УДК 35.004

БУТВІН Борис Леонідович
ВАСИЛЬЄВА Ольга Олександрівна

НЕЛІНІЙНИЙ МЕТОД ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ НА ОСНОВІ МЕТОДУ ГРУПОВОГО УРАХУВАННЯ АРГУМЕНТІВ

Постановка проблеми. Стрімке зростання інформатизації всіх сторін життя зумовлює появу нових форм і методів ведення війни – інформаційного протистояння як в економічних, так і політичних та військових аспектах світової політики й економіки. Це протиборство активно обговорювалося на Всесвітньому економічному форумі в Давосі у 2018 році [11], де зроблено висновки, що прямо вказують на велику небезпеку ризиків інформаційної безпеки для сучасного суспільства. У зв'язку з цим критичною стає роль аналізу й управління ризиками інформаційної безпеки як інструменту виявлення інформаційних атак, а також проведення комплексу організаційної та технічної протидії цим загрозам.

Останнім часом кількість кібернетичних атак на організації різного рівня подвоїлася. Атаки, що призводять до значних збитків, стають звичайним явищем. Фінансові збитки від атак зростають, і найбільші втрати пов'язані з атаками вірусів-вимагачів. Таким прикладом є атаки вірусів-здирників WannaCry і NotPetya [12] на понад 300 тис. комп'ютерів у 150 країнах світу, що призвели до фінансових втрат понад 300 млн дол.

Ще однією тенденцією є збільшення кількості атак на об'єкти критичної інфраструктури та стратегічні промислові об'єкти, що може призвести до виведення з ладу зловмисниками систем, які підтримують життєзабезпечення людства, та виникнення глобальних техногенних катастроф. Особливо це стало масовим під час агресії рф проти України.

Отже, ризики інформаційної безпеки входять до трійки найімовірніших ризиків, які суттєво загрожують національній безпеці України. Тому управління ризиками інформаційної безпеки є одним із пріоритетних напрямів розвитку організацій по всьому світу й абсолютно необхідне для їхнього подальшого функціонування.

Головною метою сучасних держав є створення комплексу організаційних і технічних установ із метою достовірного оцінювання, управління ризиками інформаційної безпеки й підтримки їх на прийнятному для держави рівні.

Центральним завданням таких систем є оцінювання інформаційних ризиків. Тому розроблення методичного апарату оцінювання інформаційних ризиків із високим рівнем достовірності й адекватності є одним із важливих і сучасних завдань ведення інформаційного протистояння.

Із-за своєї складності як із погляду політики, так і технологій кібербезпека є однією з головних проблем у сучасному світі та одною з найважливіших складових успішного розвитку суспільства.

Оцінювання ризиків являє собою процес систематичного контролю й оцінювання ефективності діяльності державних і комерційних установ. Слід зазначити, що без оцінювання інформаційних ризиків неможливо вирішити завдання запобігання їм.

У класичному поданні ризик – це ймовірність реалізації загрози інформаційній безпеці.

З математичного погляду при аналізі ризиків такі фактори можна вважати вхідними параметрами. При цьому потрібно враховувати безліч джерел інформації та невизначеність самої інформації. На етапі оцінювання ризиків найбільший інтерес становить безпосередньо методичний підхід до розрахунку значення ризику. Аналіз сучасного методичного забезпечення оцінювання інформаційних ризиків [1; 2] показує, що більшість методів засновано на правилах математичного та логічного складання ризиків, без урахування взаємовпливу загроз при розрахунку інтегрального інформаційного ризику для об'єкта інформаційного захисту. Неврахування цього впливу може призвести до значного спотворення результатів. Метод групового урахування є досить сучасним підходом до побудови нелінійних функціональних залежностей із досить високою достовірністю результатів. У цій статті автори зробили спробу застосування цього методу до оцінювання інформаційних ризиків.

Аналіз останніх досліджень і публікацій. Застосування інформаційних технологій є одним із важливих чинників, що визначають ефективність роботи як органів державної влади, так і комерційних установ. Унаслідок труднощів формалізації більшості інформаційних загроз їхнє кількісне оцінювання є досить складним [13].

Аналізу інформаційних ризиків та розробленню методології їх оцінювання присвячено низку робіт сучасних українських учених. Указаною проблематикою зокрема займалися: А. Корченко [1], О. Архипов [2], О. Замула [13]. Результати цієї роботи зафіксовані в міжнародних стандартах [9; 10].

Аналіз джерельної бази дає змогу зробити такі висновки.

По-перше, складно зібрати дані, необхідні для кількісного оцінювання інформаційних ризиків, оскільки потрібні точність реєстрації, її безперервність і досить тривалий період, щоб дані були придатні для побудови робочої моделі.

По-друге, сучасне інформаційне середовище схильне до частих змін через постійне вдосконалення програмного й апаратного забезпечення. Отже,

необхідно побудувати максимально гнучку модель інформаційного середовища державної установи, яку можна було б змінювати із зміною складових цього середовища.

І, по-третє, витрати часу й людських ресурсів на аналіз уразливості до ризиків досить високі, що не дає змоги проводити його з необхідною періодичністю. Для державних установ процес систематизованого збирання даних, їх відстеження та перевірки, періодичного аналізу і налагодження звітності – поки невирішене завдання. Для того, щоб реалізувати цей процес, необхідно спочатку провести ідентифікацію інформаційних ризиків.

Метою статті є викладення основних методичних положень нелінійного підходу до оцінювання інформаційних ризиків на основі методу групового урахування аргументів (МГУА) академіка А. Г. Івахненка [6–8]. Він дає змогу усунути такий недолік як неврахування взаємного впливу інформаційних загроз на конфіденційність, цілісність і доступність інформації, що значною мірою підвищує достовірність та адекватність отриманих результатів оцінювання інформаційних ризиків.

Предметом дослідження є розроблення методичних положень нелінійного методу оцінювання інформаційних ризиків, а метою – підвищення достовірності й адекватності моделей розрахунку інформаційних ризиків.

Виклад основного матеріалу. Оцінювання та управління ризиками є взаємопов'язаними процесами, які мають у цілому шість логічних кроків [1; 2; 13], за допомогою яких відбувається оцінювання, управління ризиками, розроблення та виконання стратегії управління ризиками.

Щоб отримати узагальнену оцінку ризику, на практиці використовуються такі правила [13]:

1) правило поглинання ризиків: якщо ризики належать до однієї сфери діяльності та/або їхня міра збігається, але прояв негативних факторів відбувається незалежно один від одного, ймовірність їхнього прояву оцінюється за максимальним значенням;

2) правило математичного складання ризиків: якщо ризики належать до різних сфер діяльності та/або їхні заходи різняться, але прояв негативних факторів відбувається незалежно один від одного, ймовірність їхнього прояву оцінюється як сума ймовірностей незалежних подій, а міра ризику оцінюється як середнє арифметичне (для двох факторів):

$$p_o = p_1 + p_2 + p_1 \cdot p_2$$
$$M_{po} = \frac{p_1 \cdot M_{p1} + p_2 \cdot M_{p2}}{p_1 + p_2}; \quad (1)$$

3) правило логічного складання ризиків: якщо ризики належать до різних сфер діяльності та/або їхні заходи різняться, а негативні фактори проявляються залежно один від одного, ймовірність їхнього прояву оцінюється на

основі правила логічного складання – ступінь ризику в цьому випадку розраховується за такою формулою:

$$p_o = 1 - \prod q_j. \quad (2)$$

Методи оцінювання інформаційних ризиків використовуються в міжнародних стандартах [1; 2; 9; 10].

Так, відповідно до ISO/IEC 27001 «Інформаційні технології» обрана методологія оцінювання повинна гарантувати те, що оцінки ризику дають порівняні та відтворювані результати. Але в цьому стандарті не наводиться конкретна формула розрахунку [1].

У стандарті NIST 800-30 «Risk management guide for information technology systems» [1; 2; 9; 10] наводиться така класична формула розрахунку ризику:

$$R = P(t) \cdot S, \quad (3)$$

де R – значення ризику;

P(t) – ймовірність реалізації загрози інформаційній безпеці (застосовується поєднання якісної та кількісної шкал);

S – ступінь впливу загрози на актив (ціна активу в якісній та кількісній шкалах).

У результаті обчислюється значення ризику у відносних одиницях, яке можливо ранжувати за ступенем значущості для процедури управління ризиками інформаційної безпеки [2].

Відповідно до ИСО/МЭК ТО 13335-3-2007 «Інформаційні технології. Методи та засоби забезпечення безпеки. Частина 3. Методи менеджменту безпеки інформаційних технологій», на відміну від стандарту NIST 800-30 «Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology» [1; 2; 9; 10], оцінювання ризиків відбувається за такою формулою:

$$R = P(t) \cdot P(v) \cdot S, \quad (4)$$

де P(t) – ймовірність реалізації загрози інформаційній безпеці;

P(v) – ймовірність наявності вразливості;

S – цінність активу.

Для розрахунку значень імовірностей P(t) і P(v) застосовується якісна шкала з трьома рівнями (низьким, середнім і високим). Для оцінювання значення цінності активу S застосовуються числові значення в інтервалі від 0 до 4.

Відповідно до стандарту BS 7799-2:2005 «Специфікація системи управління інформаційною безпекою» рівень ризику обчислюється з урахуванням таких показників: цінності ресурсу, рівня загрози та ступеня вразливості. Зі

збільшенням значень цих параметрів ризик зростає. Отже, формулу можна подати в такому вигляді:

$$R = S\ L\ (t)\ L\ (v), \tag{5}$$

де S – цінність активу (ресурсу);
L(t) – рівень загрози;
L(v) – рівень (ступінь уразливості).

Для виконання якісного оцінювання ризиків інформаційної безпеки використовується таблиця відповідності ступеня тяжкості наслідків та ймовірності реалізації загрози. Якщо необхідно провести кількісне оцінювання, то формулу можна подати в такому вигляді:

$$R = P(v) \cdot S, \tag{6}$$

де S – цінність активу (ступінь тяжкості наслідків).

Найповнішим є врахування факторів ризику інформаційної безпеки, що складається з імовірностей реалізації загроз і використання вразливостей кожного компонента інформаційної інфраструктури з урахуванням рівня його конфіденційності, цілісності та доступності, вираховується за такими формулами [13]:

$$\begin{aligned} X_{Rc} &= X_c \cdot P(T) \cdot P(V); \\ X_{Ri} &= X_i \cdot P(T) \cdot P(V); \\ X_{Ra} &= X_a \cdot P(T) \cdot P(V), \end{aligned} \tag{7}$$

де X_{Rc} – значення оцінки ризику конфіденційності;
X_c – оцінка конфіденційності інформаційного активу;
$P(T)$ – можливість реалізації небезпеки;
$P(V)$ – ймовірність використання вразливості;
X_{Ri} – значення оцінки ризику цілісності;
Ki – коефіцієнт цілісності інформаційного активу;
X_{Ra} – значення ризику доступності;
X_a – значення оцінки доступності інформаційного активу.

Застосування такого алгоритму дає змогу провести детальніше оцінювання ризику, отримати в результаті безрозмірне значення ймовірності виникнення ризику компрометації кожного інформаційного активу окремо.

Надалі можливе обчислення значення шкоди. Для цього використовується усереднене значення ризику кожного інформаційного активу та розмір потенційних втрат. Значення збитків (L) розраховується за такою формулою:

$$L = Rcp \cdot S, \tag{8}$$

де Rcp – середнє значення ризику;
S – втрати, ум. од.

Однак слід зазначити, що ці підходи не дають можливості врахувати взаємний вплив конфіденційності, цілісності та доступності, що значною мірою знижує їхню цінність і становить наукову суперечність цих підходів.

Для вирішення цієї суперечності розрахуємо нелінійну функціональну залежність на основі методу групового урахування аргументів такого вигляду:

$$Y_R = F(X_{Rc}, X_{Ri}, X_{Ra}), \quad (9)$$

де $F(X_{Rc}, X_{Ri}, X_{Ra})$ – нелінійний функціонал.

Вибір МГУА для вирішення задачі нелінійного оцінювання (9) інформаційних ризиків зумовлений тим, що побудова адекватного рівняння лінійної регресії та його уточнення як класичного підходу до побудови нелінійних функціоналів потребує дедалі більшої ретроспективи (періоду розгляду статистичних даних), що зазвичай є неможливим. Збільшення кількості факторів супроводжується «прокляттям розмірності» [3; 5–8], сутність якого полягає в накопиченні сумарної помилки. Кількість структурних елементів моделі є обмеженою, що згідно з теоремою Геделя про неповноту [6] свідчить про існування такої заданої табличної залежності, яка не може бути апроксимована за допомогою композиції даного набору структурних елементів.

У загальному вигляді постановка нелінійного оцінювання інформаційних ризиків буде такою. Нехай є вибірка з A спостережень вхідних X_{Ri} та вихідних Y_{RI} векторів. За результатами спостережень треба визначити $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$, причому структура моделі $F(*)$ невідома. Найповніша залежність між входами X_{Ri} і виходами може бути представлена за допомогою узагальненого полінома Колмогорова – Габора [4–7].

Нехай є вибірка $X = \{x_{R1}, \ldots, x_{RN}\}$, тоді такий поліном має вигляд, наведений у формулі:

$$Yir = f(\mathrm{X}ri) = a_0 + \sum_{j=1}^{k} a_j x_j + \sum_{j=1}^{k} a_{jj} x_j^2 + \sum_{j,\gamma=1}^{k} a_{j\gamma} x_j x_\gamma + \cdots + \\ + \sum_{j=1}^{k} a_{jjj} x_j^3 + \cdots, \quad (10)$$

де $j<\gamma<k$.

У побудові моделі (визначенні значень коефіцієнтів) як критерій використовується критерій регулярності (селекції) [6].

Однак, ураховуючи те, що плани експериментів для побудови нелінійного функціоналу, які використовуються, є ортогональними, а класичні алгоритми МГУА некоректно працюють із наборами ортогональних даних, пропонується використовувати модифікований алгоритм, а саме – багатоетапний алгоритм з ортогоналізацією змінних [8]. Беручи до уваги те, що вхідні змінні вже є ортогональними, можна знехтувати першими двома етапами алгоритму, на яких здійснюється центрування вектор-стовпців матриці навчальної вибірки (A) та їхня ортогоналізація.

Безпосередньо процес побудови нелінійних моделей такий. На кожному кроці в поточну модель

$$\hat{y}_s\left(x_1, \dots, x_s, \hat{\theta}_1, \dots, \hat{\theta}_s\right) = \sum_{i=1}^{s} x_i \hat{\theta}_i \quad (11)$$

додаються два параметри: аргумент x_{s+1}, який не міститься серед множини аргументів поточної моделі, та оцінка коефіцієнта $\hat{\theta}_{s+1}$ при x_{s+1}:

$$\hat{y}_s\left(x_1, \dots, x_s, x_{s+1}, \hat{\theta}_1, \dots, \hat{\theta}_s, \hat{\theta}_{s+1}\right) = \sum_{i=1}^{s+1} x_i \hat{\theta}_i, \quad (12)$$

де s – номер кроку.

На першому етапі будується множина моделей, які залежать від одного аргументу, на другому – від двох і так далі до моделі, яка містить усі аргументи. На кожному кроці здійснюється відбір F найкращих моделей за критерієм селекції, які переходять на наступний етап. Критерій селекції розраховується за формулою:

$$AR_{B,r+1}=y_B^T y_B - 2c_{B,r+1} + a_{B,r+1}, \quad (13)$$

де B – перевірочна вибірка, $A \cap B = \emptyset$;

r – номер шагу ітерації;

$c_{B,r+1}$ та $a_{B,r+1}$ – оціночні коефіцієнти, які визначаються як:

$$c_{B,r+1} = c_{B,r}\hat{\theta}_{B,r+1} + x_{B,r+1}^T y_B \hat{\theta}_{B,r+1}^{r+1},$$
$$a_{B,r+1} = a_{B,r}\left(\hat{\theta}_{B,r+1}\right)^2 + + 2\hat{\theta}_{B,r+1}\hat{\theta}_{B,r+1}^{r+1} b_{B,r} + + \left(\hat{\theta}_{B,r+1}^{r+1}\right)^2 x_{B,r+1}^T x_{B,r+1}, \quad (14)$$
$$b_{B,r} = \hat{y}_{B,r}^T x_{B,r+1}.$$

Після побудови всіх моделей відбувається представлення моделі через вихідні ознаки та розрахунок вільного члена моделі як:

$$\hat{\theta}_{A,0} = \bar{y}_A - \sum_{i=1}^{m} \hat{\theta}_{A,i}\bar{x}_{A,i}. \quad (15)$$

За отриманою моделлю, яка описується таким функціоналом:

$$y = f(x_1, x_2, \dots, x_N), \quad (16)$$

здійснюються розрахунки значень відповідних станів залежно від показників нижнього рівня. При цьому, як зазначалося вище, кожен із множини $(x_1, x_2, \dots, x_N)$ у свою чергу може бути функцією.

Розглянемо практичні аспекти побудови функціоналу $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ за допомогою програми GMDH Shell 3_6_7 [4] за кроками.

Крок 1. Завдання матриці планування експериментів вхідних даних такого вигляду (див. рис. 1). Для цього потрібне залучення спеціалістів з інформаційної безпеки, які здатні провести експертно-аналітичне оцінювання інформаційних загроз у багатовимірному просторі показників X_{Rc}, X_{Ri}, X_{Ra}. Як шкали оцінювання в таблиці застосована п'ятирангова рівномірна шкала, де перший ранг – це мінімальний рівень, а п'ятий ранг – максимальний.

ID	Xrc	Xri	Xra	Yr
1	1	5	5	4
2	5	5	5	5
3	5	1	5	5
4	5	1	1	3
5	5	5	1	4
6	1	1	5	3
7	1	1	1	1
8	3	5	1	2
9	1	5	1	3
10	1	3	1	2
11	5	1	3	3
12	1	1	3	2
13	1	5	3	3
14	5	1	3	4
15	3	3	3	3

Рисунок 1 – Матриця вхідних даних A

Крок 2. Вибір вихідної змінної (див. рис. 2). Як вихідна оцінка застосована змінна Y_R.

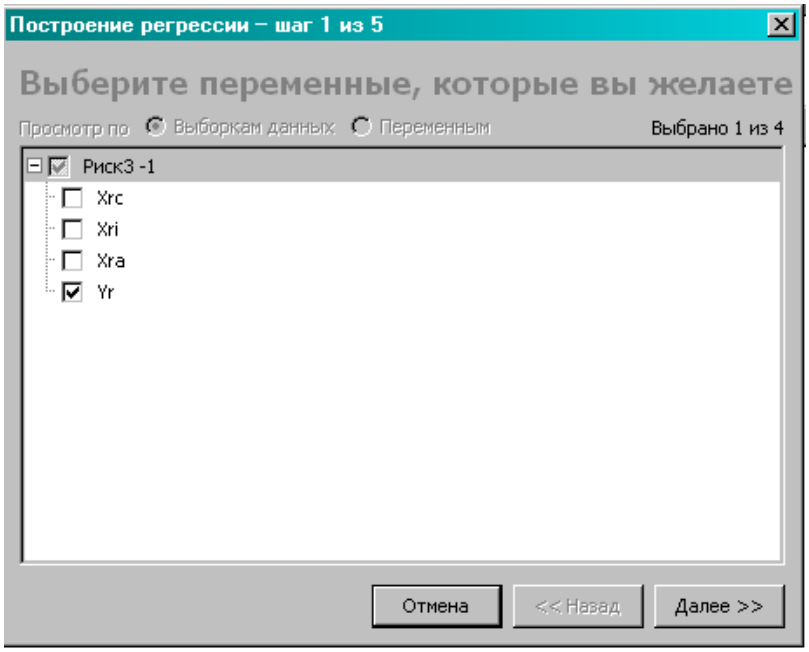


Рисунок 2 – Вибір вихідної змінної

Крок 3. Вибір вхідних змінних (див. рис. 3).

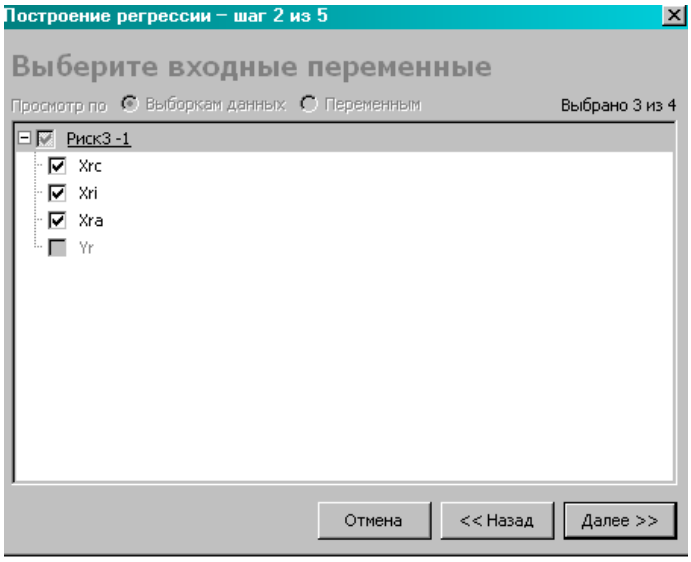


Рисунок 3 – Вибір вхідних змінних

Крок 4. Обробка – побудова нелінійного функціоналу (див. рис. 4). Програма застосовує комплекс адаптивних методів розрахунку нелінійної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$, результати оцінювання яких наведено на рис. 4.

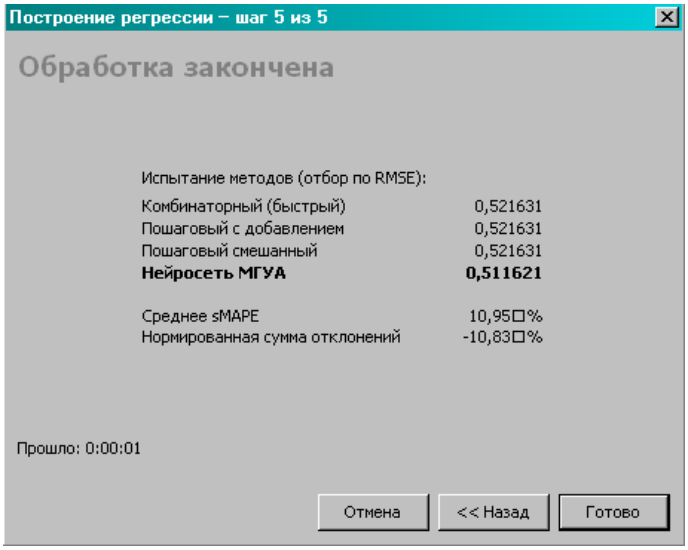


Рисунок 4 – Побудова нелінійного функціоналу $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$

Крок 5. Кінцеве отримання результатів розрахунків. Графічне уявлення результатів розрахунків (див. рис. 5).

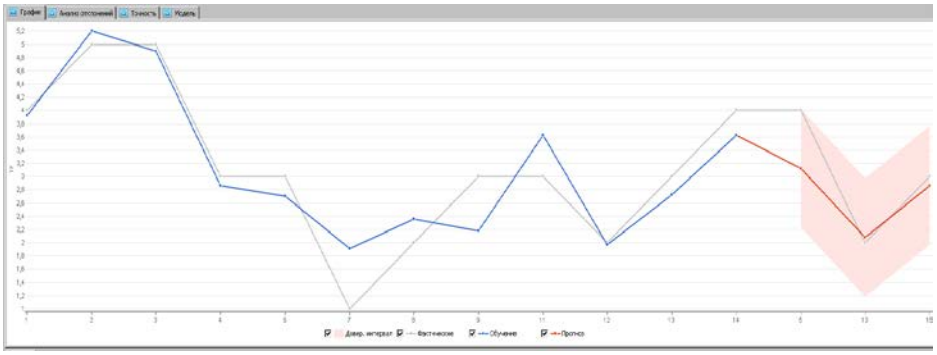


Рисунок 5 – Графічне уявлення результатів розрахунків

Крок 6. Оцінювання вкладу вхідних змінних X_{Rc}, X_{Ri}, X_{Ra} у вихідну змінну Y_R (див. рис. 6).

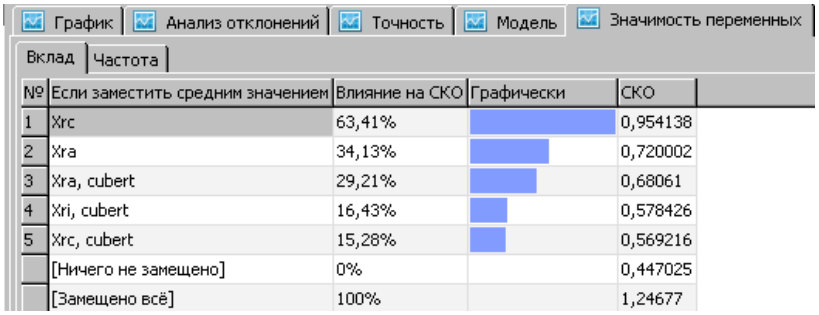


График | Анализ отклонений | Точность | Модель | Значимость переменных

Вклад | Частота

№	Если заместить средним значением	Влияние на СКО	Графически	СКО
1	Xrc	63,41%		0,954138
2	Xra	34,13%		0,720002
3	Xra, cubert	29,21%		0,68061
4	Xri, cubert	16,43%		0,578426
5	Xrc, cubert	15,28%		0,569216
	[Ничего не замещено]	0%		0,447025
	[Замещено всё]	100%		1,24677

Рисунок 6 – Вклад вхідних змінних X_{Rc}, X_{Ri}, X_R у вихідну змінну Y_R

Крок 7. Розрахунок аналітичної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ (див. рис. 7).

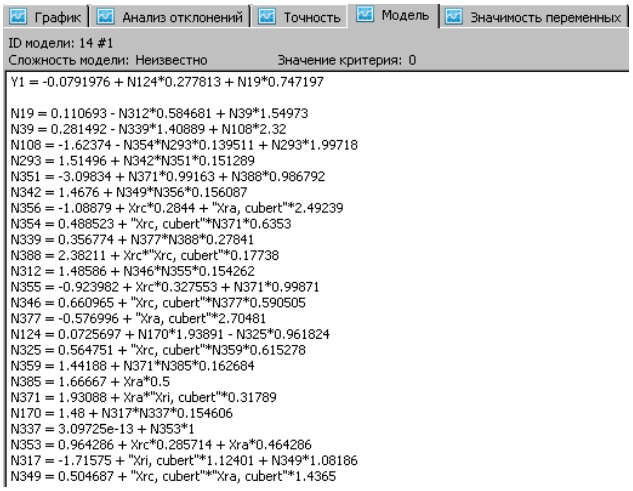


График | Анализ отклонений | Точность | Модель | Значимость переменных

ID модели: 14 #1
Сложность модели: Неизвестно Значение критерия: 0

```
Y1 = -0.0791976 + N124*0.277813 + N19*0.747197

N19 = 0.110693 - N312*0.584681 + N39*1.54973
N39 = 0.281492 - N339*1.40889 + N108*2.32
N108 = -1.62374 - N354*N293*0.139511 + N293*1.99718
N293 = 1.51496 + N342*N351*0.151289
N351 = -3.09834 + N371*0.99163 + N388*0.986792
N342 = 1.4676 + N349*N356*0.156087
N356 = -1.08879 + Xrc*0.2844 + "Xra, cubert"*2.49239
N354 = 0.488523 + "Xrc, cubert"*N371*0.6353
N339 = 0.356774 + N377*N388*0.27841
N388 = 2.38211 + Xrc*"Xrc, cubert"*0.17738
N312 = 1.48586 + N346*N355*0.154262
N355 = -0.923982 + Xrc*0.327553 + N371*0.99871
N346 = 0.660965 + "Xrc, cubert"*N377*0.590505
N377 = -0.576996 + "Xra, cubert"*2.70481
N124 = 0.0725697 + N170*1.93891 - N325*0.961824
N325 = 0.564751 + "Xrc, cubert"*N359*0.615278
N359 = 1.44188 + N371*N385*0.162684
N385 = 1.66667 + Xra*0.5
N371 = 1.93088 + Xra*"Xri, cubert"*0.31789
N170 = 1.48 + N317*N337*0.154606
N337 = 3.09725e-13 + N353*1
N353 = 0.964286 + Xrc*0.285714 + Xra*0.464286
N317 = -1.71575 + "Xri, cubert"*1.12401 + N349*1.08186
N349 = 0.504687 + "Xrc, cubert"*"Xra, cubert"*1.4365
```

Рисунок 7 – Результат розрахунку аналітичної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$

Для оцінювання адекватності побудови аналітичної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ були застосовані статистичні показники. Результати їхнього оцінювання наведено на рис. 8.

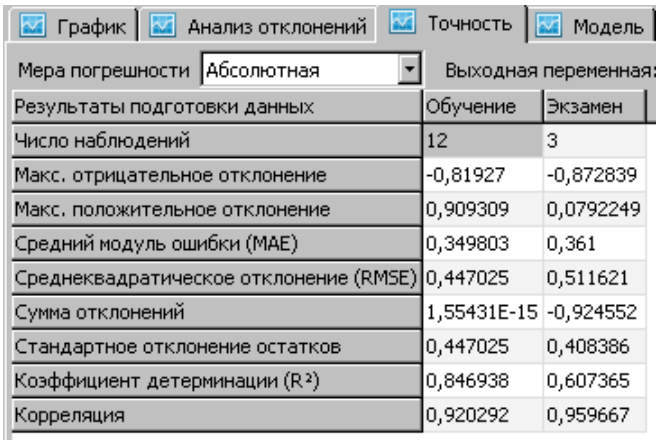


График	Анализ отклонений	Точность	Модель

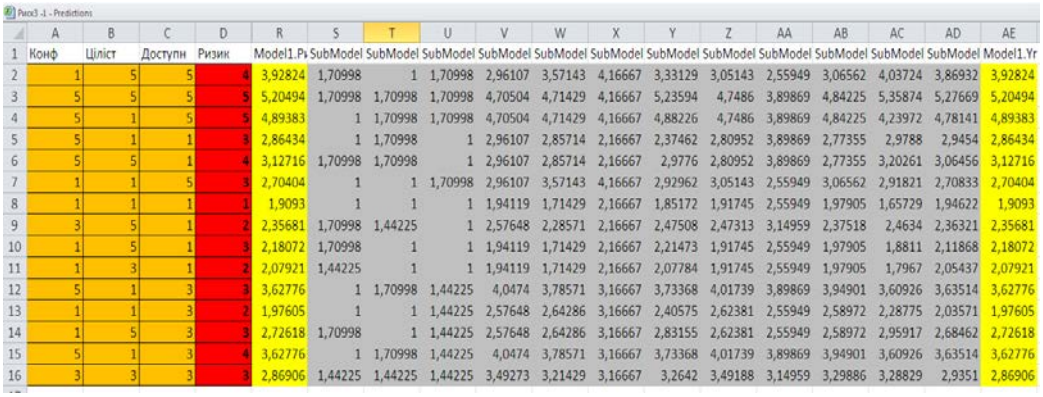
Мера погрешности: Абсолютная — Выходная переменная:

Результаты подготовки данных	Обучение	Экзамен
Число наблюдений	12	3
Макс. отрицательное отклонение	-0,81927	-0,872839
Макс. положительное отклонение	0,909309	0,0792249
Средний модуль ошибки (MAE)	0,349803	0,361
Среднеквадратическое отклонение (RMSE)	0,447025	0,511621
Сумма отклонений	1,55431E-15	-0,924552
Стандартное отклонение остатков	0,447025	0,408386
Коэффициент детерминации (R^2)	0,846938	0,607365
Корреляция	0,920292	0,959667

Рисунок 8 – Результати оцінювання адекватності нелінійної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$

У процесі практичного застосування нелінійної моделі $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ виникають значні труднощі. Більше розповсюдженим є середовище *EXEL*. Тому для практичного використання доцільно конвертувати нелінійну модель $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ у програмне середовище EXCEL.

Крок 8. Конвертування нелінійного функціоналу в середовище EXEL із метою отримання практичного результату у найпоширенішому програмному середовищі (див. рис. 9).



	A	B	C	D	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
1	Конф	Ціліст	Доступн	Ризик	Model1.Pr	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	SubModel	Model1.Yr
2	1	5	5	4	3,92824	1,70998	1	1,70998	2,96107	3,57143	4,16667	3,33129	3,05143	2,55949	3,06562	4,03724	3,86932	3,92824
3	5	5	5	5	5,20494	1,70998	1,70998	1,70998	4,70504	4,71429	4,16667	5,23594	4,7486	3,89869	4,84225	5,35874	5,27669	5,20494
4	5	1	5	5	4,89383	1	1,70998	1,70998	4,70504	4,71429	4,16667	4,88226	4,7486	3,89869	4,84225	4,23972	4,78141	4,89383
5	5	1	1	3	2,86434	1	1,70998	1	2,96107	2,85714	2,16667	2,37462	2,80952	3,89869	2,77355	2,9788	2,9454	2,86434
6	5	5	1	4	3,12716	1,70998	1,70998	1	2,96107	2,85714	2,16667	2,9776	2,80952	3,89869	2,77355	3,20261	3,06456	3,12716
7	1	1	5	3	2,70404	1	1	1,70998	2,96107	3,57143	4,16667	2,92962	3,05143	2,55949	3,06562	2,91821	2,70833	2,70404
8	1	1	1	1	1,9093	1	1	1	1,94119	1,71429	2,16667	1,85172	1,91745	2,55949	1,97905	1,65729	1,94622	1,9093
9	3	5	1	2	2,35681	1,70998	1,44225	1	2,57648	2,28571	2,16667	2,47508	2,47313	3,14959	2,37518	2,4634	2,36321	2,35681
10	1	5	1	3	2,18072	1,70998	1	1	1,94119	1,71429	2,16667	2,21473	1,91745	2,55949	1,97905	1,8811	2,11868	2,18072
11	1	3	1	2	2,07921	1,44225	1	1	1,94119	1,71429	2,16667	2,07784	1,91745	2,55949	1,97905	1,7967	2,05437	2,07921
12	5	1	3	3	3,62776	1	1,70998	1,44225	4,0474	3,78571	3,16667	3,73368	4,01739	3,89869	3,94901	3,60926	3,63514	3,62776
13	1	1	3	2	1,97605	1	1	1,44225	2,57648	2,64286	3,16667	2,40575	2,62381	2,55949	2,58972	2,28775	2,03571	1,97605
14	1	5	3	3	2,72618	1,70998	1	1,44225	2,57648	2,64286	3,16667	2,83155	2,62381	2,55949	2,58972	2,95917	2,68462	2,72618
15	5	1	3	4	3,62776	1	1,70998	1,44225	4,0474	3,78571	3,16667	3,73368	4,01739	3,89869	3,94901	3,60926	3,63514	3,62776
16	3	3	3	3	2,86906	1,44225	1,44225	1,44225	3,49273	3,21429	3,16667	3,2642	3,49188	3,14959	3,29886	3,28829	2,9351	2,86906

Рисунок 9 – Результат конвертування аналітичного функціоналу $Y_R = F(X_{Rc}, X_{Ri}, X_{Ra})$ у середовище EXEL

Отже, застосування МГУА для вирішення задачі нелінійного оцінювання інформаційних ризиків є досить доцільним як із прагматичного, так і

теоретичного погляду. Застосування нелінійного підходу до розрахунку аналітичних функціоналів оцінювання інформаційних ризиків забезпечує досить високу достовірність збігу експериментальних і розрахункових даних (R = 0.8469 у прикладі розрахунку, що наведено на рис. 9).

Висновки.

1. Проведено аналіз сучасних підходів до оцінювання інформаційних ризиків. Він показав, що більшість відомих методів оцінювання інформаційних ризиків засновані на правилах математичного та логічного складання ризиків, що суттєво знижує достовірність отриманих результатів. Для підвищення достовірності й адекватності результатів оцінювання інформаційних ризиків авторами запропоновано застосування нелінійного методу групового урахування аргументів.

2. Викладено загальний методичний підхід до оцінювання інформаційних ризиків у нелінійній постановці задачі.

3. Як нелінійний метод оцінювання інформаційних ризиків має практичне втілення застосування методу групового урахування аргументів на основі програми GMDH Shell 3_6_7.

4. Конвертування отриманого нелінійного функціоналу дає змогу проводити практичні розрахунки в середовищі EXEL, що значною мірою розширює можливості застосування цього методичного підходу.

Список використаних джерел

1. Корченко А. Г., Архипов А. Е., Казмирчук С. В. Анализ и оценивание рисков информационной безопасности. Київ : ООО «Лазурит-Полиграф», 2013. 275 с.

2. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навчальний посібник. Київ : НА СБУ, 2019. 268 с.

3. Ивахненко А. Г., Юрачковский Ю. П. Моделирование сложных систем по экспериментальным данным. Москва : Радио и связь, 1986. 118 с.

4. Основи застосування програми GMDH. URL: http://www.GMDH (дата звернення: 12.11.2022).

5. Маркова Е. В., Грановский Ю. В. Планирование эксперимента при поиске оптимальных условий. Москва : Наука, 1976. 280 с.

6. Ивахненко А. Г., Юрачковский Ю. П. Моделирование сложных систем по экспериментальным данным. Москва : Радио и связь, 1987. 120 с.

7. Ивахненко А. Г. Индуктивный метод самоорганизации моделей сложных систем. Киев : Наукова думка, 1982. 296 с.

8. Павлов А. В. Многоэтапный алгоритм МГУА с ортогонализацией переменных и его рекуррентный метод расчета коэффициентов и критерия селекции моделей. *Вісник НТЕУ «КПІ» Інформатика, управління та обчислювальна техніка.* 2012. № 57. С. 18–24.

9. Основи стандарту ISO 27001-2013. URL: www.pqm-online.com/assets/files/pubs/translations/std/iso-mek—2013 (rus).pdf (дата звернення: 12.11.2022).

10. Основи стандарту ISO 27001. URL: http://www.amu.kz/inf-bezopasnost/ISO27001.pdf ; http://www.almaz-art.com/docs/dstuISO_IEC27001_2015u.pdf (дата звернення: 12.11.2022).

11. Результати Економічного форуму в Давосі. URL: https://rus.lb.ua/economics/2018/01/29/388395_davos2018_glavnie_

temi_world.html (дата звернення: 12.11.2022).

12. Результати дослідження дії вірусу-шантажиста Петя. URL: https://habr.com/ru/company/varonis/blog/337186/ (дата звернення: 12.11.2022).

13. Замула О. А., Черниш В. І., Землянко Ю. В. Математичні методи оцінювання інформаційних ризиків компанії. *Прикладна радіоелектроніка* : науково-технічний журнал. 2011. Т. 10. № 2. С. 259–263.

Анотація. У статті викладено основні методичні положення нового нелінійного підходу на основі методу групового врахування аргументів до оцінки інформаційних ризиків як одної із складових дослідження інформаційної безпеки держави.

На етапі розвитку інформаційних технологій оцінювання інформаційних ризиків може бути автоматизовано за допомогою відповідних програмно-технічних систем. Аналіз показав, що існуючі методи та методики оцінювання інформаційних ризиків здебільшого використовують лінійні підходи, що може призвести до суттєвих методичних помилок.

Тому застосування нелінійних методів для оцінювання інформаційних ризиків є актуальним як у теоретичному значенні, так і практичній площині. Застосування розробленого нелінійного методу оцінювання інформаційних ризиків дає можливість суттєво підвищити достовірність і адекватність математичних моделей розрахунку інформаційних ризиків. Розроблений метод конвертування отриманого нелінійного функціоналу дає змогу проводити практичні розрахунки в середовищі EXEL, що значною мірою розширює можливості застосування цього методичного підходу.

Ключові слова: національна безпека, кібербезпека, інформаційні ризики, групове врахування аргументів.

Abstract. The article outlines main methodical provisions of the new non-linear approach on the basis of the group method of data handling to assess information risks as one of the components of the state information security research.

At the stage of information technologies advancement, information risk assessment can be automated through applying appropriate software and hardware systems. The analysis showed that existing methods and techniques for assessing information risks mostly use linear approaches, which can lead to significant methodological errors.

Therefore, the use of non-linear methods for assessing information risks is significantly relevant both in theory and practice. The nonlinear method application to assess information risks enables significant increase of the reliability and adequacy of mathematical models for calculating information risks. The developed method of converting the obtained nonlinear functional analysis enables carrying out practical calculations in the EXEL environment, which greatly expands the potential of applying this methodological approach.

Key words: national security, cyber security, information risks, group method of data handling.