УДК 004.056
DOI: 10.31673/2409-7292.2019.021724

Г.В. Шуклін, А.М. Правдивий, О.Ю. Котомчак

ДИНАМІЧНА МОДЕЛЬ ДІАГНОСТИКИ СТАНІВ КІБЕРЗАХИСТУ СИСТЕМ ІНФОРМАТИЗАЦІЇ З ВИКОРИСТАННЯМ FUZZY-ТЕХНОЛОГІЙ

У роботі запропоновано підхід отримання миттєвого розрахунку ймовірностей негативних наслідків від успішної реалізації кібератак на об'єкти інформаційної діяльності на основі теорії диференціальних рівнянь із запізненням і механізму побудови логічної Fuzzy – функції. Це дає можливість здійснювати діагностику стану захищеності інформаційної системи.

***Ключові слова**:* кіберзахист, fuzzy-функція,інтенсивність кібератак,функція належності, щільність розподілу ймовірності.

Вступ

При побудові архітектури систем кіберзахисту, однією з важливих завдань є створення методики поточної діагностики стану кіберзахисту систем інформатизації та об'єктів інформаційної діяльності. Складність даної процедури полягає в тому, що маючи потужний рівень захищеності об'єкту на програмному рівні, ще не означає, що така потужність є на рівні апартних ресурсів або на криптографічному рівні. В усіх рівнях інформаційної захищеності завжди існують слабкі місця, які злочинці постійно шукають. Тому задача оперативного розрахунку ймовірності можливих негативних наслідків від успішної реалізації кібератак є актуальною задачею сьогодення.

Аналіз останніх публікацій. Існують багато підходів щодо моделювання оцінки захищеності інформаційних систем від кіберзагроз з використанням різних математичних підходів. В роботі [4] оцінка ризику інформаційної безпеки реалізується завдяки апарату нечіткої логіки з введенням лінгвістичних змінних. В роботі [5] це здійснюється завдяки стохастичним різницевим рівнянням для дескриптор них систем, де випадковим впливом виступає білий шум. В роботах [6], [7] оцінка кіберзахисту систем інформатизації здійснюється на основі логічних суджень, які в кінцевому випадку зводяться до побудови функції належності для аналізу лінгвістичних змінних.

Мета роботи. Мета даної роботи полягає в отриманні аналітичних залежностей між інтенсивностями кібератак на об'єкти інформаційної діяльності і ймовірностями негативних наслідків від успішної реалізації останніх для здійснення діагностики рівня захищеності інформаційних систем.

Основна частина

Однією з завдань діагностики стану кіберзахисту систем інформатизації діяльності є оцінка стану системи інформаційного захисту і моніторинг стану кіберзахисту об'єкту. Даний процес діагностики складається з трьох функцій:

1. Оцінка стану кіберзахисту об'єкту;
2. Виявлення уразливості системи кіберзахисту від кібератак і локалізація пошкодження від успішної реалізації кібератаки;
3. Прогнозування уразливостей остаточних ресурсів об'єкту.

Задачу діагностики кіберзахисту можна розглядати як побудову відображення множини параметрів, які визначають стан об'єкту в множину можливих його станів.

Нехай $S = \{s_1, s_2, ..., s_n\}$ - множина інтенсивностей різних видів кібератак, які визначають стан системи кіберзахисту. Такими кібератаками є вірусні програми, Ddos атаки, 17риптог, тощо. Кожній інтенсивності певного виду кібератак поставимо у відповідність свій клас інтенсивностей $s_i = \left\{ s_i^{(\Delta_1(i))}, s_i^{(\Delta_2(i))}, ..., s_i^{(\Delta_{r_i}(i))} \right\}$. Наприклад, якщо s_i - інтенсивність вірусних програм, то $s_i^{(\Delta_1(i))}$ - інтенсивність троянів, $s_i^{(\Delta_2(i))}$ - інтенсивність храпаків, тощо. Множина $L = \{l_1, l_2, l_3\}$ - є множиною можливих станів кіберзахисту об'єкту, елементи якої є лінгвістичні змінні, яким відповідають числові значення, елементи якої належать множині

$\{0;1\}$. Лінгвістична змінна l_1= «система кіберзахисту має високий рівень» і відбиття кібератаки здійснюється на програмному рівні. Змінна l_2= «система кіберзахисту має середній рівень захищеності» і відбиття здійснюється на апаратному рівні. Змінна l_3= «система кіберзахисту має низький рівень кіберзахисту» і відбиття здійснюється на криптографічному рівні. Нехай S_k - поточне значення вектору інтенсивностей кібератак на об'єкт, а L_j - вектор можливих станів.

Інтенсивності кібератак s_i - є неперервними функціями від часу протягом якого здійснюється керування системою кіберзахисту (цикл керування).

Задача оцінки стану кіберзахисту ситеми інформатизації полягає в побудові деякої Fuzzy - логічної функції

$$l_j = f_j(s_1, s_2, ..., s_n),\ j = 1,...,m. \tag{1}$$

Множина S є множиною неперервних функцій від часу, протягом якого здійснюється керування системою кіберзахисту, а L є Fuzzy - множиною, яка задана на універсальній множині відповідних інтервалів значень лінгвістичних змінних l_j, з заданими функціями належності

$$\mu_{s_i}(s_i^{(\Delta_i)}) = \int_{s_i(t-\tau)}^{s_i(t)} \frac{\mu_{s_i}(s_i^{(k)})}{s_i^{(k)}},\ k = 1,...,r_i,\ i = 1,...,n; \tag{2}$$

$$\mu_L(l_j) = \int_{l_j(t-\tau)}^{l_j(t)} \frac{\mu_L(l_j)}{l_j},\ j = 1,...,m. \tag{3}$$

Класифікація станів кіберзахисту на основі нечіткого логічного висновку здійснюється за допомогою бази знань, яка створюється за наступним логічним висновком

$$f_j = \bigcup_{z \in Z_j} \left[\bigcap_{i=1}^{n} \left\{ (s_i \in s_i^{(\Delta_1(i))}) \bigcap (s_i \in s_i^{(\Delta_2(i))}) \bigcap .. \bigcap (s_i \in s_i^{\Delta_{r_i}(i)}) \wedge w_{ij} \geq \varepsilon / z \right\} \right],\ j = 1,...,m. \tag{4}$$

Множина Z_j - є множиною різних логічних правил, які визначають клас можливих станів L_j. Якщо при деякому z - му логічному правилі ($z \in Z_j$) бази знань кожна вхідна змінна s_i належить деякому значенню $s_i^{\Delta_k(i)}$, яке належить класу $\Delta_k(i)$ ($k = 1..r_i$) і вага w_{ij} цього логічного висновку не перевищує деякого граничного значення ε ($w_{ij} \geq \varepsilon$), то значення вихідної змінної належить класу станів L_j.

Для визначення значень функції f_j використовують різні оператори нечіткої логіки, а також норми Fuzzy- логіки.

При діагностиці кіберзахисту об'єктів інформатизації, на практиці зручно визначати функцію (1) наступним чином

$$f_j = \max_{z \in Z_j} \min_{1 \leq i \leq n} \left\lfloor \max_{1 \leq k \leq r_i} \mu_{s_i}(s_i^{(k)}) / z \right\rfloor. \tag{5}$$

При даному підході, кожний рядок матриці бази знань визначає не тільки систему логічних висновків, але і види Fuzzy- логічних операторів, які дають можливість обчислювати реальні значення функції належності до відповідного лінгвістичного терму вихідної змінної.

Грані кібербезпеки об'єктів, які розглядаються в даній роботі, мають три рівні, які представлено в таблиці 1.

Таблиця 1.

Грані кібербезпеки об'єктів інформатизації кредитно-фінансової сфери

Високий рівень	Кіберзахист здійснюється на програмному рівні	Змінна стану l_1 =1, $L=(1,0,0)$
Середній рівень	Кіберзахист здійснюється на апаратному рівні	Змінна стану l_2 =1, $L=(0,1,0)$
Низкий рівень	Кіберзахист здійснюється на 19риптографічному рівні	Змінна стану l_3 =1, $L=(0,0,1)$

Вхідні параметри s_i, які визначають стан системи захисту – інтенсивності кібератак визначаються диференціальними рівняннями із запізненням

$$\frac{ds_i}{dt} = a_i \cdot s_i(t) + b_i \cdot s_i(t-\tau),\ \ s_i(t) \in R^1,\ t>0,\ \ \tau>0,\ \tau = const, \tag{6}$$

з початковими умовами

$$s_i(t) \equiv \omega_i(t), \qquad t_0 - \tau \le t \le t_0 \quad , \tag{7}$$

де $\omega_i(t)$ - деяка частинно – неперервна функція від часу, $b=\frac{a_i}{K}$, a_i - параметр початкової крутизни функції $s_i(t)$, K - кількість об'єктів, на які здійснюється атака.

Розв'язок рівняння (6) з початковими умовами (7) має наступне представлення [1].

$$s_i(t) = \begin{cases} \overline{s_i}\left(1+\left\{e^{a_i t}-1\right\}\left(1+\frac{1}{K}\right)\right), 0 \le t < \tau, \\ \overline{s_i}\left(1+\left\{e^{a_i t}-1\right\}\left(1+\frac{1}{K}\right)+\left\{e^{a_i(t-\tau)}\left[\frac{a_i\cdot(t-\tau)}{1!}-1\right]+1\right\}\frac{1}{K}\left(1+\frac{1}{K}\right)\right), \tau \le t < 2\tau, \\ \overline{s_i}\left(1+\left(e^{a_i t}-1\right)\left(1+\frac{1}{K}\right)+\left(e^{a_i(t-\tau)}\left(a_i(t-\tau)-1\right)+1\right)\frac{1}{K}\left(1+\frac{1}{K}\right)-e^{a_i(t-2\tau)}\left(\left(\frac{a_i(t-2\tau)^2}{2!}+1\right)-1\right)\frac{1}{K^2}\left(1+\frac{1}{K}\right)\right) \\ 2\tau \le t \le 3\tau \end{cases}$$

де $\overline{s_i}$ - середня інтенсивність i-го виду кібератаки за попередній цикл керування системою кіберзахисту.

Умови отримання інформації про рівень захищеності системи. Якщо при спостерігаємому значенні параметра a_i існує такий момент часу $t \in (0;\tau)$, що рівняння

$$\overline{s_i}\left(1+\left(e^{a_i t}-1\right)\left(1+\frac{1}{K}\right)\right)=q_1(2\tau-t)+q_2\left(1-\frac{(t-\tau)^2}{2!}\right), \quad (8)$$

має хоча б один розв'язок, то рівень захищеності системи високий в інтервалі часу $(0;\tau)$. Якщо ця умова не виконується, то якщо існує момент часу $t\in(\tau;2\tau)$ такий, що рівняння

$$\overline{s_i}\left(1+\left(e^{a_i t}-1\right)\left(1+\frac{1}{K}\right)+\left(e^{a_i(t-\tau)}\left(a_i(t-\tau)-1\right)+1\right)\frac{1}{K}\left(1+\frac{1}{K}\right)\right)=q_1(2\tau-t)+q_2, \quad (9)$$

має хоча б один розв'язок, то система має середній рівень захищеності. Аналогічно, якщо умови (8) і (9) не виконуються, то шукається розв'язок рівняння

$$\begin{aligned}&\overline{s_i}\left(1+\left(e^{a_i t}-1\right)\left(1+\frac{1}{K}\right)+\left(e^{a_i(t-\tau)}\left(a_i(t-\tau)-1\right)+1\right)\frac{1}{K}\left(1+\frac{1}{K}\right)\right)+\\&+\overline{s_i}\left(e^{a_i(t-2\tau)}\left(\frac{a_i(t-2\tau)^2}{2!}+1\right)-1\right)\frac{1}{K^2}\left(1+\frac{1}{K}\right)=q_2\end{aligned}. \quad (10)$$

Якщо розв'язок (10) існує, то система має низький рівень захищеності. Якщо хоча б одна з умов (8)-(10) не виконуються, то система не захищена.

Тут

$$q_1=-4\tau^4(2\tau^2-1)-\left(2\tau^2-\frac{5}{24}\tau^4\right)\left(3\tau-\frac{1}{6}\tau^3\right),$$

$$q_2=-\left(2\tau^2-\frac{5}{24}\tau^4\right)(2\tau^2-1)-3\tau+\frac{1}{6}\tau^3.$$

Маючи аналітичні залежності (8), будується функція розподілу ймовірності успішної реалізації кібератаки, яка має наступне представлення

$$F_{s_i}(t)=\frac{\int_{(n-1)\tau}^{t}s_i(\theta)d\theta}{\int_{(n-1)\tau}^{n\tau}s_i(\theta)d\theta},\ (n-1)\tau\le t\le n\tau,\ n=\overline{1,3}.$$

Звідки, щільність розподілу ймовірності успішної реалізації кібератаки має вид

$$\varphi_{s_i}(t)=\frac{dF_{s_i}(t)}{dt},\ (n-1)\tau\le t\le n\tau,\ n=\overline{1,3}.$$

Тоді функція належності (2) при заданому циклі керування $([0,3\tau])$ системою кіберзахисту, можна визначати наступним чином

$$\mu_{s_i}(s_i^{(\Delta_i)}) = \int_{(n-1)\tau}^{t} \varphi_{s_i}(\theta)d\theta, (n-1)\tau \le t \le n\tau,\ n = \overline{1,3}.$$

Функція належності (3) при визначеному циклі керування має вид

$$\mu_L(l_j) = \max\left\{\mu_{s_i}(s_i^{(\Delta_i)})/l_j\right\}$$

Приклад імітаційної моделі. Нехай спостерігались три види кібератак на інформаційну систему банківської установи і результати спостережень представлено в таблиці 2.

Таблиця 2.

Початкові дані для імітаційного моделювання

Вид кібератаки i	Середня інтенсивність за попередній цикл керування кіберзахистом $\overline{s_i}$ (кількість атак за одиницю часу)	Поточний час циклу керування 3τ (в годинах)	Початкова крутизна кібератаки a_i (безрозмірна величина)	Кількість об'єктів K (штук)
Трояни	3	6	2	2
Храпаки	2	6	1	2
DdoS	3200	6	0,5	2

В даному випадку ми маємо два класи вірусних програм, а саме s_1 - інтенсивність вірусних програм, s_2 - інтенсивність DdoS атак. При цьому, $s_1^{(\Delta_1(1))}$ - інтенсивність троянів, $s_1^{(\Delta_2(1))}$ - інтенсивність храпаків, $s_2^{(\Delta_1(2))}$ - інтенсивність DdoS атак.

Час поточного циклу керування дорівнює 6 годин. Тому $\tau = 2$ години. Для кожного виду кібератак записуємо рівняння (8), які представлено в таблиці 3. При цьому $q_1 = -469{,}8$ $q_2 = -37{,}3.$

Таблиця 3.

Дослідження рівняння (8)

Вид кібератаки	Інтервал часу поточного часу керування	Рівняння (8)	Розв'язок рівняння відносно часу t на заданому інтервалі
Трояни	$(0;2)$	$4{,}5e^{2t} = 18{,}65t^2 + 395{,}2t - 1840{,}4$	-
Хропаки	$(0;2)$	$3e^{t} = 18{,}65t^2 + 395{,}2t - 1840{,}9$	-
DdoS	$(0;2)$	$4800e^{0{,}5t} = 18{,}65t^2 + 395{,}2t - 241{,}9$	-

Виходячи з результатів, які представлено в таблиці 3 видно, що відбиття кібератак не було здійснено на програмному рівні. Тобто, рівень захищеності системи не є високий.

При цьому,множина векторів станів $L=\{(0,1,1);(0,1,1);(0,1,1)\}$. Це означає, що протягом двох годин антивірусні програми не змогли відбити троянів і хропаків, а також не було виявлено DdoS атак. При цьому, припускаємо, що система захисту здійснює відбиття на апаратному рівні і на криптографічному рівні.

Функції розподілу і щільності розподілу ймовірності успішної реалізації кібератак на систему інформатизації банку мають наступні види

Трояни: $F_1(t)=\dfrac{\int_0^t(4{,}5e^{2\theta}-1{,}5)d\theta}{\int_0^2(4{,}5e^{2\theta}-1{,}5)d\theta}=0{,}019e^{2t}-0{,}013t-0{,}019$, при $0\le t\le 2$.

$$\varphi_1(t)=0{,}038e^{2t}-0{,}013\text{, при } 0\le t\le 2.$$

Хропаки: $F_2(t)=\dfrac{\int_0^t(3e^{\theta}-1)d\theta}{\int_0^2(3e^{\theta}-1)d\theta}=0{,}18e^{t}-0{,}06t-0{,}18$, при $0\le t\le 2$.

$$\varphi_2(t)=0{,}18e^{t}-0{,}06\text{, при } 0\le t\le 2.$$

DdoS: $F_3(t)=\dfrac{\int_0^t(4800e^{0{,}5\theta}-1600)d\theta}{\int_0^2(4800e^{0{,}5\theta}-1600)d\theta}=2{,}66e^{0{,}5t}-0{,}77t-2{,}66$, при $0\le t\le 2$.

$$\varphi_3(t)=1{,}33e^{0{,}5t}-0{,}77\text{, при } 0\le t\le 2.$$

Тоді, функція належності $\mu_{s_i}(s_i^{(\Delta_i)})$ відбиття i- ї кібератаки буде визначатись наступним чином:

$$\mu_{s_i}(s_i^{(\Delta_i)})=\frac{\varphi_i(t)}{\max\{\varphi_i(t)\}},\ (n-1)\tau\le t\le n\tau. \qquad (11)$$

Графіки функцій належності при визначеному циклі керування ($0\le t\le 6$), відбиття троянів, храпаків та Ddos атак представлено відповідно на рис.1, рис.2, рис.3.

З рисунків видно, що можливість відбиття троянів і храпаків згідно формули (11) було здійснено в кінці другої години часу керування. Це далі підтверджує рівняння (9) (таблиця 4). Однак, можливість відбиття Ddos атак, відбувалось протягом першої години, та в кінці другої. Це свідчить про те, що захист системи від Ddos значно потужніший, ніж від троянів та храпаків.

При цьому,множина векторів станів $L=\{(0,1,0);(0,1,0);(0,1,0)\}$. Це означає, що в кінці другої години антивірусні програми відбили троянів і хропаків, а також було виявлено DdoS атаки, які були відбиті протягом першої години, та при повторній атаці, були відбиті в кінці другої години. Це дає можливість стверджувати, що на апаратному рівні система захищена.

Рис.1. Функція належності відбиття троянів.

Рис.2. Функція належності відбиття хропаків.

Рис.3. Функція належності відбиття Ddos атак.

Таблиця 4.

Дослідження рівняння (9)

Вид кібератаки	Інтервал часу поточного часу керування	Рівняння (9)	Розв'язок рівняння відносно часу t на заданому інтервалі
Трояни	$(2;4)$	$4{,}5e^{2t} + 3e^{2(t-2)}(t-2) = 469.8t - 1916.5$	+
Хропаки	$(2;4)$	$3e^{t} + 3e^{t-2} = 469.8t - 1916.5$	+
DdoS	$(2;4)$	$4800\,e^{0,5t} + 3e^{0.5(t-2)}(t-2) = 469.8t - 1916.5$	+

Висновки

В результаті проведенних досліджень було здійснено моделювання рівня кіберзахисту об'єктів інформаційної діяльності, в якій на відміну від існуючих, було використано одночасно апарат диференціальних рівнянь із запізненням, за допомогою якого здійснюється оперативний розрахунок ймовірності негативних наслідків від успішної реалізації кібератак на інформаційну систему. Це дає можливість будувати функцію належності для аналізу можливих станів бази знань на основі логічних висновків для прийняття рішень при проведенні заходів для підвищення кіберзахисту об'єктів інформаційної діяльності.

Список використаної літератури

1. Зак Ю.А. Принятие решений в условиях нечётких и размытых данных. /Ю.А.Зак. Москва, Книжный дом «Либроком», 2012.
2. Шуклін Г.В. Модель розрахунку інтенсивності кібернетичних атак в системі електронних торгів на фондовому ринку / Г.В. Шуклін, О.В. Барабаш // Сучасні інформаційні системи. – 2018. – Том 2. – №3. – С.111–114.
3. Шуклін Г.В. Метод побудови стабілізаційної функції керування кібербезпекою на основі математичної моделі коливань під дією сил із запізненням / Г.В. Шуклін, О.В. Барабаш // Телекомунікаційні та інформаційні технології. – 2018. – № 2 (59). – С.110–116.
4. Yevseiev S. Algorithm of information security risk assessment based on fuzzy-multiple approach / S. Yevseiev, O. Shmatko, N. Romashchenko // Сучасні інформаційні системи. – 2019. – Том 3. – №2. – С.73–79.
5. Марценюк В. Про модель кібер – фізичної системи з атаками стану та вимірювань на основі стохастичних різницевих рівнянь / В. Марценюк, А. Сверстюк // Захист інформації. – 2019. – Том 21.- № 1, січень-березень. – С.5–12.
6. Самохвалов Ю. Оценка информационной безоавсности организации по критерию уверенности / Ю. Самохвалов, Н. Браиловский // Захист інформації. – 2019. – Том 21.- № 1, січень-березень. – С.13–24.
7. Стремецька М. Оцінка пріоритетів механізмів кіберзахисту національної системи оплати комунальних послуг за допомогою методу аналізу ієрархій / М. Стремецька // Захист інформації. – 2019. – Том 21. – № 2, квітень-червень. – С.5–12.

Надійшла: 20.05.2019 Рецензент: д.т.н., проф. Савченко В.А.