УДК 621.396.933 (043.2)

д.т.н., проф. **Барабаш О.В.** (ДУТ)
Галахов Є.М. (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-06

ДОСЛІДЖЕННЯ ФУНКЦІЇ ІНТЕНСИВНОСТІ КІБЕРАТАК ЗА ДОПОМОГОЮ СТЕПЕНЕВОГО *P*-ПЕРЕТВОРЕННЯ АНАЛІТИЧНОЇ ФУНКЦІЇ

Забезпечення заданого рівня кібербезпеки вимагає визначення суб'єктів загрози, їх мету, наміри нападів на інфраструктуру та слабкі місця інформаційної безпеки підприємства. Для досягнення цих цілей, підприємства потребують нових рішень інформаційної безпеки, які поширюються на області, які захищені традиційною безпекою. Представлено відповідно рівні еволюції та адаптованості вірусів, а також політики захисту кібербезпеки. Показано, що помилки прогнозування функцій інтенсивності кібератак на підприємство частково обумовлені підбором моделі при дослідженні показників кібератак. Представлено відомі методології аналізу інтенсивності кібератак на підприємство. Доведено, що проблематика дослідження інтенсивності кібератак та їх передбачення є мало дослідженою у науковій літературі, що пов'язано із непередбаченістю кібератак та відсутністю у багатьох випадках реальних даних, а також доступних методів їх прогнозування.

Представлено математичне моделювання часових рядів інтенсивності кібератак на підприємство для надання комплексних рішень і прогнозів посилення стійкості підприємства проти поточних цільових кіберзагроз. Розглядається нелінійне диференціальне рівняння першого порядку – рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак. Аналіз функції інтенсивності кібератак проводиться аналітично завдяки степеневого p-перетворення аналітичною функцією. Розглянуто статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал. Представлено види кібератак на ураження мережевої інфраструктури, пропрієтарних додатків, рівня виправлень і конфігурацій сервера, стандартного програмного забезпечення та їх кількість на підприємстві за певні часові періоди. Представлена геометрична візуалізація зміни крутизни логістичної кривої інтенсивності кібератак при різних значеннях параметра з рівномірним кроком за період часу між плановими аудитами при застосуванні p-перетворення.

Ключові слова: кібербезпека, інтенсивність кібератак, рівняння Бернуллі, ураження, логістична крива.

Вступ та постановка завдання. По мірі появи нових IT-технологій зростає інтенсивність нових кібератак на IT-системи підприємства. Традиційні заходи кібербезпеки не справляються запобіганню або стримуванню цих нападів через їх швидкість та частоту. Існує декілька систем таких, як, наприклад система IBM i2 Enterprise Insight Analysis, для контролю кіберзагроз, що можуть допомогти підприємствам слугувати захистом від множини кібератак.

На рис. 1 представлено відповідно рівні еволюції та адаптованості вірусів та політики захисту кібербезпеки [1]. Таким чином, зміцнення кібербезпеки вимагає визначення суб'єктів загрози, їх мету, наміри нападів на інфраструктуру та слабкі місця інформаційної безпеки підприємства. Для досягнення цих цілей, підприємства потребують нових рішень інформаційної безпеки, які поширюються на області, які захищені традиційною безпекою.

Таким чином, захист кіберпростору підприємства у площині його інформаційної безпеки починається з кіберрозвідки у реальному часі. В сучасних умовах постає необхідність у математичному моделюванні часових рядів інтенсивності кібератак на підприємство для надання комплексних рішень і прогнозів посилення стійкості підприємства проти поточних цільових кіберзагроз.

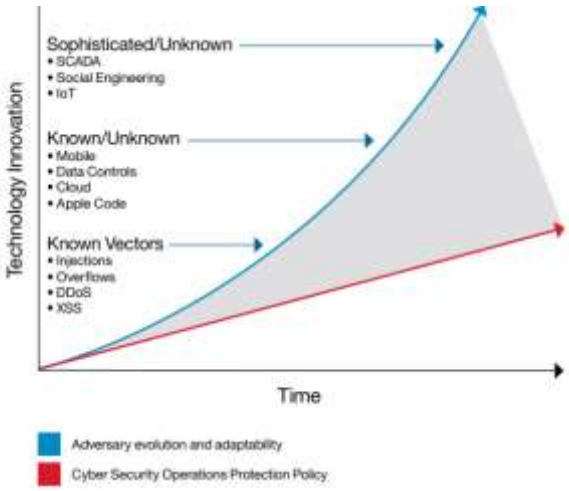


Рисунок 1 – Рівні еволюції та адаптованості вірусів та політики захисту у площині кібербезпеки [4]

Аналіз останніх досліджень і публікацій. Помилки прогнозування функцій інтенсивності кібератак на підприємство частково обумовлені підбором моделі при дослідженні показників кібератак [2]. Дослідження кібератак між плановими аудитами в технічній літературі називають смисловим розривом [3]. Автори у роботі [1] вивчають розрізнення відомих та невідомих атак. Ідентифікації характеристик зміни кібератак протягом певного часу присвячено праці [4-6].

Діаграми часових рядів інтенсивності кібератак на підприємство (кількість атак на годину) представлено на рис. 2 [7]. Горизонтальні лінії – це порогові значення, перевищення яких є небажаними для інформаційної безпеки підприємства.

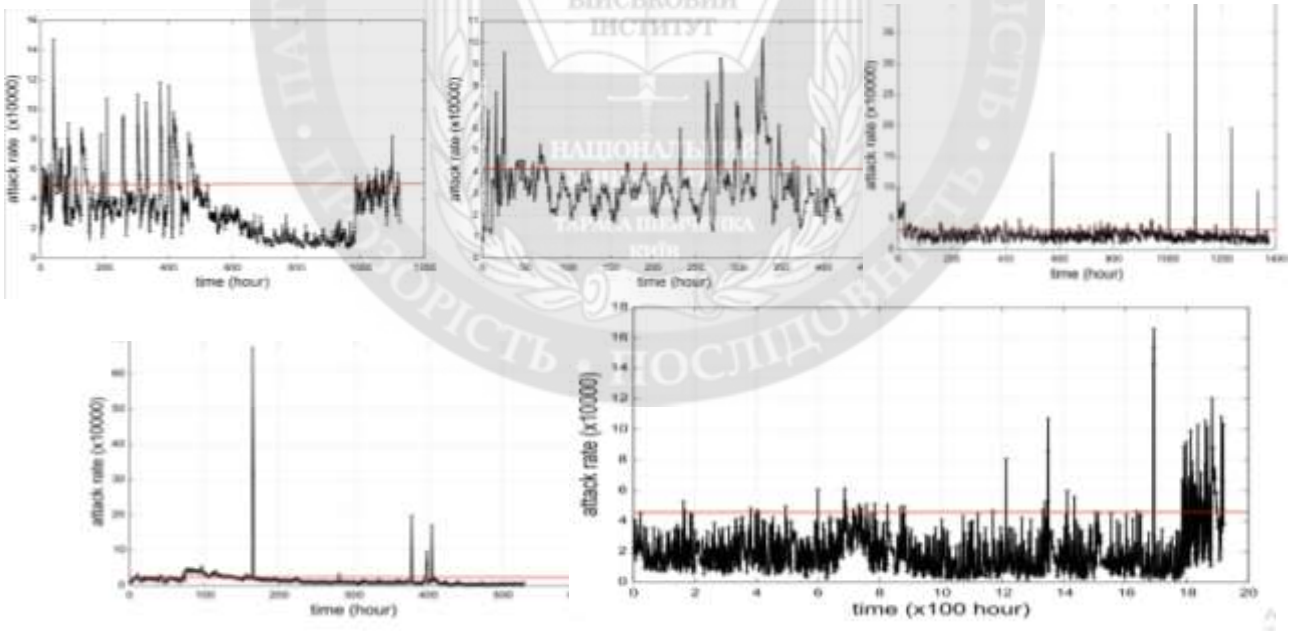


Рисунок 2 – Діаграми часових рядів частоти атак (кількість атак на годину) за 5 часових періодів між плановими аудитами [7]

У науковій праці [7] представлено нову методологію аналізу інтенсивності кібератак на підприємство. Методика аналізу використовує моделі EVT і TST, і має на меті точніше прогнозувати рівень кібератак. Застосування моделі FARIMA + GARCH дозволило прогнозувати швидкість атаки на 1 годину випередження з точністю, що можна вважати практичною. На рис. 3 представлено моделювання функції інтенсивності кібератак на підприємство на основі TST з порівнянням прогнозів на основі FARIMA + GARCH та FARIMA

[7]. Модель на основі TST, де точки чорного кольору представляють спостережувані частоти атак, а червоні крапки – це відповідні прораховані значення із застосуванням моделювання. Автори зазначають, що з рис. 3 видно, що модель FARIMA + GARCH підходить для I-III періодів краще, ніж FARIMA (особливо для екстремальних швидкостей атаки), але не підходить до IV-V періодів (хоча FARIMA + GARCH підходить точніше, ніж FARIMA) [7].

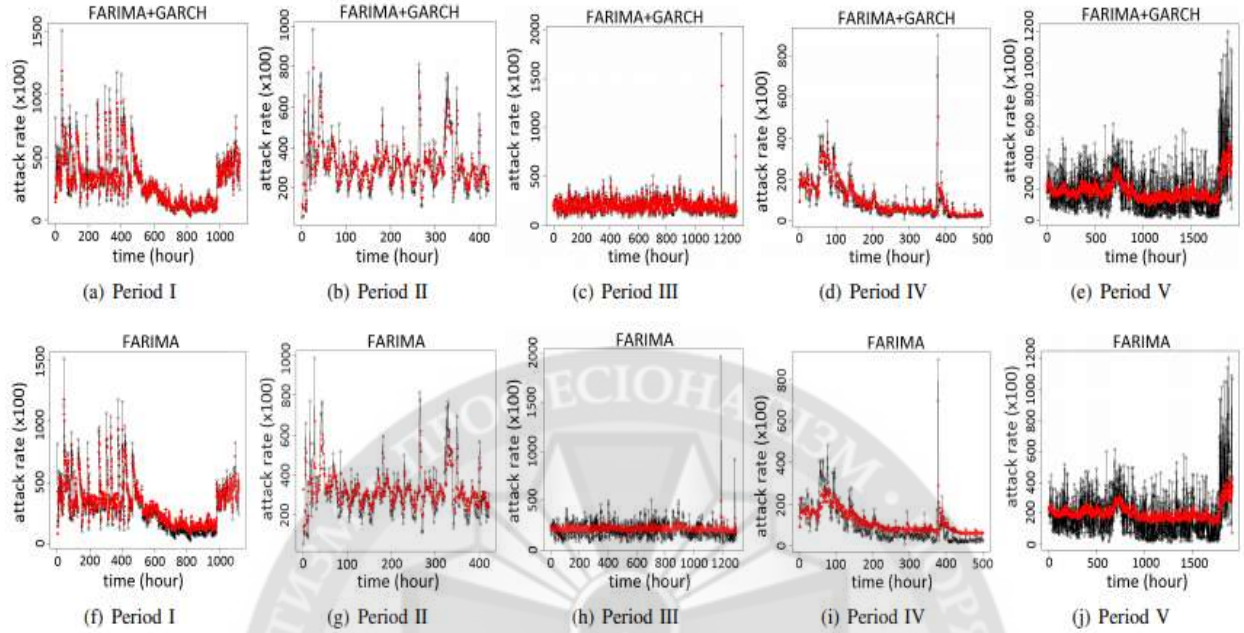


Рисунок 3 – Моделювання функції інтенсивності кібератак на підприємство на основі моделей TST з порівнянням прогнозів на основі FARIMA + GARCH та FARIMA [3]

На рис. 4 представлено порівняння прогнозів рівня віддачі від кібератак на основі EVT (тобто очікуваних величин екстремальної швидкості атаки), спостережуваних частот атаки протягом останніх 120 годин у кожному періоді та прогнозовані темпи атаки на основі TST.

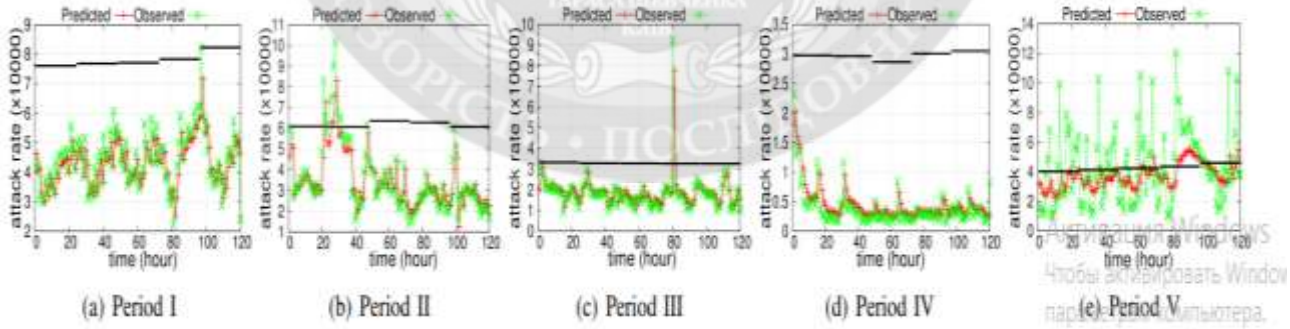


Рисунок 4 – Порівняння прогнозів рівня віддачі кібератак на основі EVT та TST [3]

Прогнози рівня на основі EVT виробляються спеціальним алгоритмом нанесені у вигляді горизонтальних ліній протягом відповідних інтервалів з 24 годин. Прогнози на основі TST виробляються алгоритмом 3. Для періодів I-III, побудовані прогнози повернення на основі EVT та TST, а також максимальні показники атак є точними. Для періоду IV, прогнози на основі EBT екстремальних частот нападу приблизно на порядок вище спостережуваних частот нападу, але прогнози на основі TST максимальних показників атаки є точними. Для періоду V ні EVT, ні TST не можуть дати точні прогнозі інтенсивності кібератак (рис. 3) [7].

У науковій літературі досліджуються кібератаки з відмовою в обслуговуванні (DoS) [8], вивчення хробаків та діяльності ботнетів [9], аналіз даних кількості кібератак, зібраних в чорному отворі [10] та в однобічному русі [11]. Дослідження [2, 12] присвячені класифікації дані на класи (сканування, однорангове сканування, програми, недоступні послуги, неправильні конфігурації, черв'яки тощо). У роботі [13] характеризується позиція кібербезпеки підприємства на основі даних зібраних в чорних дірах.

Таким чином, на сьогодні проблематика дослідження інтенсивності кібератак та їх передбачення є мало дослідженою у науковій літературі, що пов'язано із непередбаченістю кібератак та відсутністю у багатьох випадках реальних даних, а також доступних методів їх прогнозування.

Виклад основного матеріалу. Позначимо інтенсивність кібератак $I_K(t)$. Рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак має вигляд

$$dI_K(t)/dt - \zeta \cdot I_K(t) = -\zeta \frac{1}{I_K(t)_{Max}} \cdot {I_K}^2(t), \qquad I_K(0) = I_{K_0}, \tag{1}$$

де $I_K(t)_{Max}$ – максимально можливий рівень функції інтенсивності кібератак;

$I_K(0) = I_{K_0}$ – початковий рівень функції інтенсивності кібератак після проведення планового аудиту;

ζ – рівень корегування загроз кібератак завдяки звичайного аудиту;

Застосуємо до функції інтенсивності кібератак p-перетворення наступного вигляду:

$$I_K(t) \to i_K(t)^{p-1}, \quad . \quad p \in (0,1) \cup (1,\infty). \tag{2}$$

З урахування p-перетворення рівняння (1) перетворюється таким чином:

$$(p-1) \cdot i_K(t)^{p-2} - \zeta \cdot i_K(t)^{p-1} = -\zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}} \cdot i_K(t)^{2p-2},$$

або

$$(p-1) \cdot i_K(t)^{-p} - \zeta \cdot i_K(t)^{1-p} = -\zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}. \tag{3}$$

Домножимо ліву і праву частину на (–1). Тоді маємо:

$$-(p-1) \cdot i_K(t)^{-p} + \zeta \cdot i_K(t)^{1-p} = \zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}.$$

Зробимо заміну:

$$i_K(t)^{1-p} = \Psi,$$
$$(1-p) \cdot i_K(t)^{-p} \cdot di_K(t)/dt = d\Psi/dt,$$

або

$$-(p-1) \cdot i_K(t)^{-p} \cdot di_K(t)/dt = d\Psi/dt.$$

Тепер рівняння (3) зводиться до лінійного диференціального рівняння 1-го порядку:

$$d\Psi/dt + \zeta \cdot \Psi = \zeta \cdot \frac{1}{{i_K(t)^{p-1}}_{Max}}. \tag{4}$$

Загальний розв'язок цього рівняння має вигляд:

$$\Psi = \frac{1}{{i_K(t)^{p-1}}_{Max}} + ce^{-\zeta t}. \tag{5}$$

Враховуючи p-перетворення, початкові умови набувають вигляду:

$$\Psi(0) = i_K^{1-p}(0). \tag{6}$$

Тепер одержимо розв'язок диференціального рівняння (4) у вигляді:

$$i_K(t) = \frac{i_K(t)_{Max}}{\left(1 + \frac{i_K(t)^{p-1}_{Max} - i_K{}^{p-1}(0)}{i_K{}^{p-1}(0)} \cdot e^{-\zeta t}\right)^{\frac{1}{p-1}}}. \tag{7}$$

Функція (7) у безрозмірному вигляді:

$$\frac{i_K(t)}{i_K(t)_{Max}} = \frac{1}{\left(1 + \frac{1 - \frac{i_K{}^{p-1}(0)}{i_K(t)^{p-1}_{Max}}}{\frac{i_K{}^{p-1}(0)}{i_K(t)^{p-1}_{Max}}} \cdot e^{-\zeta \frac{t}{T}}\right)^{\frac{1}{p-1}}}, \tag{8}$$

Введемо позначення безрозмірних змінних:

$$i_K{}^*(t) = \frac{i_K(t)}{i_K(t)_{Max}}, \qquad t^* = \frac{t}{T}. \tag{9}$$

де T – період між плановими аудитами.

Остаточно отримаємо функцію інтенсивності кібератак із урахуванням степеневого p-перетворення у вигляді:

$$i_K{}^*(t) = \frac{1}{\left(1 + \frac{1 - i_K{}^*(0)}{i_K{}^*(0)} \cdot e^{-\zeta t^*}\right)^{\frac{1}{p-1}}}. \tag{10}$$

Знайшовши першу та другу похідні функції (8), знаходимо координати точки перегину:

$$\left(t^*, i_K{}^*(t)\right) = \left(\frac{1}{\zeta} \ln\left(\frac{1}{(p-1)} \cdot \frac{i_K{}^{p-1}(t)_{Max} - i_K{}^{p-1}(0)}{i_K{}^{p-1}(0)}\right);\ i_K(t)_{Max} \cdot p^{-\frac{1}{p-1}}\right). \tag{11}$$

Розглянемо статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал.

На рис. 5 представлено розподіл кількості кібератак за три часових періоди 2019 року за основними моделями кібератак.

Стосовно ураження мережевої інфраструктури (див. рис. 5), то відмітимо, що зловмисні користувачі використовують програми HackTool під час налаштування атак на локальні або віддалені комп'ютери, що актуально при залученні фріланс-ресурсу. Програми цього класу можуть активувати незареєстровані програмні продукти Microsoft. Такі програми можна використовувати разом із шкідливим чи небажаним програмним забезпеченням. Програми HackTool використовуються для створення нових користувачів зі списку дозволених відвідувачів системи та видалення інформації із системних журналів, щоб приховати присутність зловмисного користувача в системі. Ці програми також використовуються для аналізу та збору мережевих пакетів для здійснення конкретних шкідливих дій.

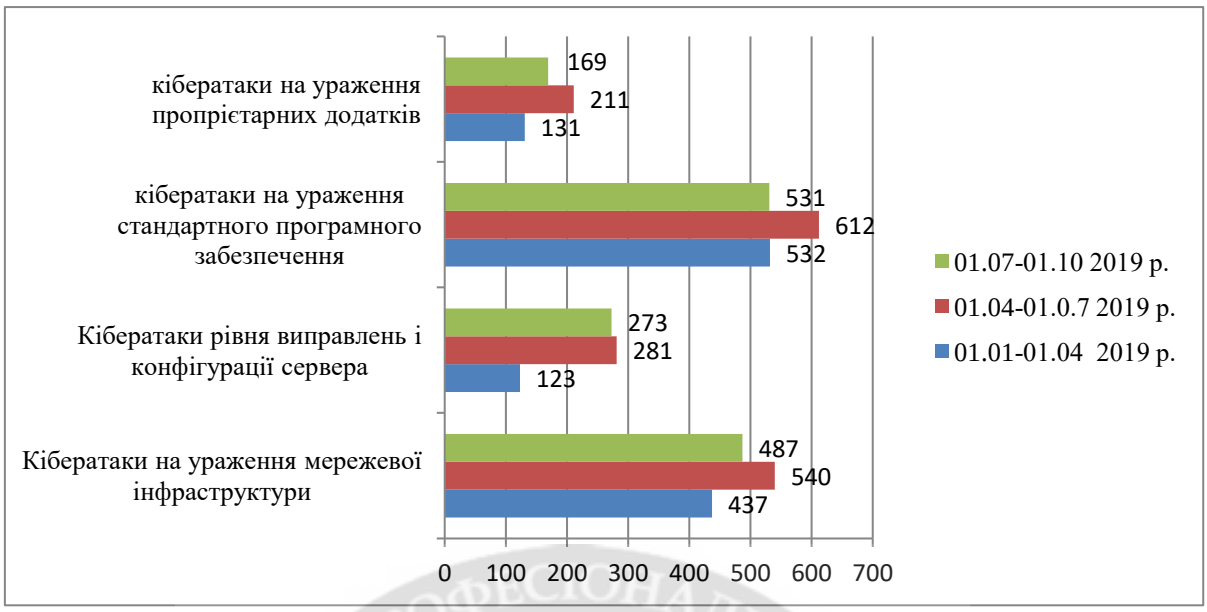


Рисунок 5 – Діаграма кількості кібератак за три часових періоди за основними моделями кібератак

Джерело: складено автором на основі даних підприємства

У табл. 1 представлено види кібератак на ураження мережевої інфраструктури та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 1

Види кібератак на ураження мережевої інфраструктури та їх кількість на підприємстві за період 2017 – 2019 рр.

Джерело: складено на основі даних підприємств

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
U1	HackTool.Win32.KMSAuto.c	19	36	58	35	66	78	33	46	70	43	57	75
U2	HackTool.Win32.KMSAuto.ew	21	35	56	34	63	75	32	45	69	42	54	72
U3	DangerousObject.Multi.Generic	23	33	53	31	59	70	26	36	55	40	50	67
U4	Trojan.Script.Generic	19	31	50	26	49	58	24	33	51	38	40	55
U5	HackTool.MSIL.KMSAuto.by	18	28	46	25	47	56	21	28	44	35	38	53
U6	HackTool.Win64.KMSAuto.b	16	27	43	20	39	46	20	28	43	34	30	43
U7	HackTool.MSIL.KMSAuto.bx	15	27	42	18	34	42	20	27	42	34	25	39
U8	HackTool.Win32.KMSAuto.bu	15	24	40	18	31	40	18	26	40	31	22	37
U1	HackTool.MSIL.KMSAuto.dc	10	18	28	17	32	38	17	25	38	25	23	35
U10	HackTool.MSIL.KMSAuto.a	8	13	21	15	29	37	15	23	35	20	20	34

У табл. 2 представлено види кібератак на ураження рівня виправлень і конфігурації сервера та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 2

Види кібератак (рівня виправлень і конфігурації сервера) та їх кількість на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємств

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
N1	Intrusion.Win.MS17-010.o	18	19	21	35	41	47	30	33	35	32	38	42
N2	Bruteforce.Generic.Rdp.d	11	12	14	34	39	39	28	30	33	30	36	40
N3	Intrusion.Win.MS17-010.p	9	13	13	31	32	36	26	29	31	28	29	38
N4	Bruteforce.Generic.Rdp.a	10	10	13	24	31	35	24	26	29	26	28	36
N5	Bruteforce.Generic.Rdp.c	9	10	12	25	24	31	24	27	29	26	21	36
N6	Intrusion.Win.NETAPI.buffer-overflow.exploit	7	11	12	20	23	27	23	25	28	25	20	35
N7	Intrusion.Win.CVE-2017-0147.d.leak	8	9	11	19	22	27	21	23	26	23	19	33
N8	Intrusion.Generic.CVE-2018-1273.exploit	7	7	11	18	11	15	20	20	25	22	8	32
N1	Intrusion.Win.CVE-2019-0708.b.exploit	5	5	9	17	10	13	14	16	19	16	7	26
N10	Intrusion.Win.EternalRomance.s	8	5	7	13	7	11	13	11	18	15	4	25

У табл. 3 представлено види кібератак на ураження стандартного програмного забезпечення та їх кількість підприємстві по кварталам за період 2017 – 2019 рр.

Таблиця 3

Види кібератак та їх кількість (стандартне програмне забезпечення) на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємства

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
H1	Trojan.Multi.BroSubsc.gen	45	55	68	53	67	84	27	51	61	25	29	65
H2	HackTool.MSIL.KMSAuto.a	42	52	65	52	66	83	28	52	62	26	30	62
H3	HackTool.MSIL.KMSAuto.cz	39	49	62	45	65	77	22	44	62	20	24	59
H4	Trojan.Script.Generic	35	45	58	44	51	75	24	44	51	22	26	55
H5	DangerousObject.Multi.Generic	31	41	56	33	47	64	22	37	50	20	24	53
H6	Trojan.Multi.Agent.gen	30	40	53	19	33	50	23	19	50	21	25	50
H7	Trojan.Multi.GenBadur.gen	29	39	52	16	31	48	21	11	50	19	23	49
H8	HackTool.Win32.KMSAuto.er	26	37	50	15	29	46	18	15	50	16	20	47
H9	HackTool.MSIL.KMSAuto.dc	15	22	38	13	19	44	14	10	49	12	16	35
H10	HackTool.Win32.KMSAuto.bu	7	9	30	3	7	41	14	4	46	12	16	27

У табл. 4 представлено кібератаки на ураження пропрієтарних додатків та їх кількість на підприємстві по кварталам за період 2017 – 2019 рр.

На рис. 6 представлено часові ряди кількості кібератак на систему підприємства за однакові часові періоди 2017 – 2019 років, що попадають у часовий проміжок від кінця аудиту до початку наступного.

Таблиця 4

Види кібератак (пропрієтарні додатки) та їх кількість
на підприємстві за період 2017 – 2019 рр.

Джерело: складено автором на основі даних підприємства

Позначення	*Ураження*	*Кількість кібератак за часовий період*											
		01.01-01.04			*01.04-01.0.7*			*01.07-01.10*			*01.10-31.12*		
		2017	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*	*2017*	*2018*	*2019*
E1	Exploit.VBS.Agent.ad	27	51	29	30	24	33	27	26	25	22	20	26
E2	Exploit.Win32.Agent.gen	12	52	14	31	25	31	28	27	23	7	21	11
E3	Exploit.MSOffice.CVE-2017-11882.gen	11	49	13	28	22	29	22	24	21	3	15	10
E4	Exploit.AndroidOS.Lotoor.be	11	45	13	24	18	27	24	20	19	6	13	10
E5	Exploit.AndroidOS.Lotoor.bg	10	41	12	20	14	25	22	16	18	9	15	9
E6	Exploit.WinLNK.CVE-2017-8464.ecr	10	40	12	19	13	21	23	15	16	5	16	9
E7	Exploit.Win32.ShellCode.jhs	9	39	11	18	12	19	21	14	16	4	9	8
E8	Exploit.AndroidOS.Lotoor.bm	9	37	11	16	10	11	18	12	15	7	11	8
E1	Exploit.AndroidOS.Lotoor.cd	7	22	9	3	3	9	14	5	11	2	7	6
E10	Exploit.Win32.ShadowBrokers.ae	5	9	7	5	2	6	14	4	5	5	7	4

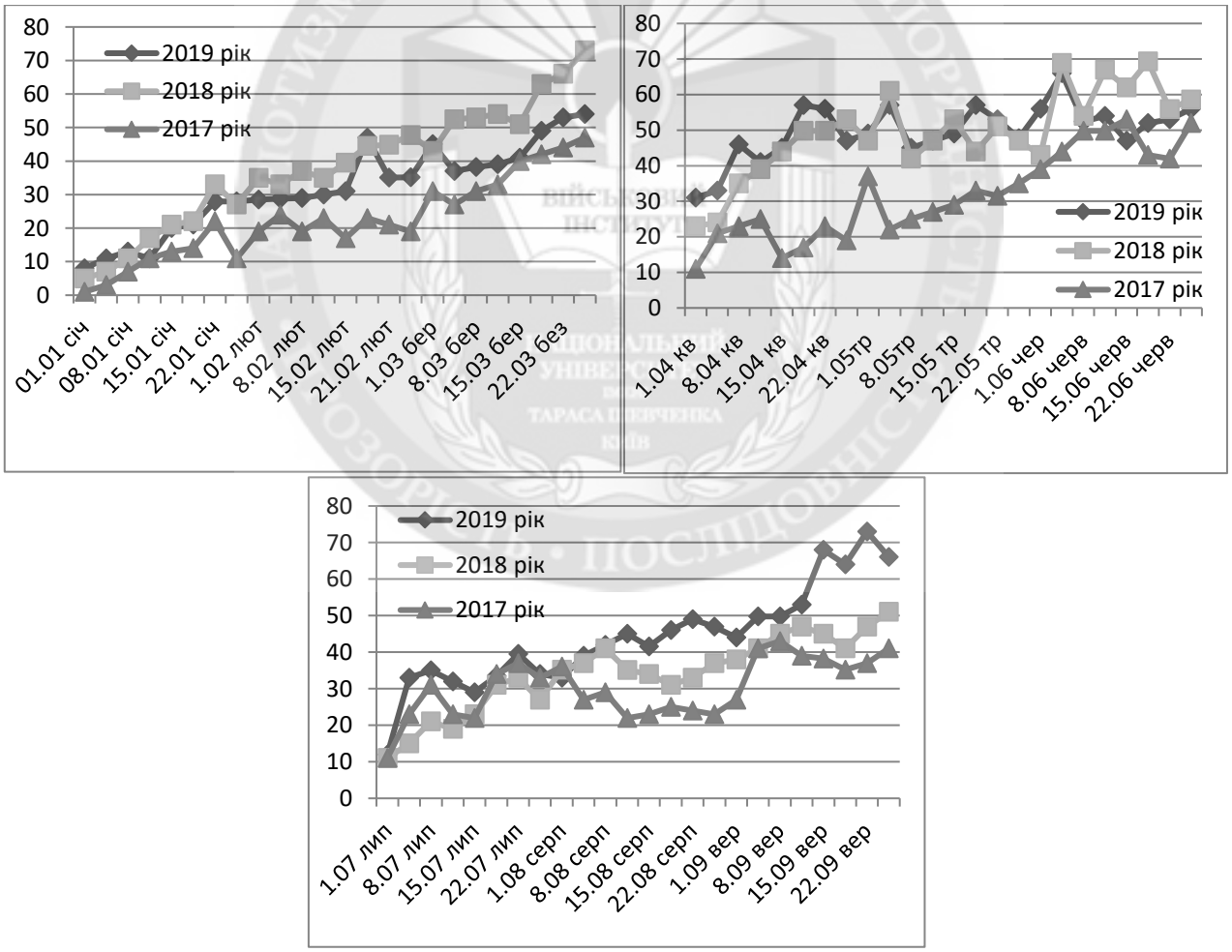
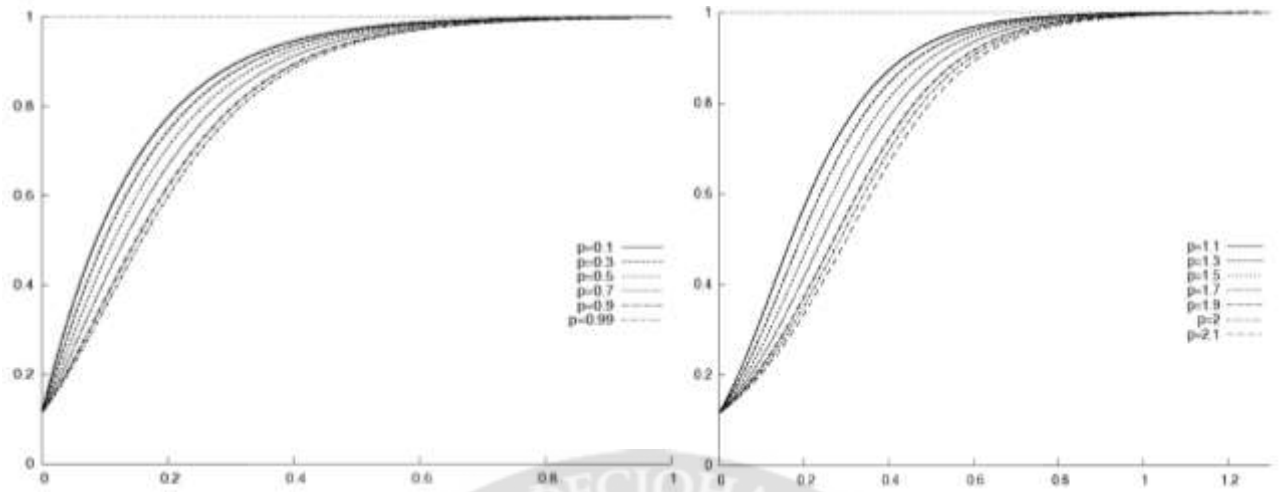


Рисунок 6 – Часові ряди кібератак на систему підприємства за часові періоди:
(1.01-31.03); (1.04-31.06); (1.04-31.06); (1.07-30.09) 2017 – 2019 років,
що починаються після проведення планових аудитів

Джерело: авторські розрахунки

На рис. 7 представлена геометрична візуалізація зміни крутизни логістичної кривої інтенсивності кібератак при параметрі $p \in (0,1)$ та $p \in (1,\ 2.1)$ з кроком 0,2 за період часу T.



а) б)

Рисунок 7 – Зміна крутизни логістичної кривої інтенсивності кібератак з кроком 0,2 за період часу T при параметрі: а) $p \in (0,1)$; б) $p \in (1,\ 2.1)$

Джерело: авторські розрахунки

Отже, необхідно апроксимувати загальну кількість статистичних даних за 4 періодами за 2017 – 2019 років з підбором відповідних параметрів *p* з *p*-перетворення і знайти прогнозний довірчий інтервал функції інтенсивності кібератак, що дасть можливість застосувати теорію еластичності функції інтенсивності кібератак, що, в свою чергу, приведе до визначення часового інтервалу, в якому ефективно проводити спеціальний аудит на підприємстві.

Висновки. Математичне моделювання часових рядів інтенсивності кібератак на підприємство розглядається з точки зору аналітичної інтерпретації за допомогою нелінійного диференціального рівняння 1-го порядку рівняння Бернуллі, що описує процес часового ряду інтенсивності кібератак. Для проведення аналізу функції інтенсивності кібератак було застосовано степеневе *p*-перетворення аналітичною функцією. Це дало можливаість введення малого параметра у функцію інтенсивності кібератак, що виражає чутливість логістичної кривої до зміни статистики і аналітично характеризує зміну крутизни логістичної кривої інтенсивності кібератак. Розглянуто статистичні дані кількості кібератак на підприємстві за умови того, що плановий аудит проводиться раз в квартал. Представлено види кібератак на ураження мережевої інфраструктури, пропрієтарних додатків, рівня виправлень і конфігурацій сервера, стандартного програмного забезпечення та їх кількість на підприємстві за певні часові періоди з їх геометричною візуалізацією. Дослідження є підгрунтям застосування теорії еластичності функції інтенсивності кібератак, що приведе до визначення часового інтервалу, на якому ефективно проводити спеціальний аудит на підприємстві.

ЛІТЕРАТУРА:

1. IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. ZZS03196-USEN-06. URL: https://www.ibm.com/downloads/cas/WZKLWGPB

2. Шуклін Г.В., Барабаш О.В. Метод побудови стабілізаційної функції керування кібербезпекою на основі математичної моделі коливань під дією сил із запізненням. *Телекомунікаційні та інформаційні технології*. Київ. 2018. № 2 (59). С. 110–116.

3. Xu, Tingyang, Jiangwen Sun and Jinbo Bi (2015) ”Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction”. ACM, KDD 2015.

4. A. Joulin, E. Grave, P. Bojanowski and T. Mikolov (2017) “Bag of tricks for efficient text classification”. In Proceedings of the 15th Conference of the European Chapter of the Association for

Computational Linguistics: Volume 2, Short Papers. Association for Computational Linguistics, April 2017, pp. 427–431.

5. R. A. Bridges, C. L. Jones, M. D. Iannacone, K. M. Testa and J. R. Goodall (2014) "Automatic labeling for entity extraction in cyber security". In ASE Third International Conference on Cyber Security, Academy of Science and Engineering (ASE), 2014.

6. S. K. Lim, A. O. Muis, W. Lu and C. H. Ong (2017) "Malwaretextdb: A database for annotated malware articles". Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Vancouver, Canada: Association for Computational Linguistics, July 2017, pp. 1557–1567. [Online]. Available: http://aclweb.org/anthology/P17-1143.

7. Zhenxin Zhan, Maochao Xu and Shouhuai Xu. (2016) "Predicting Cyber Attack Rates with Extreme Values". arXiv:1603.07432v1 [cs.CR] 24 Mar 2016.

8. B. J. Dorr, M. Petrovic, J. F. Allen, C. M. Teng and A. Dalton (2014) "Discovering and characterizing emerging events in big data". AAAI Fall Symposium Series, 2014.

9. Sauerwein, C. Sillaber, M. M. Huber, A. Mussmann and R. Breu (2018) "The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter". IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2018, pp. 201–215.

10. Babko-Malaya O., Cathey R., Hinton S., Maimon D. and Gladkova T. (2017) "Detection of hacking behaviors and communication patterns on social media". In: Proceedings of the 2017 IEEE International Conference on Big Data, pp. 4636 – 4641.

11. Accenture Security (2017). Cost of cyber crime study. https://www.accenture. com/us-en/insight-cost-of-cybercrime-2017. Accessed 5 Jan 2018.

12. Bilge L., Han Y. and Dell'Amico M (2017). "Riskteller: Predicting the risk of cyber incidents". In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, New York. pp 1299 – 1311. https://doi.org/10.1145/3133956.3134022.

13. Okutan A., Yang S.J. and McConky K. (2018). "Forecasting cyber attacks with imbalanced data sets and different time granularities". CoRR abs/1803.09560. http://arxiv.org/abs/1803.09560. 1803.09560.

REFERENCES:

1. IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. ZZS03196-USEN-06. URL: https://www.ibm.com/downloads/cas/WZKLWGPB

2. Shuklin, H.V. and Barabash, O.V. (2018) "Metod pobudovy stabilizatsiinoi funktsii keruvannia kiberbezpekoiu na osnovi matematychnoi modeli kolyvan pid diieiu syl iz zapiznenniam" [A method of constructing a stabilization function for cybersecurity management based on a mathematical model of oscillations under the influence of delayed forces], Telecommunication and information technologies, Kyiv, No. 2 (59), pp. 110–116.

3. Xu, Tingyang, Jiangwen Sun and Jinbo Bi (2015) "Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction". ACM, KDD 2015.

4. A. Joulin, E. Grave, P. Bojanowski and T. Mikolov (2017) "Bag of tricks for efficient text classification". In Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers. Association for Computational Linguistics, April 2017, pp. 427–431.

5. R. A. Bridges, C. L. Jones, M. D. Iannacone, K. M. Testa and J. R. Goodall (2014) "Automatic labeling for entity extraction in cyber security". In ASE Third International Conference on Cyber Security, Academy of Science and Engineering (ASE), 2014.

6. S. K. Lim, A. O. Muis, W. Lu and C. H. Ong (2017) "Malwaretextdb: A database for annotated malware articles". Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Vancouver, Canada: Association for Computational Linguistics, July 2017, pp. 1557–1567. [Online]. Available: http://aclweb.org/anthology/P17-1143.

7. Zhenxin Zhan, Maochao Xu and Shouhuai Xu. (2016) "Predicting Cyber Attack Rates with Extreme Values". arXiv:1603.07432v1 [cs.CR] 24 Mar 2016.

8. B. J. Dorr, M. Petrovic, J. F. Allen, C. M. Teng and A. Dalton (2014) "Discovering and characterizing emerging events in big data". AAAI Fall Symposium Series, 2014.

9. Sauerwein, C. Sillaber, M. M. Huber, A. Mussmann and R. Breu (2018) "The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter". IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2018, pp. 201–215.

10. Babko-Malaya O., Cathey R., Hinton S., Maimon D. and Gladkova T. (2017) “Detection of hacking behaviors and communication patterns on social media”. In: Proceedings of the 2017 IEEE International Conference on Big Data, pp. 4636 – 4641.

11. Accenture Security (2017). Cost of cyber crime study. https://www.accenture. com/us-en/insight-cost-of-cybercrime-2017. Accessed 5 Jan 2018.

12. Bilge L., Han Y. and Dell’Amico M (2017). “Riskteller: Predicting the risk of cyber incidents”. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, New York. pp 1299 – 1311. https://doi.org/10.1145/3133956.3134022.

13. Okutan A., Yang S.J. and McConky K. (2018). “Forecasting cyber attacks with imbalanced data sets and different time granularities”. CoRR abs/1803.09560. http://arxiv.org/abs/1803.09560. 1803.09560.

д.т.н., проф. Барабаш О.В., Галахов Е.М.

ИССЛЕДОВАНИЕ ФУНКЦИИ ИНТЕНСИВНОСТИ КИБЕРАТАК ПРИ ПОМОЩИ СТЕПЕННОГО *P*-ПРЕОБРАЗОВАНИЯ АНАЛИТИЧЕСКОЙ ФУНКЦИИ

Обеспечение заданного уровня кибербезопасности требует определения субъектов угрозы, их целей, намерения нападений на инфраструктуру и слабые места информационной безопасности предприятия. Для достижения этих целей, на предприятиях нужно разрабатывать новые решения информационной безопасности, распространяющиеся на области, которые защищены традиционной безопасностью. Представлены соответственно уровни эволюции и адаптированности вирусов, а также политики защиты кибербезопасности. Показано, что ошибки прогнозирования функций интенсивности кибератак на предприятие частично обусловлены подбором модели при исследовании показателей кибератак. Представлены известные методологии анализа интенсивности кибератак на предприятие. Доказано, что проблематика исследования интенсивности кибератак и их предсказания мало исследованы в научной литературе, что связано с непредсказуемостью кибератак и отсутствием во многих случаях реальных данных, а также доступных методов их прогнозирования.

Представлены математическое моделирование временных рядов интенсивности кибератак на предприятие для предоставления комплексных решений и прогнозов усиления устойчивости предприятия против текущих целевых киберугроз. Рассматривается нелинейное дифференциальное уравнение первого порядка – уравнение Бернулли, которое описывает процесс временного ряда интенсивности кибератак. Анализ функции интенсивности кибератак проводится аналитически благодаря степенному p-преобразованию аналитической функцией. Рассмотрены статистические данные количества кибератак на предприятии при условии того, что плановый аудит проводится раз в квартал. Представлены виды кибератак на поражение сетевой инфраструктуры, проприетарных приложений, уровня исправлений и конфигураций сервера, стандартного программного обеспечения и их количество на предприятии за определенные временные периоды. Представлена геометрическая визуализация изменения крутизны логистической кривой интенсивности кибератак при различных значениях параметра с равномерным шагом за период между плановыми аудитами при применении p-преобразования.

Ключевые слова: кибербезопасность, интенсивность кибератак, уравнение Бернулли, поражения, логистическая кривая.

Prof. Barabash O.V., Halakhov Y.

RESEARCH OF THE FUNCTION OF INTENSITY OF CYBER ATTACKS USING THE DEGREE OF P-TRANSFORMATION OF ANALYTICAL FUNCTION

Strengthening cybersecurity requires identifying the subjects of the threat, their goals, intentions of attacks on the infrastructure and weaknesses of the information security of the enterprise. To achieve these goals, enterprises need new information security solutions that extend to areas that are protected by traditional security. The levels of evolution and adaptability of viruses, as well as cybersecurity protection policies, respectively, are presented. It is shown that errors in predicting the functions of the intensity of cyberattacks at an enterprise are partially due to the selection of a model in the study of indicators of cyberattacks. Known methodologies for analyzing the intensity of cyberattacks at an enterprise are presented. It is proved that the problems of studying the intensity of cyberattacks and their predictions have

been little studied in the scientific literature, which is associated with the unpredictability of cyberattacks and the absence in many cases of real data, as well as available methods for predicting them.

Mathematical modeling of time series of the intensity of cyberattacks per enterprise is presented to provide comprehensive solutions and predictions of strengthening the enterprise's resistance against current targeted cyber threats. We consider a first-order nonlinear differential equation, the Bernoulli equation, which describes the process of the time series of the intensity of cyberattacks. The analysis of the intensity function of cyberattacks is carried out analytically due to the power-law p-transformation by the analytical function. Statistical data on the number of cyberattacks at the enterprise are considered, provided that a scheduled audit is carried out once a quarter. The types of cyberattacks to defeat network infrastructure, proprietary applications, the level of patches and server configurations, standard software, and their number at the enterprise for certain time periods are presented. A geometric visualization of the change in the steepness of the logistic curve of the intensity of cyberattacks is presented at various parameter values with a uniform step for the period between scheduled audits when applying p-conversion.

Keywords: cyber security, cyberattack intensity, Bernoulli equation, defeat, logistic curve.

УДК 004.85

к.т.н., доц. **Бойчук В.О.** (ХмНУ)
к.е.н., доц. **Бойчук А.А.** (ТНЕУ)
Бойчук М.В. (ХмНУ)
Бурдюг О.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/66-07

МЕТОД ФОРМУВАННЯ ПОСЛІДОВНОСТІ ДІЙ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ

У статті запропоновано підхід, де реалізація формування послідовностей дій інтелектуальних агентів виконується по аналогії з діяльністю біологічних організмів з використанням механізму емоцій для динамічного налаштування організму на виконання дій. Таким чином імітуються функції лімбічної системи в організації рухів на основі мотиваційної поведінки. При плануванні в першу чергу визначається загальний стан агенту. Використовуючи отриманий стан формується послідовність дій. Такий підхід дасть можливість динамічно переналаштовувати послідовність і реагувати на небезпечну ситуацію або на зміну внутрішнього стану агенту.

Інтелектуальний агент отримує з сенсорів і рецепторів ознаки початкової умови по ній визначається ціль та формується послідовність дій. Елементами послідовності дій є елементарні дії. Елементарна дія характеризується набором вхідних параметрів для функціонування. Ознаки передумови відповідають першій дії в послідовності, остання дія в послідовності прив'язана до ознаки цілі.

Послідовність дій агенту представляється орграфом, де вершини визначають елементарні дії, а ребра визначають ступінь сили зв'язку між ними. Початкові умови відповідають першій дії в послідовності, з неї розпочинається реалізація послідовності дій. Ознаки цілі відповідають останній вершині в послідовності дій

Ваги зв'язків змінюються при встановлені змінних загального стану, що дає змогу виконати послідовність дій в реальному масштабі часу з динамічним переналаштуванням і вибрати серед характерних для конкретного стану послідовностей дій. Метод формує послідовність дій, яка ініціюється емоційними станами, і переводить її в послідовність автоматичних дій на основі досягнення цілі і яка в майбутньому буде виконуватись в нормальному стані. Для перевірки функціонування методу реалізований симулятор агенту-роботу в середовищі програми V-REP. Отримані результати можуть бути використані для інтелектуального планування на основі підкріплення при керуванні агентами, роботами на виробничих підприємствах, військовими агентами, потоками міського руху, логістичними системами, соціальними явищами.

Ключові слова: інтелектуальний агент, планування, модель, Q-навчання, емоційні стани, навчання з підкріпленням.