{cases} P_0(k+1)=\dfrac{T}{k+1}\left(-\left(\mu_{сзі}+\mu_{імс}\right)P_0(k)+\lambda_{сзі}P_1(k)+\lambda_{імс}P_2(k)\right); \\ P_1(k+1)=\dfrac{T}{k+1}\left(-\left(\mu_{сзі}+\lambda_{сзі}\right)P_1(k)+\mu_{сзі}P_0(k)+\lambda_{сзі}P_3(k)\right); \\ P_2(k+1)=\dfrac{T}{k+1}\left(-\left(\lambda_{імс}+\mu_{імс}\right)P_2(k)+\mu_{імс}P_0(k)+\lambda_{імс}P_3(k)\right); \\ P_3(k+1)=\dfrac{T}{k+1}\left(-\left(\lambda_{сзі}+\lambda_{імс}\right)P_3(k)+\mu_{сзі}P_1(k)+\mu_{імс}P_2(k)\right). \end{cases} \quad (2)$$

де T – тривалість потенційно небезпечної КбА, k – номер дискрети, $к$=0,1,2…

Виходячи зі спектральної системи рівнянь визначимо інтенсивності дій порушника $\lambda_{сзі}$, $\lambda_{імс}$ та сторони, що захищається $\mu_{сзі}, \mu_{імс}$ за умови оптимізації деякого критерію – рівня незахищеності ІТС E в стані $P_0(t)$, при чому $E=1-I$, де I – гарантований рівень захищеності ІТС в стані $P_3(t)$, який визначається за виразом [18], [22] (при чому $P_1(t)=P_2(t)=0$):

$$I=\frac{1}{T}\int_0^T P_3(t)\,dt. \quad (3)$$

Фізичний зміст введеного критерію зводиться до опису усередненої ймовірності перебування ІТС в незахищеному стані під час здійснення на неї потенційно небезпечної КбА.

Оскільки моделювання узагальненого шаблону потенційно небезпечної КбА звівся до диференціальної гри то визначенню підлягатимуть: траєкторія гри $P_0(k+1)$, яка є узагальненою диференціально-ігровою моделлю шаблону потенційно небезпечної кібератаки; рівень незахищеності ІТС $E\left(\lambda_{сзі}^{opt}, \lambda_{імс}^{opt}\ \mu_{сзі}^{opt}, \mu_{імс}^{opt}\right)$; оптимальні стратегії гравців нападу $\lambda_{сзі}^{opt}$, $\lambda_{імс}^{opt}$ та захисту $\mu_{сзі}^{opt}$ $\mu_{імс}^{opt}$ відповідно.

Знайдемо в аналітичному вигляді дискрети відповідних диференціальних спектрів (2), присвоюючи послідовно цілочислові значення аргументу k=0, 1, 2 ,3. Виходячи з [19], [23] маємо:

ISSN 2663 - 4023

початкові умови визначають нульову дискрету:

$$P_0(0)=1, P_1(0)=P_2(0)=P_3(0)=0; \tag{4}$$

решта дискрет диференціального спектру для спектральної моделі $P_0(k+1)$:

$$P_0(1)=-T\left(\mu_{сзі}+\mu_{імс}\right), \tag{5}$$

$$P_0(2)=\frac{1}{2}T^2\left(\lambda_{сзі}\mu_{сзі}+\lambda_{імс}\mu_{імс}+\mu_{сзі}^2+2\mu_{сзі}\mu_{імс}+\mu_{імс}^2\right), \tag{6}$$

$$\begin{aligned}P_0(3)=-\frac{1}{6}T^3\left(\lambda_{імс}^2\mu_{імс}+3\lambda_{імс}\mu_{імс}^2+2\lambda_{імс}\mu_{імс}\mu_{сзі}+\lambda_{сзі}^2\mu_{сзі}+2\lambda_{сзі}\mu_{імс}\mu_{сзі}+\right.\\ \left.+3\lambda_{сзі}\mu_{сзі}^2+\mu_{імс}^3+3\mu_{імс}^2\mu_{сзі}+3\mu_{сзі}^2\mu_{імс}+\mu_{сзі}^3\right).\end{aligned} \tag{7}$$

З урахуванням визначених дискрет (4)-(7) рівень незахищеності ІТС (3) матиме вигляд функції чотирьох змінних, тобто:

$$\begin{aligned}E\left(\lambda_{сзі}^{opt},\lambda_{імс}^{opt},\mu_{сзі}^{opt},\mu_{імс}^{opt}\right)=1-\frac{1}{2}T\left(\mu_{сзі}+\mu_{імс}\right)+\\ +\frac{1}{6}T^2\left(\lambda_{сзі}\mu_{сзі}+\lambda_{імс}\mu_{імс}+\mu_{сзі}^2+2\mu_{сзі}\mu_{імс}+\mu_{імс}^2\right)-\\ -\frac{1}{24}T^3\left(\lambda_{імс}^2\mu_{імс}+3\lambda_{імс}\mu_{імс}^2+2\lambda_{імс}\mu_{імс}\mu_{сзі}+\lambda_{сзі}^2\mu_{сзі}+2\lambda_{сзі}\mu_{імс}\mu_{сзі}+\right.\\ \left.+3\lambda_{сзі}\mu_{сзі}^2+\mu_{імс}^3+3\mu_{імс}^2\mu_{сзі}+3\mu_{сзі}^2\mu_{імс}+\mu_{сзі}^3\right).\end{aligned} \tag{8}$$

Для визначення рівня незахищеності ІТС (8) знайдемо оптимальні інтенсивності проведення потенційно небезпечної КбА $\lambda_{сзі}^{opt}, \lambda_{імс}^{opt}$ та оптимальні інтенсивності захисних дій $\mu_{сзі}^{opt}, \mu_{імс}^{opt}$. Для цього розв'яжемо систему лінійних алгебраїчних рівнянь (СЛАР) вигляду:

$$\begin{cases}\dfrac{\partial}{\partial\lambda_{сзі}^{opt}}E=0;\\ \dfrac{\partial}{\partial\lambda_{імс}^{opt}}E=0;\\ \dfrac{\partial}{\partial\mu_{сзі}^{opt}}E=0;\\ \dfrac{\partial}{\partial\mu_{імс}^{opt}}E=0,\end{cases} \tag{9}$$

яка буде визначати необхідні умови.

ISSN 2663 - 4023

Розв'язок СЛАР (9) будь-яким з відомих методів [24] відносно невідомих матиме вигляд

$$\begin{cases} \lambda_{csi}^{opt} = \dfrac{1}{3T}; \\ \lambda_{imc}^{opt} = \dfrac{1}{3T}; \\ \mu_{csi}^{opt} = \dfrac{2}{3T}; \\ \mu_{imc}^{opt} = \dfrac{2}{3T}. \end{cases} \tag{10}$$

Виконання достатніх умов визначеної функції (8) матиме вигляд

$$\begin{cases} \dfrac{\partial^2}{\partial \lambda_{csi}^{opt2}} E < 0; \\ \dfrac{\partial^2}{\partial \lambda_{imc}^{opt2}} E < 0; \\ \dfrac{\partial^2}{\partial \mu_{csi}^{opt2}} E > 0; \\ \dfrac{\partial^2}{\partial \mu_{imc}^{opt2}} E > 0. \end{cases} \Rightarrow \begin{cases} -\dfrac{1}{12} T^3 \mu_{csi} < 0; \\ -\dfrac{1}{12} T^3 \mu_{imc} < 0; \\ \dfrac{1}{3} T^2 > 0; \\ \dfrac{1}{3} T^2 > 0. \end{cases} \tag{11}$$

дозволяє стверджувати, що порушник для досягнення максимального рівня незахищеності ІТС E, реалізуючи потенційно небезпечну КбА, докладає максимальні зусилля $\lambda_{csi\ \max}^{opt}, \lambda_{imc\ \max}^{opt}$. При цьому, сторона, що захищається для забезпечення гарантованого рівня захищеності ІТС I, застосовує мінімально необхідні заходи захисту $\mu_{csi\ \min}^{opt}, \mu_{imc\ \min}^{opt}$.

При виконанні необхідних (9) і достатніх (11) умов після підстановки знайдених відповідних значень інтенсивностей (10) визначимо рівень захищеності ІТС (3) матиме значення:

$$I \approx 0,46, \tag{12}$$

що дає змогу стверджувати, що використанні програмних засобів захисту не достатньо для забезпечення гарантованого рівня захищеності ІТС.

Враховуючи (4)-(7) узагальнена диференціально-ігрова модель шаблону потенційно небезпечної КбА $P_0(t)$ матиме вигляд:

$$P_0(t) = 1 - t(\mu_{сзі} + \mu_{імс}) + \frac{1}{2}t^2\left(\lambda_{сзі}\mu_{сзі} + \lambda_{імс}\mu_{імс} + \mu_{сзі}^2 + 2\mu_{сзі}\mu_{імс} + \mu_{імс}^2\right) -$$
$$-\frac{1}{6}t^3\left(\lambda_{імс}^2\mu_{імс} + 3\lambda_{імс}\mu_{імс}^2 + 2\lambda_{імс}\mu_{імс}\mu_{сзі} + \lambda_{сзі}^2\mu_{сзі} + 2\lambda_{сзі}\mu_{імс}\mu_{сзі} + \right. \quad (13)$$
$$\left. + 3\lambda_{сзі}\mu_{сзі}^2 + \mu_{імс}^3 + 3\mu_{імс}^2\mu_{сзі} + 3\mu_{сзі}^2\mu_{імс} + \mu_{сзі}^3\right),$$

а при підстановці в (13) визначених стратегій порушника та сторони, що захищається (10), узагальнена диференціально-ігрова модель шаблону потенційно небезпечної КбА (13) набуває вигляду:

$$P_0(t) = 1 - \frac{4}{3}\left(\frac{t}{T}\right) + \frac{10}{9}\left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3. \quad (14)$$

Отже, отримана вище в аналітичному вигляді модель (13) є узагальненою диференціально- ігровою моделлю шаблону потенційно небезпечної КбА. Отриманий шаблон, на відміну від відомих, дозволяє оцінювати ефективність проведення потенційно небезпечної КбА, та у разі не забезпечення програмними засобами СЗІ гарантованого рівня захищеності ІТС вжити заходів до його підвищення.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, набула подальшого розвитку розгалужена графова модель процесу нападу на інформацію, що дало змогу вперше розробити узагальнену диференціально-ігрову модель шаблону потенційно небезпечної КбА, який на відміну від існуючих дає змогу оцінювати рівень незахищеності ІТС, враховуючи при цьому інтенсивності дій порушника та сторони, що захищається. Оскільки впливати на інтенсивності дій порушника не можливо, то для зменшення рівня незахищеності ІТС слід відхилитися від визначеного шаблону шляхом корегування інтенсивності дій сторони, що захищається.

Перспективним напрямом подальших досліджень є верифікація розробленої моделі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Грищук, Р., 2011. Атаки на інформацію в інформаційно-комунікаційних системах. *Сучасна спеціальна техніка* , 1 (24), с.61-66. doi: 10.36486/mst2411-3816

[2] Олифер, В. и Олифер, Н., 2015. *Безопасность компьютерных сетей*. М: Горячая линия - Телеком, с.644..

[3] Охрімчук, В. та Завада, А., 2012. Системи виявлення вторгнень: сучасний стан та перспективи розвитку. *Сучасний захист інформації* , 2 (11), с.9-17.

[4] Охрімчук, В., Завада, А. та Самчишин, О. 2012. *Аналіз сучасних систем виявлення і запобігання вторгнень*. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць, (6), Житомир: ЖВІ НАУ, с.97-106.

[5] Грищук, Р. та Даник Ю., 2016. *Основи Кібернетичної Безпеки. Монографія* . Житомир: ЖНАЕУ, с.636.

[6] Ten, C.-W. Manimaran, G., Liu, C.-C. 2010. Cybersecurity for criticalinfrastructures: Attack and defense modeling. *IEEETrans. Syst., Man Cybern* , 40(4) pp.853 -865. doi: 10.1109/TSMCA.2010.2052700

[7] Рубан, І., Мартовицький, В. та Партика, С., 2016. Класифікація методів виявлення аномалій в інформаційних системах. *Системи озброєння і військова техніка*, 3 (47), с.100-105.
[8] Корченко, О., Терейковський, І. та Казмірчук, С., 2014. Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак. *Вісник Інженерної академії України* , (2), с.87-93. - Режим доступу: http://nbuv.gov.ua/UJRN/Viau_2014_2_19.
[9] Ложковский, А., 2010. *Теорія масового обслуговування в телекомунікаціях*. Одеса: ОНАЗ ім. О.С. Попова, с.112.
[10] Гаврилова, Е. 2017. Исследование методов обнаружения сетевых атак. *Научные записки молодых исследователей*, 4, с. 55–58.
[11] Охрімчук, В. та Грищук, Р. 2015. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак. *Безпека інформації,* 21(3), с. 276 – 282. doi: 10.18372/2225-5036.21.9704
[12] Охрімчук, В., Грищук, Р. та Ахтирцева, В. 2016. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак. *Захист інформації*, 1(18), с.21-29. doi: 10.18372/2410-7840.18.10109
[13] Охрімчук, В. 2018. Модель шаблону потенційно небезпечної кібератаки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник*, 1 (35), с.30-39.
[14] Дудикевич, В. та Опірський, І. 2016. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*, № 4 (141), с.86-89.
[15] Щеглов, К. и Щеглов, А. 2015. Интерпретация и моделирование угрозы атаки на информационную систему. Часть 1. Моделирование угрозы уязвимости и интерпретация угрозы атаки. *Информационные технологии*, 21(12) с. 930-940.
[16] Щеглов, К. и Щеглов, А. 2016. Интерпретация и моделирование угрозы атаки на информационную систему. Часть 2. Моделирование угрозы атаки. *Информационные технологии*, 22(1), с. 54-64.
[17] Грищук, Р. 2009. Диференціально-ігрова розгалужена спектральна модель процесу нападу на інформацію. *Вісник Житомирського державного технологічного університету,* 1 (48), с. 152-159. https://doi.org/10.26642/tn-2009-1(48)-152-159
[18] Грищук, Р., 2010. *Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія*. Житомир: Рута, с.280.
[19] Пухов, Г., 1986. *Дифференциальные преобразования и математическое моделирование физических процессов : монография*. К.: Наук. думка, с.160.
[20] Грищук, Р., 2009. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію. *Інформаційна безпека,* 2 (2), с.128–132.
[21] Грищук, Р., 2009. Диференціально-тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу. *Захист інформації*, 1 (42), с.19-27. doi: 10.18372/2410-7840.11.5370
[22] Грищук, Р., 2010. Диференціально-ігрова модель шаблону нормальної поведінки Web-серверу. *Проблеми телекомунікацій*, 2 (2), с. 96-106.
[23] Пухов, Г., 1984. *Дифференциальные преобразования функций и уравнений*. К.: Наук. думка, с.420.
[24] Мартинюк, П. та Гошко, О., 2013. Порівняльний аналіз ефективності застосування чисельних методів розв'язання великих систем лінійних алгебричних рівнянь. *Вісник Національного університету водного господарства та природокористування*, 1(61), с. 289-297.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Volodymyr Okhrimchuk
senior lecturer
Zhytomyr military institute after S. P. Korolyov., Zhytomyr, Ukraine
ORCID: 0000-0001-7518-9993
okhrimchuk84@ukr.net

GENERAL DIFFERENTIAL-GAME MODEL OF POTENTIALLY DANGEROUS PATTERN OF CYBER-ATTACK

Abstract. Today, there is a significant increase in the number of cyber-attacks in the world. At the same time their technological complexity increases proportionally. In the near future, new potentially dangerous cyber-attacks will appear, which in turn may lead to a deterioration of their detection and neutralization and, as a consequence, adversely affect the level of security of information and information and telecommunication systems of critical information infrastructure. Based on the mentioned in the article is solved the urgent task of identifying and neutralizing potentially dangerous cyber-attacks, which boils down to the development of differential-game model of their pattern. The basis of the created pattern of potentially dangerous cyberattacks is proposed to put the Denning`s model of information protection and the method of differential-game simulation of cyber-attack on information processes. The article shows that the pattern of a potentially dangerous cyberattack is modeled under the a priori uncertainty of the input data, since the potential cyberattacks that will take place may be quite diverse. In view of this, it is proposed that the hybrid model be used as a generic template for a potentially dangerous cyberattack due to the inability to make the correct input requirements for the model. This approach provides the evolving model that is being developed, that is, convergence with real physical phenomena and processes in information and information and telecommunication systems. As a result of the application of the differential-game modeling method in analytical form, a generalized differential-game model of a pattern of potentially dangerous cyber-attacks is generalized. Thus, the article further developed a generalized differential-game model of a potentially dangerous cyber-attack pattern, which is based on a Denning's model of information protection and methods of differential-game modeling of the attack on information, which, unlike the existing ones, takes into account the intensity of the offender and the protected party. It allows to estimate the level of insecurity of the information and telecommunication system in the conditions of a priori uncertainty of the input data. The application of the model in practice allows the creation of effective information security systems that will be able to detect potentially dangerous cyber-attacks in the critical infrastructure information and telecommunication system with minimal errors of the first kind.

Keywords: a potentially dangerous cyber-attack; cyber threat; pattern; differential-game model; differential transformations; P-transformation; information and telecommunication system; critical information infrastructure;

REFERENCES

[1] Hryshchuk, R., 2011. Attacks on information in the information and communication systems. *Suchasna Spetsialna Tekhnika*, 1(24), p.61-66. (in Ukrainian) doi: 10.36486/mst2411-3816
[2] Olifer, V. and Olifer, A., 2015. *Computer Network Security* M.: Goryachaya liniya - Telecom, p. 644. (in Russian)
[3] Okhrimchuk, V. and Zavada, A., 2012. Intrusion detection systems: current status and prospects. *Suchasnyi zakhyst informatsii*, 2 (11), p. 9-17. (in Ukrainian)
[4] Okhrimchuk, V., Zavada, A. and Samchyshyn, O., 2012. *Analysis of modern intrusion detection and prevention systems*. Problems of creation, testing, application and operation of complex information systems: collection of scientific works, (6), Zhytomyr: ZVI NAU, p. 97-106. (in Ukrainian)
[5] Hryshchuk, R. and Danik Yu., 2016. *Basics of cybernetic security. Monograph*. Zhytomyr: ZNAEU, p. 636.
[6] Ten, C.-W. Manimaran, G., Liu, C.-C. 2010. Cybersecurity for criticalinfrastructures: Attack and defense modeling. IEEETrans. Syst., Man Cybern , 40(4) pp.853 -865. doi: 10.1109/TSMCA.2010.2052700

[7] Ruban, I., Martovytskyi, V. and Partyka, S., 2016. Classification of methods for detecting anomalies in information systems. *Systemy ozbroiennia i viiskova tekhnika*, 3(47), p 100-105. (in Ukrainian)
[8] Korchenko, O., Tereikovskyi, I. and Kazmirchuk, I., 2014. Neural network assessment method for internet-oriented cyber attacks. *Visnyk inzhenernoi akademii Ukrainy* , 2(87), p 93. (in Ukrainian) Access mode: http://nbuv.gov.ua/UJRN/Viau_2014_2_19.
[9] Lozhkovskyi, A., 2010. *Queuing theory in telecommunications.* Odessa: ONAZ im. O.S. Popova, p 112 (in Ukrainian)
[10] Havrylova, E., 2017. Research on network attack detection methods. *Nauchnye zapysky molodykh yssledovatelei*, 4, p. 55–58. (in Russian)
[11] Okhrimchuk, V. and Hryshchuk, R., 2015. Setting a scientific task to develop templates for potentially dangerous cyber attacks. *Bezpeka informatsii* , 21(3), p 276-282. (in Ukrainian) doi: 10.18372/2225-5036.21.9704
[12] Okhrimchuk, V., Hryshchuk, R. and Akhtyrtseva, V., 2016. The sources of primary data for the development potentially dangerous patterns of cyber-attacks. *Information protection*, 1(18), p. 21-29. (in Ukrainian) doi: 10.18372/2410-7840.18.10109
[13] Okhrimchuk, V., 2018. Model of potentially dangerous pattern of cyber-attack. *Pravove normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. Scientific and Technical Collection*, 1 (35), p. 30-39. (in Ukrainian)
[14] Dudykevych, V. and Opirskyi, I., 2016. Analysis of models of information protection in the state information networks. *Systemy obrobky informatsii*, 4 (141), p 86-89 p. (in Ukrainian)
[15] Shchehlov, K. and Shchehlov, A., 2015. Interpretation and modeling of threats to attacks on the information system. Part 1. Vulnerability threat modeling and attack threat interpretation. *Informaczionny`e tekhnologii*, 21(12) p. 930-940. (in Russian)
[16] Shchehlov, K. and Shchehlov, A., 2015. Interpretation and modeling of threats to attacks on the information system. Part 2. Modeling an attack threat. *Informaczionny`e tekhnologii*. 22(1), p. 54-64. (in Russian)
[17] Hryshchuk, R., 2009. Differential-game branched spectral model of the attack on information process. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu*, 1 (48), p. 152–159. (in Ukrainian) https://doi.org/10.26642/tn-2009-1(48)-152-159
[18] Hryshchuk, R., 2010. *Theoretical foundations of modeling the processes of attack on information by the methods of theories of differential games and differential transformations: monograph*. Zhytomyr: Ruta, p. 280. (in Ukrainian)
[19] Pukhov, H., 1986. *Differential transformations and mathematical modeling of physical processes: monograph*. K. : Nauk. dumka, p. 160. (in Russian)
[20] Hryshchuk, R., 2009. The method of differential-igrovoy P-modeling processes in attacking information. *Informatsiina bezpeka*, 2 (2), p. 128-132. (in Ukrainian)
[21] Hryshchuk, R., 2009. Differential-Taylor model of finding a technical object under the influence of unauthorized access methods. *Zakhyst informatsii*, 1 (42), p. 19-27. (in Ukrainian) doi: 10.18372/2410-7840.11.5370
[22] Hryshchuk, R., 2010. Differential-game model of template of normal behavior of Web-server. *Problemy telekomunikatsii*, 2 (2), p. 96-106. (in Ukrainian)
[23] Pukhov, H., 1984. *Differential transformations of functions and equations*. K.: Nauk. dumka, p. 420. (in Russian)
[24] Martyniuk, P. and Hoshko, O., 2013. Comparative analysis of the efficiency of the application of numerical methods for solving large systems of linear algebraic equations. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia*, 1(61), p. 289-297. (in Ukrainian)